Rapport d'habilitation à diriger les recherches

Contribution de la métrologie Internet à l'ingénierie des réseaux

Par

Philippe Owezarski

Chargé de recherche au CNRS

LAAS-CNRS - 7 Avenue du Colonel Roche - 31077 Toulouse cedex 4 – France
Tél : 05 61 33 63 17 e-mail : owe@laas.fr

Septembre 2006

Remerciements

Arrivé à la fin de la rédaction de ce mémoire d'HDR, qui est le fruit de 14 années de recherches (même s'il n'en retrace que 6) d'abord en DEA, puis en thèse, et enfin en tant que chargé de recherche – toujours au LAAS, avec cependant une parenthèse sabbatique chez Sprint aux Etats-Unis – force est de constater qu'il décrit surtout le travail d'une équipe de recherche – le groupe OLC du LAAS – avec des contributions de tous les membres de la communauté française et internationale des chercheurs en réseaux, et parfois même un peu plus. Il est évident que sans toutes les aides et toutes les discussions que j'ai eues, jamais ce travail n'aurait été accompli. Je tiens donc à adresser à chacune des personnes qui m'ont aidé, que j'ai côtoyées et avec lesquelles j'ai interagi, mes plus sincères remerciements.

Je tiens tout particulièrement à remercier Michel Diaz, directeur de recherche au CNRS, de m'avoir suivi depuis le premier jour où je suis arrivé au LAAS et de me faire profiter au quotidien de toute son expérience du métier de chercheur. Michel est assurément quelqu'un qui a énormément compté et compte toujours beaucoup pour moi. C'est pour beaucoup à son contact que le chercheur que je suis devenu s'est façonné.

Je tiens également à remercier chaleureusement tous les membres du jury d'avoir accepté mon invitation à participer à cette soutenance, d'avoir lu ce manuscrit, de l'avoir commenté – souvent critiqué – pour me permettre de le rendre meilleur. De plus, vous êtes tous des chercheurs que j'ai eus le plaisir de côtoyer très régulièrement et avec qui j'ai eu plaisir à discuter et à travailler. Je vous remercie très sincèrement de votre présence et de votre soutien.

J'adresse donc de très sincères et chaleureux remerciements à :

- Abdelmalek Benzekri, Professeur à l'université Paul Sabatier à Toulouse, qui me prodigua mes premiers cours de réseau alors que j'étais en maîtrise d'informatique ;
- Christophe Diot, aujourd'hui directeur d'un laboratoire de recherche à Thomson, avec qui j'ai travaillé régulièrement depuis ma thèse, et qui m'a également accueilli dans son équipe à Sprint ATL lors de mon séjour sabbatique où il m'initia à la métrologie ;
- Serge Fdida, Professeur à l'université Pierre et Marie Curie à Paris 6, avec lequel je collabore depuis le début ;
- Olivier Festor, Directeur de recherche INRIA, et responsable d'une équipe de recherche avec laquelle j'entretiens de fréquentes et fructueuses collaborations ;
- Guy Leduc, Professeur à l'université de Liège, avec qui j'ai notamment eu le plaisir de travailler dans le cadre de projets européens, comme E-NEXT par exemple ;
- Francis Lepage, Professeur à l'université Henry Poincaré à Nancy, pour toutes les discussions que nous avons eues lors de conférences ou de réunions de travail, notamment celles de l'AS métrologie.

Si je peux aujourd'hui soutenir cette habilitation, je le dois en grande partie aux doctorants que j'ai encadrés ou que j'encadre encore (Nicolas, Yu, Silvia, Ion) et tous les stagiaires (trop nombreux à énumérer). Merci à chacun de vous pour tout ce que vous m'avez apporté, et surtout de m'avoir supporté. Je garderai toujours un souvenir ému de chacun de vous, en espérant vous avoir également apporté tout ce que je pouvais.

De même, ces travaux sont largement extraits des projets Metropolis et MétroSec. Je tiens donc à remercier sincèrement et chaleureusement tous les partenaires de ces projets et leur exprimer le plaisir que cela m'a procuré de travailler avec eux. J'adresse les mêmes remerciements à tous les partenaires de tous les projets dans lesquels j'ai eu le plaisir de travailler.

Je remercie également tous les membres – présents et passés – du groupe OLC et du LAAS pour leur amitié et leur patience.

Enfin, j'adresse mes remerciements à ma femme Anne pour son amour et son soutien, pour supporter depuis plus de 10 ans – sans trop me les reprocher – mes journées de travail à

rallonges et mes trop nombreux déplacements. J’espère malgré ces contraintes parvenir à faire ton bonheur. J’espère aussi que je serai un bon père pour notre petite Eve qui vient d’arriver dans notre foyer. Je vous aime toutes les deux plus que tout.

Table des matières

Résumé

Contribution de la métrologie Internet à l'ingénierie des réseaux

La croissance et les évolutions de l'Internet lors de ces deux dernières décennies ont considérablement augmenté la complexité des techniques mises en œuvre dans ce réseau, ainsi que les caractéristiques de son trafic. Ainsi, alors qu'on demande à l'Internet de fournir des services de communication de qualités garanties, la méconnaissance des caractéristiques de l'Internet et de son trafic ont conduit à l'échec de toutes les propositions faites en ce sens.
Mon travail de ces 6 dernières années a donc proposé d'utiliser la métrologie Internet pour régler ce problème et montre comment cette nouvelle (dans l'Internet) « science des mesures » fournit des éléments essentiels à l'évolution technique des réseaux. Ce travail aborde donc essentiellement la caractérisation et l'analyse du réseau et de son trafic, dont les résultats ont été utilisés pour la conception d'une nouvelle architecture de l'Internet basée sur un système de métrologie global qui permet de sensiblement améliorer les performances et la qualité des services de l'Internet. A noter que les résultats de caractérisation du trafic permettent de classifier les anomalies du trafic en anomalies légitimes (foules subites) et illégitimes (attaques) et ouvrent donc la voie à une nouvelle façon de penser la sécurité des réseaux de communication.

Mots clés : Internet, Métrologie, Qualité de Service, expérimentation réseau, sécurité.

Abstract

Contribution of Internet monitoring to network engineering

The increase and the evolution of the Internet during the two last decades have significantly increased the complexity of communication techniques in this network, as well as its traffic characteristics. Thus, while the Internet is requested to provide services with guaranteed qualities, the bad knowledge of its characteristics and its traffic lead to the failure of all proposals made for this purpose.
My work during the 6 last years proposed to use Internet monitoring for solving this issue, and shows how this new (new in the Internet) "science of measurements" provides essential information for the technical evolution of networks. This work then essentially deals with the characterization and analysis of the Internet networks and traffic, whose results lead to the design of a new Internet architecture based on a global monitoring system which allows a significant increase of the Internet performance and quality of service. Note also that the results on traffic characterization allow the classification of traffic anomalies into legitimate (as flash crowds) and illegitimate (attacks), and open new ways for the security of communication networks

Keywords: Internet, Monitoring, Quality of Service, network experiments, security.

Première partie

Curriculum Vitæ

1. Activité scientifique

1.1. Etat civil

Philippe Owezarski
Né le 16 janvier 1970 à Asnières / Seine (92)
36 ans, marié, 1 enfant
Nationalité française

1.2. Profil académique

Chargé de recherche au CNRS
Laboratoire et équipe d'accueil :

Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS – CNRS)
Groupe Outils Logiciels pour la Communication (OLC) – thème Architectures et Protocoles de Communication (APC)
7, Avenue du Colonel Roche
31077 Toulouse cedex 4
Tél : 05 61 33 63 17 ; Fax : 05 61 33 64 11 ; e-mail : owe@laas.fr

Décembre 1996 Doctorat de l'université Paul Sabatier Toulouse III obtenu le 20 décembre 1996 avec la mention « très honorable et félicitations du jury » devant le jury :

Guy Juanole	Président
Michel Banâtre Richard Castanet	Rapporteurs
Michel Diaz	Directeur de thèse
Claude Bétourné Jean-Pierre Courtiat Christophe Diot Jean-François Schmidt	Examinateur
Dominique Wartelle	Invité

Octobre 1997 Recruté au CNRS avec le statut de chargé de recherche de 2ème classe

Mars-Novembre 2000 Mis à disposition de Sprint ATL (Advanced Technology Labs) à Burlingame, Californie, USA pour un séjour sabbatique de 9 mois

Depuis janvier 2005 Responsable du thème APC du groupe OLC. Le thème APC que j'anime est constitué de 13 chercheurs permanents (2 directeurs de recherche CNRS, 1 chargé de recherche CNRS et 10 maîtres de conférences), 8 doctorants et 1 post-doc

1.3. Activités scientifiques

Activités de recherche

Depuis que j'ai été recruté au CNRS (1er octobre 1997), mon travail de recherche a principalement porté sur l'étude, la conception, l'implémentation et la mise en œuvre de systèmes distribués multimédias coopératifs à hauts débits, et plus particulièrement sur de nouvelles techniques de communications, de nouvelles architectures et de nouveaux protocoles pour la prochaine génération d'Internet (Internet Nouvelle Génération ou IPng), pour des applications telles la télé-ingénierie coopérative ou la téléformation par exemple. Ces travaux se situent dans le cadre de ceux du groupe "Outils Logiciels pour la Communication" qui se consacre à la recherche de méthodes, de techniques et d'outils pour la conception des systèmes, architectures et protocoles de communication et de coopération répartis. Les domaines principaux d'application de ces travaux concernent les réseaux informatiques et les télécommunications.

Plus précisément, et suite à un séjour de 9 mois aux Etats-Unis en 2000, passé à travailler dans le groupe de recherche Internet des laboratoires de Sprint – l'un des 3 principaux opérateurs Internet au monde – mon activité s'est enrichie d'une phase de métrologie des réseaux Internet existants et de leurs trafics. Les travaux en métrologie représentent la plus grande partie de mon activité de recherche aujourd'hui. La métrologie permet de caractériser le trafic réel, de le modéliser, d'analyser le comportement des protocoles et architectures de communication face à des situations de trafic concrètes, et de prédire ce que sera le trafic dans le futur. En particulier, les premiers résultats ont montré que le trafic n'était pas aussi régulier que ce qui était généralement admis. En particulier, le trafic Internet est très loin des modèles simples de Poisson ou de Gilbert (pour les pertes) qui sont ceux qui ont servi à concevoir le réseau téléphonique. Le trafic Internet est bien plus irrégulier et présente des propriétés de dépendance à long terme (LRD) et d'auto-similarité entraînant des variances énormes sur le trafic, et donc des problèmes considérables pour le dimensionnement des réseaux, la gestion de la qualité de service (ou QoS), ou les protocoles de routage et d'ingénierie des trafics. En particulier, ces observations sur les caractéristiques du trafic expliquent pourquoi les architectures et protocoles récents développés pour l'Internet nouvelle génération n'ont pas donné satisfaction une fois confrontés à la réalité. La métrologie – grâce aux possibilités de caractérisation, modélisation et prédiction des trafics qu'elle offre – permet de concevoir des solutions architecturales et protocolaires convenant parfaitement à la réalité qui sera celle du trafic Internet dans le futur.

Visibilité de ces travaux

Outre ces activités de recherche menées au LAAS-CNRS, je contribue ou ai aussi contribué à des groupes de travail nationaux et internationaux :

- **COST 237** de la commission européenne sur les "Multimedia telecommunications services", en particulier dans le domaine de la synchronisation multimédia (1995 – 1998) ;
- **ESPRIT CABERNET** qui était un réseau d'excellence sur les systèmes distribués ;
- le groupe de réflexion "Logiciels et réseaux de communication" de l'**OFTA** (Observatoire Français des Techniques Avancées), dont j'étais le rapporteur (septembre 1997 – mars 2000) ;
- le Groupe de Recherche **PRS** (Parallélisme, Réseaux et Systèmes), notamment dans le thème "Réseaux Hauts Débits Multimédias" (1993 – 1998). Ce GDR est aujourd'hui terminé, mais son action se prolonge dans le cadre du GDR **ARP** (Architecture Réseaux et Protocoles) et du thème **ING** (Internet Nouvelle Génération) auquel je participe également ;
- le groupe d'expert du **RNTL** (Réseau National de Technologie Logicielle) sur le thème : « Système de conception de produits et de services » (groupe B4). L'objectif de ce groupe

était d'identifier les besoins et manques au niveau des technologies logicielles, afin de préparer le premier appel d'offre du RNTL.
- Le **RTP (Réseau Thématique Pluri-disciplinaire) Sécurité du CNRS**
- Le **RTP « Réseaux de Communication » du CNRS**
- **L'AS (Actions spécifiques) Sécurité** du département STIC du CNRS
- **L'AS « Métrologie des réseaux de l'Internet »** du département STIC du CNRS dont j'étais co-animateur
- Le conseil scientifique du pôle **SINC** (Systèmes Informatiques Critiques) du LAAS

Par ailleurs, la visibilité de mes travaux s'est manifestée sous différents aspects :
- ***co-organisateur*** et ***co-président*** de la conférence internationale « Interactive Distributed Multimedia Systems and teleservices » (IDMS'99), Toulouse, France, 12 – 15 octobre 1999
- ***co-organisateur*** des Journées Doctorales en Informatique et Réseaux (JDIR'2002), Toulouse, France, 4 au 6 mars 2002
- ***co-président*** des rencontres francophones sur les aspects algorithmiques des télécommunications (ALGOTEL), mai 2005
- ***co-président*** du workshop on End-to-End MONitoring (E2EMON), mai 2005
- ***co-organisateur*** et ***co-président*** du comité de programme de la conférence on emerging technologies and experiments in networking (Co-NEXT), Toulouse, France, 24 – 27 Octobre 2005
- ***co-président*** de la session sur Internet Performance (IPERF'2006) lors de l'International Conference on Internet Surveillance and Protection (ICISP'2006)
- Rapporteur pour le RNTL (Réseau National de Technologie Logicielle)
- Auteur de 9 tutoriels :
  - 'Métrologie de la QoS Internet', Ecole d'été temps-réel'2003, Toulouse, France, 9-12 septembre 2003, avec Nicolas Larrieu
  - 'Trace based simulation', Ecole d'été du groupe Internet Nouvelle Génération (ING'2003) du GDR ARP, Porquerolle, France, 26-30 mai 2003
  - 'IP Network Monitoring and Measurements: Techniques and Experiences', ECOTEL'2002, Golfe-Juan, France, 2-6 Décembre 2002
  - 'IP Network Monitoring and Measurements: Techniques and Experience', Joint Internal Workshops on Interactive Distributed Multimedia Systems and Protocols for Multimedia Systems (IDMS/PROMS'2002), Coimbra, Portugal, November 26-29th, 2002
  - 'Métrologie des réseaux IP : application à la sécurité et à l'amélioration de la qualité de service des réseaux', Sécurité et Architectures Réseaux (SAR'2002), Marrakech, Maroc, 8-12 juillet 2002
  - 'What does IP monitoring tell about the future of the Internet', Journées Doctorales en Informatique et Réseaux (JDIR'2002), Toulouse, France, 4 mars 2002
  - 'Internet Traffic Analysis: Monitoring the Sprint IP backbone', Ecole d'été du groupe RHDM (Réseaux Hauts Débits Multimédias) du GDR ARP, Calcatoggio, Corse, 6-12 mai 2001, avec Christophe Diot
  - 'Le temps dans les réseaux longues distances', Ecole d'été temps-réel'99 – Applications, réseaux et systèmes, Poitiers, France, 13-16 septembre 1999
  - 'Modélisation, conception et implémentation de mécanismes de gestion des contraintes temps-réel dans les applications multimédias', Ecole d'été temps-réel'97 - Applications, réseaux et systèmes, Poitiers, France, 22-26 septembre 1997

- Co-éditeur avec Michel Diaz et Patrick Sénac de l'ouvrage 'Interactive Distributed Multimedia Systems and Telecommunication Services', Lecture Notes in Computer Science N° 1718 (LNCS 1718), Michel Diaz, Philippe Owezarski, Patrick Sénac Editors, Springer, October 1999
- Co-éditeur avec E. Al-Shaer et A. Pras de l'ouvrage 'Proceedings of the 3rd IEEE/IFIP Workshop on End-to-End Monitoring Techniques and Services – Monitoring Internet Traffic and Services' (E2EMON'2005), IEEE press, Nice, France, 15 may 2005
- Co éditeur avec Houssem Assadi et Ben Anderson d'un numéro spécial de la revue "Annals of Telecommunications" sur le sujet "Analysis of traffic and usage traces on the Internet: From network engineering to sociology of uses », Publication prévue pour le 1er semestre 2006
- Membre de nombreux comités de programmes de conférence ou de comités de lecture de journaux :
  - Computer Communication Journal,
  - Interactive Distributed Multimedia Systems (IDMS) : 1999, 2000, 2001, 2002
  - Ecole Temps Réel (ETR) : 1999, 2003
  - Journées Doctorales en Informatique et Réseaux (JDIR) : 2002, 2004
  - Sécurité et Architectures Réseau (SAR) : 2002, 2003, 2004, 2005, 2006
  - Multimedia Interactive Protocols and Systems (MIPS) : 2003, 2004
  - Service Assurance with Partial and Intermittent Resources (SAPIR) : 2004, 2005
  - IFIP/IEEE Integrated Management (IM) : 2005
  - IFIP/IEEE End-to-End Monitoring (E2EMON): 2005, 2006
  - International Conference on Multi-Provider QoS/SLA Internetworking (MPQSI) : 2005
  - Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (Algotel) : 2005, 2006
  - Conference on Emerging Technologies in Networking and Experiments (Co-NEXT) : 2005, 2006
  - IEEE/IFIP Network Operations and Management Symposium (NOMS) - Application session : 2006
  - 3rd International Conference on Wired / wireless Internet Communications (WWIC'2006)
  - Networking'2006
  - International Conference on Telecommunications and Multimedia (TEMU'2006)
  - International Conference on Networking and Services (ICNS'2006)
  - International Conference on Internet Surveillance and Protection (ICISP'2006)
  - ACM SIGCOMM Workshop on Large-Scale Attack Defense (LSAD'2006)
- Lecteur / évaluateur pour de très nombreuses conférences et journaux (Computer networks, annales des télécommunications, Techniques et sciences informatiques, IEE/ACM transactions on Networking, CFIP, DCCS, MMM, IEEE Infocom, Networking, IWQoS, IMC, etc.)
- Rapporteur de la thèse de Rafaelle Noro sur le sujet : « Synchronization over packet-switching networks: theory and applications ». Thèse de l'EPFL (Ecole Polytechnique Fédérale de Lausanne), 12 mai 2000
- Examinateur au jury de thèse de Vijay Arya sur le sujet « Congestion inference and traffic engineering in networks », thèse de l'Université de Nice, 5 juillet 2005
- Rapporteur et membre du jury de la thèse de Remco Van de Meent sur le sujet : « Network Link Dimensioning – A measurement & modeling based approach », Thèse de l'Université de Twente, Pays-Bas, 24 mars 2006

- Rapporteur et membre du jury de thèse de Karl-Johan Grinnemo sur le sujet « Transport Level Service for Soft Real-Time Applications in IP Networks », Thèse de l'Université de Karlstad, Suède, 1er juin 2006

2. Liste des publications

2.1. Revues

[1] M. Diaz, **P. Owezarski**, "From multimedia models to multimedia protocols", in Computer Networks and ISDN Systems, n° 29, pp 745-758, 1997

[2] **P. Owezarski**, V. Baudin, M. Diaz, "Conception et développement d'un système synchrone de téléformation professionnelle", Calculateurs Parallèles, Numéro thématique sur la coopération, Vol. 9, n°2, pp 209-238, juin 1997

[3] **P. Owezarski**, M. Diaz, C. Chassot, "A Time Efficient Architecture for Multimedia Applications", IEEE Journal on Selected Areas in Communications, special issue on Protocols Architectures for 21st Century Applications, vol. 16, No. 3, April 1998

[4] **P. Owezarski**, M. Diaz, "Conception et implémentation d'applications multimédias en Solaris 2", Calculateurs Parallèles, Numéro thématique "librairies de threads et applications parallèles ou distribuées, Vol. 10, n°3, pp 311-331, juillet 1998

[5] **P. Owezarski**, M. Diaz, "New formal architecture for enforcing multimedia synchronisation in videoconferencing applications", Telecommunication System Journal, Vol. 11, N° 1-2, pp 161-185, January 1999

[6] M. Diaz, **P. Owezarski**, "Protocols and Networks", Network and Information Systems journal (NIS), Vol. 3, n° 1, 2000

[7] P. Berthou, T. Gayraud, **P. Owezarski**, M. Diaz, "Multimedia Multi-Networking: a New Concept", Annales des Télécommunications / Annals of Telecommunications, Tome 57, N° 7-8, Juillet-Août 2002

[8] **P. Owezarski**, N. Larrieu, "Coherent charging of differentiated services in the Internet depending on congestion control aggressiveness", Computer Communication Journal, Vol. 26, issue 13, August 2003

[9] C. Barakat, P. Thiran, G. Iannaccone, C. Diot, **P. Owezarski**, "Modeling Internet backbone traffic at the flow level", IEEE transactions on signal processing, Vol. 51, N° 8, August 2003

[10] N. Larrieu, **P. Owezarski**, "De la métrologie pour l'ingénierie des réseaux de l'Internet", numéro spécial "Réseaux et protocoles", Techniques et Sciences Informatiques (TSI), vol. 23, n°5-6, septembre 2004

[11] N. Larrieu, **P. Owezarski**, "Towards a measurement based networking approach for Internet QoS improvement", Computer Communications, Vol.28, Issue 3, February 2005

[12] **P. Owezarski**, N. Larrieu, L. Bernaille, W. Saddi, F. Guillemin, A. Soule, K. Salamatian, "Distribution of traffic among applications as measured in the French METROPOLIS project", to appear in Annals of Telecommunications Special issue on Analysis of traffic and usage traces on the Internet - From network engineering to sociology of uses, 2006

[13] **P. Owezarski**, N. Larrieu, "Techniques et outils de métrologie pour l'Internet et son trafic", à paraître dans Techniques pour l'ingénieur, 2006

[14] A. Scherrer, N. Larrieu, **P. Owezarski**, P. Borgnat, P. Abry, "Non Gaussian and long memory statistical characterization for Internet traffic with anomalies", à paraître dans IEEE Transactions on Dependable and Secure Computing

2.2. Communications dans des congrès à comité de lecture avec publication des actes

[15] **P. Owezarski**, M. Diaz, P. Sénac, "Modélisation et implémentation de mécanismes de synchronisation multimédia dans une application de visioconférence", Actes du colloque francophone sur l'ingénierie des protocoles (CFIP'95), pp 305-319, éditions Hermès, Rennes, France, 10-12 mai 1995

[16] **P. Owezarski**, V. Baudin, M. Diaz, J.F. Schmidt, "Multimédia Teleteaching: Introduction of Synchronization and Cooperation Mechanisms in Distance Learning", Proceedings of the world conference on educational multimedia and hypermedia (ED'MEDIA 95), pp 517-522, Graz, Austria, May 17-21, 1995

[17] V. Baudin, **P. Owezarski**, M. Diaz, "Projet CESAME : conception formelle de systèmes multimédias coopératifs à hauts débits", Actes des journées réseaux (JRES'95), pp 37-44, Chambéry, France, 22-24 novembre 1995

[18] **P. Owezarski**, T. Villemur, M. Diaz, "Conception d'un système de visioconférence coopératif", Actes des 8ème rencontres francophones sur le parallélisme (RenPar'8), pages 25-28, Bordeaux, France, 20-24 Mai 1996

[19] **P. Owezarski**, T. Villemur, M. Diaz, "Conception et implémentation d'un système de visioconférence coopératif à N intervenants", Actes des journées de recherche sur le contrôle réparti dans les applications coopératives (CRAC'96), pages 87-92, Paris, France, 30-31 Mai 1996

[20] V. Baudin, M. Diaz, **P. Owezarski**, T. Villemur, "Design and realization of a synchronous cooperative shared electronic board", proceedings of the Advanced Technology Workshop (ATW'96), Toulouse, France, July 8-10, 1996

[21] **P. Owezarski**, M. Diaz, "Models for enforcing multimedia synchronization in visioconference applications", proceedings of the 3rd MultiMedia Modeling conference – Towards the information superhighway (MMM'96), pp 85-100, World scientific editor, Toulouse, France, November 12-15, 1996

[22] **P. Owezarski**, M. Diaz, "Multimedia Synchronization Issues in Visioconference Applications", 3rd CABERNET plenary workshop, Rennes, France, April 16-18th, 1997

[23] **P. Owezarski**, D. Wartelle, P. Perrot, G. Ségarra, S. Guillouet, K. Drira, A. Meftah, M. Diaz, "Assessment methodology of new technologies for collaborative automotive design", 2nd International distributed conference on network interoperability, Madeira, Portugal, June 16-18th, 1997

[24] **P. Owezarski**, M. Diaz, "Hierarchy of time streams Petri nets models in generic videoconferences",1st International workshop on multimedia and concurrency, pp 58-72, Toulouse, France, June 24th, 1997

[25] **P. Owezarski**, M. Boyer, M. Diaz, "Renégociation dynamique de qualité de service dans une application de visioconférence synchronisée", colloque francophone sur l'ingénierie des protocoles (CFIP'97), Liège, Belgique, 29 septembre - 2 octobre, 1997

[26] M. Boyer, **P. Owezarski**, M. Diaz, " Dynamic QoS renegociation in the PNSVS videoconferencing application", International conference on Interactive Distributed Multimedia Systems (IDMS'98), Oslo, Norway, September 8 - 11th, 1998

[27] T. Villemur, **P. Owezarski**, M. Diaz, "N-TSVS: A videoconferencing tool for generic cooperative groups", Proceedings of the 5th MultiMedia Modelling Conference (MMM'98), pp 102-111, Lausanne, Switzerland, October 12-15th, 1998

[28] V. Baudin, S. Owezarski, J.L. Cames, T. Villemur, **P. Owezarski**, M. Diaz, J.F. Schmidt, « Conception d"un environnement de télé-formation synchrone – Projet TOPASE », 1ère Conférence scientifique sur les Nouvelles Technologies de l'Information et de la Communication dans la Formation d'ingénieurs et dans l'Industrie (NTICF'98), pp 53-64, Rouen, France, 18-20 Novembre 1998

[29] P. Berthou, T. Gayraud, **P. Owezarski**, M. Diaz, "Partial Ordered and reliable multimedia transport protocol for satellite communications", 5th European Conference on Satellite Communications (ECSC 5), Toulouse, France, 3 – 5 November, 1999

[30] **P. Owezarski**, "La télé-ingénierie coopérative : principes et exemples", Actes des journées réseau (JRES'99), pp 151 – 159, Montpellier, France, 29 novembre – 3 décembre 1999

[31] **P. Owezarski**, V. Baudin, S. Owezarski, G. Fabre, T. Gayraud, J-M. Dorkel, P. Tounsi, "New methodology of work with concurrent engineering in electronic design", Proceedings of the symposium on Design, Test, Integration and Packaging of MEMS/MOEMS, SPIE editions, Paris, France, May 9 – 11th, 2000

[32] T. Gayraud, **P. Owezarski**, P. Berthou, M. Diaz, "M3POC : A Multimedia Multicast Transport Protocol for Cooperative Applications", Proceedings of the International Conference on Multimedia and Expo 2000 (ICME'2000), New-York City, USA, July 31st – August, 2000

[33] P. Berthou, T. Gayraud, **P. Owezarski**, M. Diaz, "Protocoles de communication multimédia multi-réseaux : un nouveau concept", Actes du 8ème Colloque Francophone sur l'Ingénierie des Protocoles (CFIP'2000), Toulouse, France, 17-20 octobre 2000

[34] **P. Owezarski**, "Enforcing multipoint multimedia synchronization in videoconferencing applications", Proceedings of the International conference on Interactive Distributed Multimedia Systems and telecommunication services (IDMS'2000), in Lecture Notes in Computer Science 1905, Enschede, The Netherlands, October 17th – 20th, 2000

[35] C. Fraleigh, C. Diot, S. Moon, **P. Owezarski**, D. Papagiannaki, F. Tobagi, "Experiences Monitoring Backbone IP Networks", Workshop on Passive and Active Measurements (PAM'2001), Amsterdam, The Netherlands, April 23-24, 2001

[36] C. Fraleigh, F. Tobagi, C. Diot, B. Lyles, S. Moon, D. Papagiannaki, **P. Owezarski**, "Design and Deployment of a Passive Monitoring Infrastructure", 2001 Tyrrhenian International Workshop on Digital Communication (IWDC'2001) – Evolutionary Trends of the Internet – LNCS 2170, Sergio Palazzo (Ed.), Taormina, Italy, September 17th – 20th, 2001

[37] **P. Owezarski**, "Is IPv6 Really Scalable ? A Theoretical Comparison Between IPv6 and IPv4+NAT Based on some IPv4 Links and Routers Monitoring", Proceedings of the Conference on Deploying IPv6 Networks, Paris, France, November 20th – 23rd, 2001

[38] **P. Owezarski**, "Que nous dit la métrologie sur le futur d'Internet ?", 4ème Journées Réseaux (JRES'2001), Lyon, France, 10 – 14 Décembre 2001

[39] V. Baudin, V. Royo, **P. Owezarski**, T. Gayraud, S. Owezarski, "Une Visioconférence sur réseau IP", 4ème Journées Réseaux (JRES'2001), Lyon, France, 10 – 14 Décembre 2001

[40] **P. Owezarski**, C. Martinie "Une nouvelle architecture pour la différenciation de services dans l'Internet basée sur le contrôle de congestion", Actes du 9ème Colloque Francophone sur l'Ingénierie des Protocoles (CFIP'2002), Montréal, Canada, 27-30 mai 2002

[41] C. Barakat, P. Thiran, G. Iannaccone, C. Diot, **P. Owezarski**, "A flow model for Internet backbone traffic", 2nd SIGCOMM Internet Measurement Workshop (IMW'2002), Marseille, France, November 6-8th, 2002

[42] **P. Owezarski**, "Does IPv6 improve the scalability of the Internet ?", Joint Internal Workshops on Interactive Distributed Multimedia Systems and Protocols for Multimedia Systems (IDMS/PROMS'2002), Coimbra, Portugal, November 26-29th, 2002

[43] N. Larrieu, **P. Owezarski**, "Un modèle de tarification du trafic Internet basé sur le contrôle de congestion", Colloque de l'école doctorale Informatique et Télécommunications (EDIT'2003), Toulouse, France, 14-15 avril 2003

[44] P. Olivier, **P. Owezarski**, K. Salamatian, "Quelques éléments caractéristiques du trafic Internet" Colloque International "Mesures de l'Internet", Nice, France, 12-14 mai 2003

[45] **P. Owezarski**, "Métrologie des réseaux de l'Internet : principales actions et impact sur les évolutions technologiques", Colloque International "Mesures de l'Internet", Nice, France, 12-14 mai 2003

[46] **P. Owezarski**, "Métrologie des réseaux de l'Internet et analyse des attaques", 2nde rencontres francophones sur le thème Sécurité et Architecture Réseaux (SAR'2003), Nancy, France, 30 juin - 4 juillet 2003

[47] N. Larrieu, **P. Owezarski**, "TFRC contribution to Internet QoS improvement", Proceedings of the fourth COST 263 international workshop on Quality of Future Internet Services (QoFIS'2003), Stockholm, Sweden, 1 - 3, October 2003

[48] N. Larrieu, **P. Owezarski**, "Une extension du modèle de tarification « smart market » pour l'Internet basé sur le contrôle de congestion", Actes du Colloque Francophone sur l'Ingénierie des Protocoles (CFIP'2003), Paris, France, 7-10 Octobre 2003

[49] **P. Owezarski**, N. Larrieu, "A trace based method for realistic simulation", IEEE International Conference on Communication (ICC'2004), Paris, France, 20-24 June, 2004

[50] **P. Owezarski**, N. Larrieu, "Internet traffic characterization – An analysis of traffic oscillations", IEEE International Conference on High Speed Networks and Multimedia Communications (HSNMC'2004), Toulouse, France, June 30th – July 2nd, 2004

[51] **P. Owezarski**, N. Larrieu, "Measurement Tools and Techniques for traffic and QoS management", International Mediterranean Modeling Multiconference / Integrated Modeling & Analysis in Applied Control & Automation (I3M/IMAACA, 2004), Genoa, Italy, 28-31 October, 2004

[52] N. Larrieu, **P. Owezarski**, "Contrôle de congestion orienté mesures pour l'Internet", 6èmes Journées Doctorales Informatique et Réseau (JDIR'04), Lannion (France), 2-4 Novembre 2004

[53] N. Larrieu, **P. Owezarski**, "Contrôle de congestion et gestion du trafic à partir de mesures", 11ème Colloque Francophone sur l'Ingénierie des Protocoles (CFIP'2005), Bordeaux (France), 29 Mars - 1er Avril 2005

[54] Y. Labit, **P. Owezarski**, N. Larrieu, "Evaluation of active measurement tools for bandwidth estimation in real environment", 3rd IEEE/IFIP Workshop on End-to-End Monitoring Techniques and Services (E2EMON'05), Nice (France), 15 Mai 2005

[55] N. Larrieu, **P. Owezarski**, "Measurement based networking approach applied to congestion control in the multi-domain Internet", 9th IFIP/IEEE International Symposium on Integrated Network Management (IM'2005), Nice, France, 15-19 May 2005

[56] **P. Owezarski**, N. Larrieu, "Un mécanisme de contrôle de congestion orienté mesures pour une QdS robuste dans l'Internet", 4th Conference on Security and Network Architectures (SAR'2005), Batz sur Mer (France), 6 - 10 Juin 2005

[57] S. Farraposo, K. Boudaoud, L. Gallon, **P. Owezarski**, "Some issues raised by DoS attacks and the TCP/IP suite", 4th Conference on Security and Network Architectures (SAR'2005), Batz sur Mer (France), 6 - 10 Juin 2005

[58] S. Farraposo, **P. Owezarski**, E. Monteiro, "On the use of traffic monitoring and measurements for improving networking", Conference on Service Assurance with Partial and Intermittent Resources (SAPIR'2005), Lisbon, Portugal, 17-21 July, 2005

[59] P. Borgnat, N. Larrieu, P. Abry, **P. Owezarski**, "Décision d'attaques de déni de Service : ruptures dans les statistiques du trafic", 20ème colloque GRETSI sur le traitement du signal et des images, Louvain-la-Neuve, Belgique, 6-9 Septembre 2005

[60] N. Larrieu, Y. Zhang, **P. Owezarski**, "Caractérisation et analyse du trafic Internet en fonction du type d'application", 20ème colloque GRETSI sur le traitement du signal et des images, Louvain-la-Neuve, Belgique, 6-9 Septembre 2005

[61] **P. Owezarski**, "On the impact of DoS attacks on Internet traffic characteristics and QoS", 14th IEEE International Conference and Computer Communications and Networks (ICCCN'2005), San Diego, CA, USA, 17-19 October 2005

[62] Antoine Scherrer, Nicolas Larrieu, Pierre Borgnat, **Philippe Owezarski**, Patrice Abry, "Non Gaussian and Long Memory Statistical Modeling of Internet Traffic", 4th International Workshop on Internet Performance, Simulation, Monitoring and Measurements (IPS-MoMe'2006), Salzburg, Austria, February 27-28, 2006

[63] S. Farraposo, **P. Owezarski**, E. Monteiro, "Contribution of anomalies detection and analysis on traffic engineering", Infocom'2006, Student Workshop, Barcelona, Spain, April 23-29, 2006

[64] S. Mota Gonzalez, B. Fontan, P. de Saqui-Sannes, T. Villemur, **P. Owezarski**, "Modélisation UML d'un protocole d'échange de clés dans un groupe sécurisé", Conférence sur les Nouvelles technologies pour la répartition (NOTERE'2006), Toulouse, France, 6 – 9 Mai 2006

[65] A; Scherrer, N. Larrieu, **P. Owezarski**, P. Borgnat, P. Abry, "Une caractérisation non gaussienne et à longue mémoire du trafic Internet et de ses anomalies", Conférence Sécurité et Architectures Réseaux (SAR'2006), Seignosse, France, 6-9 mai 2006

[66] M. Dabrowski, **P. Owezarski**, W. Burakowski, A. Beben, "Overview of monitoring and measurement system in EuQoS multi-domain network", International Conference on Telecommunications and Multimedia (TEMU'06), Heraklion, Crete, Greece, 5-7 July 2006

2.3. Contributions à des ouvrages collectifs

[67] **P. Owezarski**, C. Chassot, "La couche Transport – services et protocoles – et ses évolutions", dans "Logiciel et Réseaux de Communication : compte rendu du groupe Logiciels et Réseaux de Communication de l'OFTA (Observatoire Français des Techniques Avancées)", ARAGO N° 23, éditions Lavoisier, Mai 2000

[68] **P. Owezarski**, M. Boyer, "Modélisation d'architectures Multimédias : le cas de la visioconférence à QoS garantie", dans ":Vérification et mise en œuvre des Réseaux de Petri", sous la direction de Michel Diaz, Editions Hermés, janvier 2003

[69] M. Boyer, C. Chassot, L. Dairaine, M. Diaz, A. Lozes, **P. Owezarski**, L.M. Rojas, "Protocoles de transport multimédias", dans "Systèmes multimédias communicants", Sous la direction de Walid Dabbous, Editions Hermés, juin 2001

[70] **P. Owezarski**, N. Larrieu, "Métrologie des réseaux de l'Internet", A paraître, « Sciences humaines et sociales et Technologies de l'Information et de la Communication »**,** Claire Brossaud, Bernard Reber**, ed.,** nouvelle collection TIC, sciences cognitives et SHS**,** Hermes, 2006

2.4. Textes de vulgarisation

[71] **P. Owezarski**, « Le projet CANET (Collaborative Automotive NETwork) : Utilisation des nouvelles technologies de l'information pour la conception coopérative dans le domaine de l'automobile », Lettre du LAAS N° 20, Décembre 1998

[72] **P. Owezarski**, D. Barthe, « Le projet MIRIHADE », Lettre du LAAS N° 21, Mars 1999

[73] **P. Owezarski**, "La parole à Philippe Owezarski, chargé de recherche au CNRS", Lettre du LAAS N°26, Mai 2001

[74] **P. Owezarski**, "Le projet QoS IP 3/4", Lettre HEMERA, 2002

2.5. Mémoires ayant permis de soutenir des diplômes

[75] **P. Owezarski**, "Etude et Spécification de Systèmes de Communications de Groupes pour les Applications Coopératives", rapport de stage de DEA Interface Homme-Système MultiModale (IHS2M), Université Paul Sabatier, Juin 1993

[76] **P. Owezarski**, "Conception et formalisation d'une application de visioconférence coopérative. Application et extension pour la téléformation", Thèse de doctorat de l'Université Paul sabatier Toulouse III, Décembre 1996

2.6. Tutoriels

[77] **P. Owezarski**, "Modélisation, conception et implémentation de mécanismes de gestion des contraintes temps-réel dans les applications multimédias", Ecole d'été temps-réel'97 - Applications, réseaux et systèmes, Poitiers, France, 22-26 septembre 1997

[78] **P. Owezarski**, "Le temps dans les réseaux longues distances", Ecole d'été temps-réel'99 – Applications, réseaux et systèmes, Poitiers, France, 13-16 septembre 1999
[79] C. Diot, **P. Owezarski**, "Internet Traffic Analysis: Monitoring the Sprint IP backbone", Ecole d'été du groupe RHDM (Réseaux Hauts Débits Multimédias) du GDR ARP, Calcatoggio, Corse, 6-12 mai 2001

[80] **P. Owezarski**, "What does IP monitoring tell about the future of the Internet", Journées Doctorales en Informatique et Réseaux (JDIR'2002), Toulouse, France, 4 mars 2002

[81] **P. Owezarski**, "Métrologie des réseaux IP : application à la sécurité et à l'amélioration de la qualité de service des réseaux", Sécurité et Architectures Réseaux (SAR'2002), Marrakech, Maroc, 8-12 juillet 2002

[82] **P. Owezarski**, "IP Network Monitoring and Measurements: Techniques and Experiences", Joint Internal Workshops on Interactive Distributed Multimedia Systems and

Protocols for Multimedia Systems (IDMS/PROMS'2002), Coimbra, Portugal, November 26-29th, 2002
[83] **P. Owezarski**, "IP Network Monitoring and Measurements: Techniques and Experiences", ECOTEL'2002, Golfe-Juan, France, 2-6 Décembre 2002

[84] **P. Owezarski**, N. Larrieu, "Trace based simulation", Ecole d'été du groupe Internet Nouvelle Génération (ING'2003) du GDR ARP, Porquerolle, France, 26-30 mai 2003

[85] **P. Owezarski**, "Métrologie de la QoS Internet", Ecole d'été temps-réel'2003, Toulouse, France, 9-12 septembre 2003

[86] **P. Owezarski**, B. Parreaux, "Métrologie Internet : Techniques, Expériences et Applications", 11ème Colloque Francophone sur l'Ingénierie des Protocoles (CFIP'2005), Bordeaux (France), 29 Mars 2005

2.7. Rapports de contrats

[87] M. Diaz, **P. Owezarski**, T. Villemur, "Une Définition Logique de la Coopération Basée sur le Partage des Données", Projet CESAME. Rapport du marché CNET France Télécom 92 1B 178 - Lot 3. Rapport interne LAAS no. 94008, 19 pages, Janvier 1994

[88] D. Wartelle, G. Ségarra, S. Guillouet, K. Drira, **P. Owezarski**, P. Perrot, "Definition of business scenarios and assessment methodology", CANET project, Deliverable 1 of the ESPRIT / HPCN EP 22528 Project, 66 pages, January 1997

[89] **P. Owezarski**, C. Chassot, M. Fournier, "Etude des besoins en communication pour un environnement de téléformation synchrone", Projet TOPASE, rapport du projet No 3464 du MENESRIP, Tâche 3 - Lot 2b, 34 pages, Février 1997

[90] P. Perrot, D. Wartelle, **P. Owezarski**, G. Ségarra, "CANET : First Periodic Progress Report", periodic report of the ESPRIT / HPCN EP 22528 Project, 36 pages, March 1997

[91] **P. Owezarski**, S. Guillouet, "Application platform", CANET project, Deliverable 2 of the ESPRIT / HPCN EP 22528 Project, 31 pages, September 1997

[92] P. Perrot, A. Meftah, **P. Owezarski**, "Report on the network deployment", CANET project, Deliverable 3 of the ESPRIT / HPCN EP 22528 Project, 86 pages, September 1997

[93] P. Perrot, D. Wartelle, G. Ségarra, **P. Owezarski**, G. Muinelo, "CANET : Second Periodic Progress Report", periodic report of the ESPRIT / HPCN EP 22528 Project, 36 pages, September 1997

[94] **P. Owezarski**, V. Roca, P. Cipière, S. Fdida, M. Diaz, C. Diot, "Protocoles multimédias haut débit et expérimentations sur MIRIHADE", Rapport du projet CNRS MIRIHADE, Mars 1998

[95] T. Villemur, **P. Owezarski**, M. Diaz, "Conception et implantation d'une application de vidéoconférence basée sur des groupes coopératifs génériques et structurés", Projet TOPASE, rapport du projet No 3464 du MENESRIP, Tâche 3 - Lot 1a, 24 pages, Avril 1998

[96] **P. Owezarski**, "Evaluation de logiciels de travail coopératif pour la télé-conception automobile", rapport du contrat Renault : LAAS 96/402, 39 pages, Mai 1998

[97] S. Letailleur, D. Wartelle, P. Perrot, **P. Owezarski**, K. Drira, "Trials synthesis", CANET project, Deliverable 4 of the ESPRIT / HPCN EP 22528 Project, 26 pages, May 1998

[98] G. Ségarra, D. Wartelle, P. Perrot, M. Diaz, **P. Owezarski**, "Users exploitation plan", CANET project, Deliverable 5 of the ESPRIT / HPCN EP 22528 Project, 28 pages, May 1998

[99] P. Perrot, D. Wartelle, G. Ségarra, S. Letailleur, **P. Owezarski**, M. Diaz, G. Muinelo, "CANET : Third Periodic Progress Report" periodic report of the ESPRIT / HPCN EP 22528 Project, 19 pages, May 1998

[100] P. Perrot, D. Wartelle, G. Ségarra, S. Letailleur, **P. Owezarski**, M. Diaz, G. Muinelo, "CANET final report", final report of the ESPRIT / HPCN EP 22528 project, 26 pages, May 1998

[101] **P. Owezarski**, V. Roca, O. Fourmaux, S. Fdida, M. Diaz, « Protocoles hauts débits et applications multimédias coopératives distribuées : bilan des expérimentations sur SAFIR », Rapport du projet SAFIR, 24 pages, février 1999

[102] M. Diaz, D. Hutchison, D. Larrabeiti, **P. Owezarski**, "Specification of the experimental platform" Deliverable of the GCAP project, Project IST-1999-10 504, February 2001

[103] **P. Owezarski**, V. Baudin, J.L. Sanchez, A. Martinez, "Bilan du projet plate-forme de télé-ingénierie coopérative", rapport du projet région « plate-forme de télé-ingénierie coopérative » Avril 2001

[104] H. Postec, **P. Owezarski**, L.Dairaine, "Services & applications d'un système IP Multicast par satellite", rapport du projet RNRT DIPCAST, juin 2001

[105] P. Berthou, T. Gayraud, **P. Owezarski**, L. Plateaux, M. Diaz, D. Gentil, "Specification of the MC MM Multinetwork Protocol", Deliverable of the GCAP project, Project IST-1999-10 504, June 2001

[106] C. Bennassy, F. Zwolska, L. Dairaine, C. Fraboul, H. Postec, **P. Owezarski**, "STB de la Plate-Forme Logicielle", Rapport du projet RNRT DIPCAST, Septembre 2001

[107] **P. Owezarski**, "Le projet QoSIP 3/4 : Bilan et prospective", Rapport intermédiaire de l'ACI jeunes chercheurs JemSTIC du CNRS – projet QOS IP 3/4, mai 2002

[108] H. Postec, **P. Owezarski**, L. Dairaine, L. Lancerica, F. De Belleville, "Besoins en termes de mesures et sondes sur le système DIPCAST", Rapport de projet RNRT DIPCAST, Septembre 2002

[109] **P. Owezarski**, D. Andreu, C. Fricker, K. Salamatian, C. Chekroun, N. Benameur, P. Olivier, J. Roberts, F. Guillemin, "Projet METROPOLIS. Sous-projet 1 : Rapport d'état de l'art", Rapport du projet RNRT METROPOLIS, janvier 2003

[110] V. Baudin, **P. Owezarski**, "Présentation et manuel d'utilisation de l'environnement de travail coopératif PLATINE", Rapport du projet RNRT DIPCAST, Avril 2003

[111] F. Loisel, **P. Owezarski**, "Résultats des mesures sur l'émulateur de niveau 3", Rapport du projet RNRT DIPCAST, août 2003

[112] F. Loisel, **P. Owezarski**, "Résultats des mesures sur l'émulateur de niveau 2", Rapport du projet RNRT DIPCAST, août 2003

[113] **P. Owezarski**, P. Abry, K. Salamatian, D. Kofman, A. Aussem, F. Guillemin, P. Robert, "Métrologie des réseaux de l'Internet", Rapport final de l'Action Spécifique du département STIC du CNRS #88, décembre 2003

[114] **P. Owezarski**, N. Larrieu, G. Yonnet, E. Da Costa, D. Andreu, F.X. Andreu, "METROPOLIS : Tarification et SLA", Rapport du projet RNRT METROPOLIS, Février 2004

[115] **P. Owezarski**, N. Larrieu, K. Salamatian, A. Soule, "METROPOLIS : Analyse du réseau", Rapport du projet RNRT METROPOLIS, Février 2004

[116] **P. Owezarski**, N. Larrieu, "METROPOLIS : Conception et mise en place de la plate-forme de mesures passives", Rapport du projet RNRT METROPOLIS, Février 2004

[117] Simões Paulo, Fernando Boavida, Jorge Sa Silva, Marc Brogle, Dragan Milic, Régis Fréchin, Pascal Le gern, Stéphane Statiotis, Zbigniew Kopertowski, Pablo Vaquero, Francisco Javier Ramón Salguero, Sathya Rao, Jordi Domingo-Pascual, René Serral-Gracià, Xavi Masip, **Philippe Owezarski**, Florin Racaru, Guillaume Auriol, Nicolas Larrieu, Michał Obuchowicz, Pawan Cabell, Robert Parzydło, Isabel Borges, Abraham Gebrehiwot, Marek Dabrowski, Jaroslaw Sliwinski, Andrzej Beben, Piotr Pyda, "Technical requirements for the trial, tasks and scheduling", Deliverable of the EuQoS project, funded by the EC under grant IST 004503, February 2005

[118] Régis Fréchin, Pascal Le Gern, Francisco Javier Ramón Salguero, Pedro A. Aranda Gutiérrez, **Philippe Owezarski**, Florin Racaru, Guillaume Auriol, Nicolas Larrieu, René Serral-Gracià, Jordi Domingo-Pascual, Carles Kishimoto, José Núñez, Marek Dabrowski, Jaroslaw Sliwinski, Marc Brogle, Dragan Milic (UoB), Zbigniew Kopertowski, Luís Cordeiro, Abraham Gebrehiwot, Marco Sommani, "Connectivity and performance tests report for local and pan-European (accross GEANT) testbed design for the trial", Deliverable of the EuQoS project, funded by the EC under grant IST 004503, February 2005

[119] Wojciech Burakowski, **Philippe Owezarski**, Nicolas Larrieu, Gerardo García, María Luisa García, René Serral, Jordi Domingo, Xavi Masip, Marek Dąbrowski, Andrzej Bęben, Piotr Pyda, Damian Duda, Halina Tarasiuk, Yannick Lizzi, Enrico Angori, Giuseppe Martufi, Regis Frechin, Maxwel Carmo, Jorge Sá Silva, Paulo Simões, "Definition of monitoring equipment and software and location points", Deliverable of the EuQoS project, funded by the EC under grant IST 004503, February 2005

[120] Régis Fréchin, Pascal Le Gern, Francisco Javier Ramón Salguero, Pedro A. Aranda Gutiérrez, **Philippe Owezarski**, Florin Racaru, Guillaume Auriol, Nicolas Larrieu, René Serral-Gracià, Jordi Domingo-Pascual, Carles Kishimoto, José Núñez, Marek Dabrowski,

Jaroslaw Sliwinski, Marc Brogle, Dragan Milic (UoB), Zbigniew Kopertowski, Luís Cordeiro, Abraham Gebrehiwot, Marco Sommani, "Connectivity and performance tests report for local and pan-European (accross GEANT) testbed design for the trial – Version 2", Deliverable of the EuQoS project, funded by the EC under grant IST 004503, March 2005

[121] S. Farraposo, L. Gallon, K. Boudaoud, **P. Owezarski**, "Network security and DoS attacks", Rapport du projet de l'ACI Sécurité & Informatique MétroSec, Avril 2005

[122] Wojciech Burakowski, Marcello Yannuzzi, Xavier Masip-Bruin, Rene Serral-Gracià, Jordi Domingo-Pascual, **Philippe Owezarski**, Nicolas Larrieu, Gerardo García de Blas, María Ángeles Callejo Rodríguez, Jorge Andrés Colás, Andrzej Beben, Marek Dąbrowski, Jarosław Śliwiński, Damian Duda, Piotr Krawiec, Giovanni Saccomandi, Federico Travaglini, "Developing the monitoring and measurement system", Deliverable of the EuQoS project, funded by the EC under grant IST 004503, July 2005

[123] M. Dabrowski, D. Milic, M. Brogle, J.B. Alvarez, H.D. Manaia, **P. Owezarski**, S.F. Racaru, R. Serral-Gracia, A. Pinizzotto, M. Carmo, C. Tomasz, K. Bonarski, "First individual based EuQoS system test report", Deliverable of the EuQoS project, funded by the EC under grant IST 004503, September 2005

[124] **P. Owezarski**, N. Larrieu, Y. Labit, Y. Zhang, K. Salamatian, A. Soule, L. Bernaille, T. Friedman, B. Donnet, F. Guillemin, W. Saddi, T. Chahed, R. Casellas, G. Urvoy-Keller, E. Biersack, P. Robert, C. Friecker, "METROPOLIS : Rapport final", Rapport du projet RNRT METROPOLIS, Septembre 2005

[125] F. Capello, **P. Owezarski**, R. Namyst, O. Richard, P. Vicat-Blanc-Primet, E. Jeannot, L.A. Estefanel, D. Caromel, P. Sens, P. Fraignaud, C. Cerin, S. Petiton, J. Gustedt, C. Blanchet, C. Randriamaro, S. Tixeuil, "Data Grid eXplorer", Rapport de contrat, projet ACI Masse de Données Data Grid eXplorer, Septembre 2005

[126] **P. Owezarski**, S.F. Racaru, M. Dabrowski, A. Beben, J. Sliwinski, D. Duda, R. Serral-Gracia, L. Jakab, J. Domingo-Pascual, G. Garcia de Blas, A. Gebrehiwot, K. Bonarski, M. Brogle, D. Milic, T. Ciszkowski, J. Kowalczyk, E.M. Silva, I. Borges, "Deploying the monitoring and measurement system in testbeds", Deliverable of the EuQoS project, funded by the EC under grant IST 004503, November 2005

[127] M. Salah Bouassida, N. Chridi, I. Chhrisment, B. Fontan, S. Mota Gonzalez, **P. Owezarski**, H. Ragab Hassan, P. De Saqui-Sannes, T. Villemur, "L2.5 – Spécification du système global, intégration des services de sécurité au protocole de gestion de clés", Rapport de contrat RNRT SAFECAST, Novembre 2005

2.8. Communications, Rapports de Recherche, Séminaires, revues électroniques

[128] M. Diaz, **P. Owezarski**, "Développement d'un système de visioconférence sur réseau local", Rapport LAAS No 94354, 33 pages, Juillet 1994

[129] **P. Owezarski**, T. Villemur, "Environnement de télé-formation : visioconférence synchronisée et tableau de dialogue", Journée Multimédia pour le club des affiliés du LAAS, LAAS-CNRS, Toulouse, 22 septembre 1995

[130] **P. Owezarski**, "Applications multimédias et autoroute de l'information : problématique", Conférence de recherche, Salon International des Technologies et Energies du Futur (SITEF'95), Toulouse, 24-27 octobre 1995

[131] **P. Owezarski**, M. Diaz, "Gestion de la synchronisation multimédia et de la qualité de service dans une application de visioconférence : mécanismes système et transport", Rapport LAAS No. 95460, 62 pages, Novembre 1995

[132] **P. Owezarski**, V. Baudin, M. Diaz, "Conception et développement d'un système synchrone de téléformation professionnelle", Actes des séminaires hypermédia, éducation et formation, Paris, France, 22 mars 1996

[133] V. Baudin, M. Diaz, **P. Owezarski**, "Extensions proposal for IconAuthor", Rapport LAAS N° 96288, 6 pages, Juillet 1996

[134] **P. Owezarski**, M. Diaz, "Models for enforcing multimedia synchronization and QoS in visioconference applications", LAAS report No 96287, 16 pages, July 1996

[135] **P. Owezarski**, V. Baudin, M. Diaz, "Conception et réalisation d'un environnement de téléformation synchrone", Rapport LAAS No 96285, 27 pages, Juillet 1996

[136] **P. Owezarski**, T. Villemur, M. Diaz, "Conception et implémentation d'un système de visioconférence coopératif", Rapport LAAS N° 96401, 35 pages, Août 1996

[137] **P. Owezarski**, M. Diaz, R. Noro, "Chapter 4: Synchronisation", COST 237 final report, LAAS Report N° 98099

[138] **P. Owezarski**, S. Guillouet, "CSCW applications in engineering environment" European workshop on concurrent engineering: trends and perspectives, Paris, March 12th, 1998

[139] **P. Owezarski**, M. Diaz, "From modelling to implementation of multimedia applications", Rapport LAAS N° 98152, 17 pages, Avril 1998

[140] T. Villemur, **P. owezarski**, M. Diaz, "Design and implementation of a videoconferencing application based on generic structured cooperative groups", Rapport LAAS N° 98221, Mai 1998

[141] **P. Owezarski**, "Introduction aux codages multimédias", Table ronde sur les nouvelles technologies du multimédia, Premier congrès annuel des anciens étudiants étrangers de Toulouse Midi-Pyrénées, Toulouse, France, 11-13 juin 1998

[142] **P. Owezarski**, "Validation de services et mise en place des outils coopératifs du projet CANET", Séminaire X-ARISTOTE sur "les nouvelles technologies de l'information et de la communication au service du travail coopératif, Ecole Polytechnique, Paris Palaiseau, France, 18 juin 1998

[143] **P. Owezarski**, J.M. Valentin, J.C. Arnu, "M3POC : un protocole de transport multicast multimédia pour les applications coopératives", Rapport LAAS N° 98358, 17 pages, Septembre 1998

[144] **P. Owezarski**, "M3POC: a multimedia multicast transport protocol for cooperative applications", Rapport LAAS N° 98424, 14 pages, Octobre 1998

[145] **P. Owezarski**, M. Boyer, M. Diaz, "Mécanismes de gestion et de renégociation de la qualité de service dans une application de visioconférence", Revue électronique sur les réseaux et l'informatique répartie (RERIR), http://www.univ-pau.fr/, Décembre 1998

[146] P. Berthou, **P. Owezarski**, T. Gayraud, M. Diaz, "Multimedia multi-networks transport protocol: a new concept", Rapport LAAS N° 99440, 15 pages, Octobre 1999

[147] **P. Owezarski**, "Nouvelles approches pour la garantie de la qualité de service dans les applications multimédias distribuées", Réunion du GDR STS (Systèmes Temporisés Stochastiques), Paris, France, 22 octobre 1999

[148] **P. Owezarski**, V. Baudin, "La télé-ingénierie coopérative: introduction et exemples", Rapport LAAS N°00318, Juillet 2000

[149] C. Diot, C. Fraleigh, B. Lyles, S. Moon, **P. Owezarski**, D. Papagiannaki, P. Thiran, F. Tobagi, "Internet Traffic Analysis: Monitoring the Sprint IP backbone", ITC Specialist Seminar, Monterey, CA, USA, September 2000

[150] **P. Owezarski**, "Internet QoS: myth or reality?" LAAS report N° 01061, February 2001

[151] **P. Owezarski**, "Few words on TCP flows analysis and traffic modeling", SPRINT IP Group retreat, Miami, Florida, USA, May 20th-22nd, 2001

[152] **P. Owezarski**, V. Baudin, T. Gayraud, V. Royo, "How to make multipoint videoconferencing over the european internet? ", Rapport LAAS N° 01233, Juin 2001

[153] C. Barakat, P. Thiran, G. Iannaccone , C. Diot, **P. Owezarski**, "A flow-based model for internet backbone traffic", Rapport LAAS N°01340, Août 2001

[154] **P. Owezarski**, C. Martinie, "Conception et simulation d'une architecture à différenciation de services alternative à Diffserv", Rapport LAAS N°01447, Octobre 2001

[155] **P. Owezarski**, "A new architecture for services differentiation based on congestion control", LAAS Report N° 02070, February 2002

[156] **P. Owezarski**, "Using congestion control aggressiveness for service differentiation in the Internet", LAAS Report N° 02208, April 2002

[157] **P. Owezarski**, "IP monitoring : requirements and applications", Séminaire commun au thème RHDM du GDR ARP et à l'antenne française ACM SIGOPS, Nantes, France, 25 Avril 2002

[158] **P. Owezarski**, "IP Monitoring, network security and QoS", Journée de séminaires de l'Action Spécifique "sécurité" du département STIC du CNRS, Paris, France, 15 mai 2002

[159] **P. Owezarski**, "Introduction à la métrologie – Présentation de l'Action Spécifique « Métrologie des réseaux de l'Internet » du département STIC", Réunion inter-GDR ARP/ISIS, Paris, France, 17 Octobre 2002
[160] **P. Owezarski**, "IP Network Monitoring and Measurements: Techniques and Experiences", 1ère journée du groupe de réflexion opérateurs réseaux français (FrnOG), Paris, France, 15 Novembre 2002

[161] **P. Owezarski**, N. Larrieu, "Where are we with Internet simulation – How traffic monitoring can help? " LAAS Report N° 02548, December 2002

[162] **P. Owezarski**, N. Larrieu, "Congestion control based pricing model and charging mechanisms for Internet traffic", LAAS Report N° 03183, April 2003

[163] **P. Owezarski**, N. Larrieu, "On the impact of TFRC on traffic characteristics", LAAS Report N° 03228, May 2003

[164] **P. Owezarski**, "Métrologie Internet : techniques et expériences", Séminaire de recherche à l'IUR de Mont-de-Marsan, équipe CSySEC, 12 novembre 2003

[165] **P. Owezarski**, "La métrologie à Sprint – les techniques et outils de métrologie – Résultats de caractérisation et modélisation du trafic Internet", Séminaire à France Télécom R&D Lannion, 3 décembre 2003

[166] N. Larrieu, **P. Owezarski**, "Measurement based congestion control for improving Internet QoS", LAAS Report N° 04219, May 2004

[167] **P. Owezarski**, N. Larrieu, "A new measurement based architecture for Internet networking", LAAS report N° 04261, May 2004

[168] **P. Owezarski**, "Internet trafic monitoring: A step forward in traffic control and management", 4ème journée du groupe de réflexion opérateurs réseaux français (FrnOG), Paris, France, 9 Septembre 2004

[169] S. Farraposo, E. Monteiro, **P. Owezarski**, "An overview of Internet traffic models and some related networking issues", LAAS report N° 04456, September 2004

[170] **P. Owezarski**, Y. Labit, N. Larrieu, "Evaluation of active measurement tools for available bandwidth estimation", LAAS report N° 04548, October 2004

[171] N. Larrieu, **P. Owezarski**, Y. Zhang, "Characterization and analysis of main Internet application traffic", LAAS report N° 04549, October 2004

[172] **P. Owezarski**, N. Larrieu, "Measurement based approach of congestion control for enforcing a robust QoS in the Internet", LAAS report N° 04722, December 2004

[173] K. Salamatian, S. D'Antonio, J. Domingo-Pascual, M. Esposito, M. Janic, N. Larrieu, I. Marsh, **P. Owezarski**, T. Zseby, "Internet measurements: state and some challenges", LAAS report N0 05008, January 2005

[174] **P. Owezarski**, "Long Range Dependence : A security metrics for DoS attacks detection in next generation Internet", LAAS Report N°05383, June 2005

[175] **P. Owezarski**, N. Larrieu, Y. Labit, "Real time reporting of measurements in the Internet", LAAS report N°05519, September 2005

[176] N. Larrieu, **P. Owezarski**, H. Martin-Deidier, P. Spiesser, "Présentation du logiciel ZOO", Rapport LAAS N°05579, Octobre 2005

[177] **P. Owezarski**, "Internet Traffic Modelling and Attacks Detection", Séminaire SSI Modélisation & Sécurité du CELAR, 8 – 9 Novembre 2005

[178] **P. Owezarski**, "Internet Traffic Modelling and Attacks Detection", E-NEXT seminar on Measuring and Modeling the Internet, Lauvain-la-Neuve, Belgique, 2 décembre 2005

[179] N. Larrieu, **P. Owezarski**, "Measurement Based Networking and congestion control in the multi-domain multi-networks Internet", LAAS report N°05676, December 2005

[180] **P. Owezarski**, A. Scherrer, N. Larrieu, P. Borgnat, P. Abry, "Internet traffic monitoring and analysis for improving QoS and security", Research seminar during the CNRS-WIDE meeting, Tokyo, Japa,, February 8th, 2006

[181] **P. Owezarski**, N. Larrieu, Y. Labit, "MRP : un protocole de « reporting » pour un système global de métrologie", Rapport LAAS N°06110, Février 2006

3. Activités pédagogiques **(encadrement, enseignement)**

3.1. Enseignement

J'ai assuré des enseignements en tant que vacataire à l'ENSICA, à l'UPS Toulouse III, à l'ENSAE, et à l'INSA Toulouse et des formations dans le cadre de la formation permanente pour l'association des AMI de l'ENSICA.

• Formation à la ***technique de description formelle ESTELLE*** : dernière année de l'IUP STRI (Systèmes de Télécommunication et Réseaux Informatiques) :
6 heures de cours, 8 heures de TD et 24 heures de TP (1996, 1997).

• Formation au ***langage C*** : année de formation spéciale en informatique de l'ENSICA :
7,5 heures de cours, 7,5 heures de TD, 5 heures de TP (de 1994 à 1998).

• Formation à la ***programmation temps réel*** : année de formation spéciale en informatique de l'ENSICA :
15 heures de cours, 7,5 heures de TD, 15 heures de TP (de 1994 à 1998).

• Formation à la ***programmation temps réel*** : dernière année de l'IUP STRI (Systèmes de Télécommunication et Réseaux Informatiques) :
6 heures de cours, 8 heures de TD, 6 heures de TP (1994, 1995).

• Formation à la ***programmation réseau et aux mécanismes de communication UNIX - conception d'applications distribuées*** : année de formation spéciale en informatique de l'ENSICA :
7,5 heures de cours, 30 heures de TP (1998, 1999).

• Formation à la ***programmation réseau : transmission de flux audio sur réseau local*** : 3ème année de cycle ingénieur de l'ENSAE :
2 heures de cours, 2 heures de TP (2000, 2001, 2002).

• ***A Tier-1 IP Backbone Network, Architecture, Performance*** : DESS STRI de l'Université Paul Sabatier, Toulouse III :
3 heures de cours (2002, 2003, 2004, 2005).

• ***What does IP monitoring tell about next generation Internet?*** : DESS STRI de l'Université Paul Sabatier, Toulouse III :
3 heures de cours (2002, 2003, 2004, 2005).

• ***Caractérisation de trafic et métrologie*** : 5ème année de cycle ingénieur de l'INSA, filière RT (Réseaux et Télécommunications)
7,5 heures de cours, 10 heures de TP (2004, 2005)

• ***Bureau d'étude sur l'ingénierie des réseaux*** : 5ème année de cycle ingénieur de l'INSA, filière RT (Réseaux et Télécommunications)
15 heures de TP (2004, 2005)

• Formation aux ***technologies multimédias*** dans le cadre de la formation permanente pour les AMI de l'ENSICA :
6 heures de cours (1995).

• Formation aux ***mécanismes de communication UNIX*** dans le cadre de la formation permanente pour les AMI de l'ENSICA :
30 heures de cours, TD, TP (1996).

• Encadrement d'un Projet d'Initiation à la Recherche (PIR) en 3ème année de cycle ingénieur de l'ENSAE sur le thème : « Diffusion de flux vidéo MPEG 2 (émission télévisée retransmises par satellite) sur le réseau local de l'école » :
10 heures d'encadrement (1999).

3.2. Encadrement

Avant même la fin de ma thèse, j'ai participé à l'encadrement de stages avec Michel Diaz. Au total, j'ai encadré ou participé à l'encadrement de 38 stages allant du stage de DUT au stage de DEA, en passant par les stages ingénieurs et les stages de DRT.

J'ai de plus reçu l'agrément, par l'INSA de Toulouse, pour diriger la thèse de Nicolas Larrieu. Nicolas Larrieu a obtenu le titre de docteur en informatique de l'INSA en juillet 2005. Dans le cadre d'une convention avec la DGA, il a étudié les problèmes de métrologie dans les réseaux de l'Internet et les a utilisé pour définir un mécanisme de contrôle de congestion et de gestion du trafic à partir de mesures pour l'optimisation de la QdS. A ce jour, il a écrit 6 articles de journaux [8, 10, 11, 12, 13, 14], 15 articles de conférence [43, 47, 48, 49, 50, 51, 52, 53, 54,

55, 56, 59, 60, 62, 65], une contribution à ouvrage [70], 9 rapports de contrats [114, 115, 116, 117, 118, 119, 120, 121, 124], et a contribué à un tutoriel [84].

Depuis mon arrivée au LAAS, j'ai donc pris en charge ou contribué à l'encadrement de divers étudiants en stage :

- "Développement d'un système de visioconférence en réseau local", dans le cadre d'un stage de fin d'études d'ingénieur ENSEEIHT, septembre 1993 – juin 1994.
  (David Naïm)

- "Visioconférence sur Numéris", dans le cadre d'un stage de fin d'études d'ingénieur ENSICA, mars – septembre 1994.
  (Christophe Beljouani)

- "Développement d'une application de visioconférence synchronisée", dans le cadre de la préparation d'un diplôme d'ingénieur CNAM, octobre 1994 – septembre 1995.
  (Eric Guillochin)

- "Intégration d'un protocole de transport à ordre partiel dans une application de transfert et de visualisation d'images JPEG", dans le cadre d'un stage de fin d'études de l'IUT, janvier – février 1996.
  (Jean-Christophe Arnu)

- "Intégration et évaluation d'un protocole à ordre partiel dans une application de transfert et d'affichage d'images JPEG", dans le cadre d'un stage de deuxième année de l'IUP ISI (Ingénierie des Systèmes Informatiques), avril – septembre 1996.
  (Laurent Rocher)

- "Renégociation de qualité de service dans une application de visioconférence : PNSVS", dans le cadre d'un stage de fin d'études d'ingénieur ENSEEIHT, septembre 1995 – juin 1996.
  (Marc Boyer)

- "Analyse de la synchronisation de l'application de visioconférence avec renégociation dynamique de QoS : PNSVS 2", dans le cadre d'un stage de DEA IFP (Informatique Fondamentale et Parallélisme), septembre 1995 – septembre 1996.
  (Marc Boyer)

- "Evaluation des performances et des fonctionnalités d'outils de CSCW sur un réseau ATM pour la télé-conception automobile", dans le cadre d'un stage de fin d'études d'ingénieur ENSEEIHT, septembre 1996 – juin 1997.
  (Laurent Ostiz)

- "Conception d'un protocole de diffusion de documents multimédias à connexion d'ordre partiel", dans le cadre d'un stage de DEA de l'INSA, mars – juillet 1997.
  (Romuald Gauvin)

- "Implémentation et mesures de performance d'applications multimédias en environnement ATM", dans le cadre d'un stage de fin d'étude d'ingénieur INSA, mars – juin 1997.
  (Nicolas Portenseigne)

- "Mesures de performances et développement d'applications sur réseau ATM en environnement hétérogène ", dans le cadre d'un stage de deuxième année de l'IUP ISI (Ingénierie des Systèmes Informatiques), mai – septembre 1997.
  (Jean-Christophe Arnu)

- "Etude de mécanismes de synchronisation multimédia en JAVA", dans le cadre d'un stage pendant une thèse de l'université de Versailles - Saint Quentin, avril – septembre 1997.
  (Karima Boudaoud)

- "Conception d'un protocole de transport multicast pour les applications multimédias et coopératives", dans le cadre d'un stage de fin d'étude d'ingénieur ENSEEIHT, septembre 1997 – juin 1998.
  (Jean-Michel Valentin)

- "Conception d'un protocole de transport multicast à ordre partiel pour la diffusion de flux multimédias", dans le cadre d'un stage de DEA IFP (Informatique Fondamentale et Parallélisme), septembre 1997 – août 1998.
  (Jean-Michel Valentin)

- "Développement d'un outil de visioconférence coopératif", dans le cadre d'un bureau d'étude de troisième année de l'IUP ISI (Ingénierie des Systèmes Informatiques), janvier – mars 1998.
  (Jean-Christophe Arnu et Laurent Navarro)

- "Garantie de la qualité de service dans une application multimédia coopérative synchrone. Exemple d'une application de visioconférence" dans le cadre d'un stage de fin d'études de l'IUP ISI (Ingénierie des Systèmes Informatiques), avril – septembre 1998.
  (Jean-Christophe Arnu)

- "Modélisation sous OPNET d'un protocole de transport multicast à ordre partiel pour la diffusion de flux multimédias", dans le cadre d'un stage de seconde année de l'IMERIR, juin – août 1998.
  (Philippe Limousy)

- "Etude de l'adéquation des protocoles IP et ATM sur Satellites : adaptation pour les applications de l'Internet et notion de Qualité de Service", Diplôme de Recherche et Technologie (DRT) en "Systèmes de Télécommunications et Réseaux Informatiques" (STRI) de l'université Paul Sabatier (Toulouse III), septembre 1997 – octobre 1999, Diplôme soutenu le 18 février 2000.
  (Frédéric Charles)

- "Garantie de la qualité de service dans une application de visioconférence synchrone et coopérative" dans le cadre d'un stage de DEA IFP (Informatique Fondamentale et Parallélisme), octobre 1998 – juin 1999.
  (Jean Christophe Arnu)

- "Multiplexeur de flux de données multimédias sur réseau ATM avec garantie de qualité de service", dans le cadre d'un stage de fin d'étude d'ingénieur ENSICA, Février – septembre 1999
  (Alexandre Bour)

- "Conception et Simulation d'une architecture à différenciation de services alternative à Diffserv", dans le cadre d'un stage de fin d'études d'ingénieur de l'EPF (Ecole Polytechnique Féminine), Avril – Août 2001
  (Célia Martinié)

- "Conception et Simulation d'une architecture à différenciation de services alternative à Diffserv", dans le cadre d'un stage de DEA de l'EDITE Paris (Ecole Doctorale en Informatique, Télécommunications et Gestion), Avril – Août 2001
  (Célia Martinié)

- "Métrologie des réseaux IP : Etude des pertes dans l'Internet", dans le cadre d'un stage de fin d'études ingénieur de l'ENSICA, Mars – Août 2001
  (Olivier Verlhac)

- "Métrologie des réseaux IP : Etude des pertes dans l'Internet", dans le cadre d'un stage de DEA Réseaux et Télécommunications, Mars – Août 2001
  (Olivier Verlhac)

- "Supervision active non intrusive dans le réseau Internet pour l'ingénierie coopérative", dans le cadre d'un stage de 2nde année de l'INSA, Juin – Août 2001
  (Nicolas Larrieu)

- "Métrologie des réseaux IP : développement de nouveaux outils pour caractériser, analyser et rejouer le trafic réseau", dans le cadre d'un stage de fin d'études de l'INSA Toulouse, Février – juin 2002
  (Nicolas Larrieu)

- "Métrologie des réseaux Internet : Caractérisation de la qualité de service, analyse et propositions d'optimisation", dans le cadre d'un stage de DEA Réseaux et Télécommunications, Février – Septembre 2002
  (Nicolas Larrieu)

- "De la métrologie à la simulation Internet – Analyse de la longue mémoire introduite par les routeurs", dans le cadre d'un stage de fin d'études de l'ENSICA et d'un DEA télécommunications et réseaux, Mars – Septembre 2002
  (Thomas Nozères)

- "Evaluation d'un service de communication multicast par satellite pour des applications multimédias interactives et distribuées", dans le cadre d'un stage de fin d'études de l'IUP STRI, Décembre 2002 – Mars 2003
  (Céline Danelon)

- "Métrologie dans les réseaux IP : Modélisation du trafic Internet", dans le cadre d'un stage de DEA « Systèmes Informatiques » de l'école doctorale Système (EDSYS), février – juin 2003
  (Nadhem Marsit)

- "Mesure et analyse des attaques et de leur impact sur les réseaux", dans le cadre d'un stage de DEA « Systèmes Informatiques » de l'école doctorale Système (EDSYS), février – juin 2003
  (Kaouther Blibech)

- "Evaluation d'un service de communication multicast par satellite multispots pour la télé-formation et la télé-ingénierie coopérative", dans le cadre d'un stage de fin d'étude ingénieur de l'école 3IL, mars août 2003
  (Fabien Loisel)

- "Métrologie active sur un réseau IP – Mesures non-intrusives da bande passante", dans le cadre d'un stage de 2nde année de l'INSA, Juin – Août 2003
  (Shizu Okada)

- "Développement d'un outil de métrologie pour la caractérisation du trafic Internet", dans le cadre d'un stage de 2nde année de l'INSA, Juin – Août 2003
  (Hubert Martin-Deidier)

- "Utilisation de la métrologie pour le réalisme des simulations", dans le cadre d'un stage de fin d'études de l'IUP STRI, Décembre 2003 – Mars 2004
  (Bertrand Pages)

- "Mesure de la qualité de service dans les réseaux IP par des techniques actives", dans le cadre d'un stage de DEA « Systèmes Informatiques » de l'école doctorale Système (EDSYS), février – juin 2004
  (Mohammed Gad el rab)

- "Métrologie dans les réseaux IP : caractérisation du trafic Internet", dans le cadre d'un stage de DEA Réseaux et Télécommunications, Février – Septembre 2004
  (Yu Zhang)

- "Emulation de sources de trafic", dans le cadre d'un stage de 2nde année de l'INSA, Juin – Août 2004
  (Julien Felizat)

- "Analyse des attaques et des failles de sécurité de l'Internet avec des outils de métrologie et des pots de miel", dans le cadre d'un stage de master 2 recherche de l'école doctorale Informatique (EDIT), Février – Septembre 2006
  (Ion Alberdi)

A l'heure actuelle, j'encadre ou co-encadre 2 doctorants :

- Silvia Farraposo dans le cadre d'une thèse en co-tutelle avec Edmundo Monteiro de l'Université de Coimbra au Portugal, et dans le cadre du réseau d'excellence européen E-NEXT. Silvia travaille sur le sujet : « IP monitoring and contribution to network

improvement ». En particulier, elle doit étudier les anomalies dans le trafic Internet pour définir de nouvelles politiques d'ingénierie des trafics à partir de mesures. Silvia a débuté sa thèse en Avril 2004 et a écrit trois publications dans des conférences [57, 58, 63] et un rapport de contrat [121].

- Yu Zhang (sous couvert de Michel Diaz) sur le sujet « Métrologie et ingénierie réseau pour la sécurité ». Cette thèse financée dans le cadre d'une convention avec la fondation EADS « envol recherche » a pour cadre le projet de l'ACI Sécurité & Informatique MétroSec. L'objectif est de trouver un moyen d'analyser en temps réel le trafic pour pouvoir classer ses anomalies en anomalies légitimes et attaques, notamment en étudiant les variations au niveau des propriétés spectrales du trafic. A partir de cette analyse qui doit expliquer comment les attaques de déni de service parviennent à leurs fins, l'objectif est de proposer de nouvelles architectures protocolaires pour l'Internet qui soient robustes aux attaques, i.e. qui continuent à fournir une QoS acceptable même en présence d'attaque. Yu a débuté sa thèse en octobre 2004 et a écrit un article pour une conférence [60] et un rapport de contrat [124].

J'encadre également depuis septembre 2004 Yann Labit, un jeune maître de conférences qui vient d'intégrer le groupe OLC et le thème APC. Sa recherche porte sur la conception d'outils de supervision du trafic et de mesure de la QoS, et sur l'analyse spectrale des anomalies dans le trafic Internet. Il a écrit un article de conférence depuis son arrivée dans l'équipe [54] et un rapport de contrat [121].

4. Projets de recherche contractuels

Depuis mon arrivée au LAAS, pour mon DEA puis ma thèse, puis ensuite lorsque j'ai été recruté en tant que chargé de recherche au CNRS, j'ai participé et eu à conduire (au moins pour la partie LAAS) de nombreux projets de recherche contractuels qui s'inscrivent directement dans ma thématique de recherche. La suite décrit sommairement tous ces projets auxquels j'ai au moins participé. Pour plus de détails sur les projets auxquels j'ai participé jusqu'en 1996, consulter mon mémoire de thèse [67]. Pour les autres, et notamment ceux postérieurs à 2000, ils seront décrits en détail dans ce manuscrit (partie 2 : Eléments de contribution).

• Projet CESAME (Conception formElle de Systèmes hAuts débits Multimédias coopEratifs) : 1993 – 1995.

- Collaboration CNET-CNRS-CCETT
- Formalisation, conception et développement de systèmes de visioconférence synchronisés et coopératifs, d'architectures et de mécanismes de synchronisation et de coopération.

• Projet TOPASE (Téléformation Avancée pour l'Aéronautique et l'Espace) : juin 1996 – décembre 1997

- Partenariat entre Airbus Training, l'ISSAT, le LAAS, l'IRISA, ARAMIIHS, Synelec et l'ENSICA.
- Conception et développement d'un environnement évaluable pour la téléformation multimédia synchrone en temps réel à la fois des utilisateurs d'images satellitaires et des personnels navigants et agents de maintenance des avions de la gamme Airbus.

• Projet CANET (Collaborative Automotive NETwork : projet européen ESPRIT / HPCN) : septembre 1996 – mars 1998.

- projet que je dirigeais pour le LAAS avec Renault SA, Siemens Automotive SA, France Télécom Expertel et le LAAS.
- Conception, expérimentation et évaluation d'outils de CSCW sur une plate-forme hétérogène (Sun, HP, SGI, PC) et sur réseau ATM pour la télé-conception automobile.
- Analyse et description formelle de scénarios de coopération génériques pour la conception distribuée constructeur / sous-traitant.

• Projet RENAULT : LAAS 96/402 : septembre 1996 – mai 1998

- Projet que je dirigeais et conduisais pour le LAAS.
- Evaluation d'outils de travail coopératif pour la télé-conception automobile. Etude demandée par Renault SA dans le cadre du déploiement de ces nouvelles technologies de l'information sur leur réseau privé REUNIR.

• Projet MIRIHADE (Multimédia Inforoutes et Réseaux Informatiques Hauts Débits) : juin 1996 – janvier 1997.

- Projet du CNRS (que je dirigeais pour le LAAS) sur le déploiement et l'évaluation d'un réseau ATM national pour les applications distribuées multimédias coopératives

• Projet SAFIR (Service ATM Fédérateur d'Interconnexion RENATER) : février 1998 – février 1999

- Projet RENATER (que je dirigeais pour le LAAS) sur la mise en œuvre, l'expérimentation et l'évaluation de nouveaux services, préfigurant le futur réseau de l'enseignement et de la recherche RENATER

• Projet SAFIR 2 : mars 1999 – septembre 1999

- Seconde phase du projet SAFIR

• Le projet Multimédia et micro-systèmes : projet LAAS + Région Midi-Pyrénées : 1999-2000

- Mise en place d'une plate-forme d'ingénierie coopérative pour la télé-conception électronique.

• Le projet DIPCAST : projet RNRT : Septembre 2000 - Août 2003

- Partenariat entre Alcatel, le CNES, le LAAS, l'INRIA, l'ENSEEIHT, l'ENSICA et CRIL (que je dirigeais pour le LAAS).
- Conception des mécanismes de communication multicast à QoS garantie pour l'Internet nouvelle génération sur réseau satellite.
- Evaluation du multicast satellite multispots avec des logiciels de visioconférence et de Vidéo à la demande sur un simulateur de réseau.

• Le projet GCAP : Projet du 5ème PCRD IST : Février 2000 - Janvier 2002)

- Partenariat entre le LAAS, le LIP6, Thomson Detexis, Alcatel Space (en France), les universités de Lancaster (Grande Bretagne), Darmstadt et Karlsruhe (Allemagne), Madrid (Espagne), Telebit (Luxembourg) et Telekom Austria (Autriche).

- Conception et développement d'un nouveau protocole de transport de bout en bout assurant une QoS garantie, avec des services multicast, multi-réseaux et déployable en utilisant le concept de réseaux actifs, pour l'Internet 2nde génération.
- Des applications de vidéo à la demande et de visioconférence ont servi à valider le protocole conçu sur une plate-forme de communication interconnectant tous les partenaires européens grâce aux réseaux nationaux de nouvelle génération pour la recherche (comme RENATER 2 en France par exemple) et TEN 155 au niveau européen.
- J'étais responsable du Work Package 4 sur les expérimentations.

• Le projet METROPOLIS : Projet RNRT : Septembre 2001 – Février 2005
- Partenariat entre le LAAS, le LIP6, France Télécom R&D Lannion, le GET, EURECOM, l'INRIA et RENATER (que je dirigeais pour le LAAS).
- Métrologie pour l'Internet et ses services.
- J'étais responsable de 2 sous-projets sur la conception et la mise en place de la plate-forme de mesure et l'analyse du réseau.

• Le projet IPQoS 3/4 : ACI (Action Concertée Incitative) jeunes chercheurs : Janvier 2002 – Décembre 2003
- Etude des lacunes des protocoles actuels de l'Internet pour garantir la Qualité de Service (QoS), conception de nouveaux protocoles de transport (niveau 4) avec de nouveaux mécanismes de contrôle de congestion et adéquation avec les mécanismes des routeurs (au niveau 3).

• Grid Explorer (GdX) : Projet de l'ACI « Masses de Données » : début en septembre 2003
- Définition et mise en place d'une plate-forme d'expérimentation pour les communautés de recherche françaises en réseau, Grid, calcul parallèle.
- Je suis responsable du projet au LAAS et porteur de deux tâches

• SAFECAST : projet du RNRT : début mai 2004
- Partenariat entre EADS télécom, le LAAS, l'ENST Paris, le LORIA, l'UTC
- Sécurité des Communications de groupes
- Je suis responsable du projet au LAAS

• E-NEXT : réseau d'excellence Européen, programme IST du 6ème PCRD : début janvier 2004
- Emerging Networking Experiments and Technologies
- Partenariat entre University Carlos III de Madrid, University Politécnica de Catalunya – CCABA, Telefónica I+D, University Politécnica de Madrid, Lancaster University, University of Cambridge, University College of London, University Pierre and Marie Curie (Paris 6), LAAS-CNRS, INRIA, Eurecom, University Liège, Université catholique de Louvain, University of Coimbra, Portugal Telecom Inovação, Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática, Delft University of Technology, University of Twente, University of Athens, University of Patras, Kungliga Tekniska Hogskolan, Swedish Institute of Computer Science, University of Napoli Federico II, Politecnico di Torino, University of Pisa, University of Trento, Fraunhofer Fokus, Technical University of Darmstadt, University Mannheim, Technische Universität Braunschweig, Helsinki University of Technology, Tampere University of Technology, Technical University of Denmark,

Telecommunications Research Center Vienna, University College Cork, ETH-Zurich, AGH University of Science and Technology, Universitet i Oslo, Budapest University of Technology and Economics, University of Cyprus, Reykjavik University

• EuQoS : Integrated Project du 6ème PCRD : début septembre 2004
  - End-to-end Quality of Service support over heterogeneous networks
  - Partenariat entre Telefonica I+D, University of Pisa, Datamat, ENSICA, LAAS, France Telecom R&D, Polska Telefonia Cyfrowa, Martel, NICTA, PointerCom, Polish Telecom R&D, Portugal Telecom Inovaçao, Red Zinc, Siemens SBS C-LAB, Silogic, Soluziona, Telscom, Technical University of Catalonia, University of Bern, University of Paderborn/C-LAB, University of Rome, University of Coimbra, Warsaw University of Technology, Ericsson, Hospital Divino Espiritu Santo

• MétroSec : projet de l'ACI Sécurité et Informatique : début Septembre 2004
  - Partenariat entre LAAS, LIP6, ENS Lyon, LIAFA, ESSI, IUT Mont-de-Marsan
  - Métrologie et sécurité pour la QoS
  - L'objectif du projet est de caractériser les attaques, et plus généralement les ruptures dans le trafic, de mettre en place des méthodes pour détecter ces ruptures, proposer des méthodes pour rendre le réseau insensible à ces ruptures (et qu'il puisse donc continuer à fournir de bonnes QoS même en cas d'attaques de DoS), et que dans le cas où l'on est sûr qu'une rupture est due à une attaque, pouvoir l'éliminer.
  - Je suis le responsable de ce projet

• STM : projet LAAS inter-groupes (RST et OLC) et inter-pôles (SINC et MOCOSY)
  - Sources de Trafic et Métrologie
  - Conception de méthodes et d'outils de génération de trafic à partir de modèles issus des analyses de traces de trafic capturées par des outils de métrologie.

• Contrat de financement d'une thèse (Yu Zhang) avec la fondation EADS envol recherche (Novembre 2004 – Octobre 2007)

• Partenariat entre le CNRS et WIDE au Japon : début janvier 2006
  - Recherches communes sur la métrologie et les réseaux sans fil

• OSCAR : labellisé par le RNRT. Début : avril 2006
  - Partenariat entre France Télécom R&D, Mitsubishi Electric, Miriad technologies, le LAAS, le LIP6, le GET, l'INRIA Sophia et Rocquencourt, l'ENS Lyon
  - Overlay network Security : Characterization, Analysis and Recovery
  - L'objectif du projet est d'étudier les faiblesses des réseaux superposés thématiques comme les réseaux de P2P, de voix sur IP ou de jeux, et leurs réactions face aux attaques venant de l'Internet. A partir de l'analyse des attaques et de leur impact – qui sera fait avec des outils de métrologie ainsi que des pots de miel – le projet vise à proposer des solutions pour défendre ces réseaux superposés et les rendre plus robustes, et ce à la fois au niveau du réseau overlay que du réseau d'infrastructure.

Seconde partie

Synthèse des travaux

1. Contexte de recherche et état de l'art

L'Internet est en train de devenir le réseau universel pour tous les types de données, du transfert simple de fichiers binaires jusqu'à la transmission de la voix, de la vidéo ou d'informations interactives en temps-réel. L'Internet se doit donc de fournir de nouveaux services adaptés à ses applications et aux données qu'elles transmettent. De plus, l'Internet croît très rapidement, en taille (nombre d'utilisateurs, d'ordinateurs connectés, etc.) et en complexité, en particulier à cause de la nécessité d'offrir de nouveaux services et d'optimiser l'utilisation des ressources de communication pour améliorer la QoS offerte aux utilisateurs. En effet, l'Internet doit évoluer d'une offre de service « best effort » unique vers une offre multi-services.

Au cours des dix dernières années, la QoS est apparue comme un enjeu majeur dans l'Internet. De nombreuses propositions faites dans la communauté Internet pour offrir des QoS différenciées et garanties n'ont pour l'heure pas complètement abouti et continuent à se heurter à de nombreuses difficultés. L'analyse de cet échec fait apparaître un certain nombre de difficultés toujours d'actualité : la complexité de l'Internet et ses nombreuses interconnexions, l'hétérogénéité de ses ressources en termes de technologies mais aussi de dimensionnement ou encore les caractéristiques de son trafic. En effet, l'augmentation de la complexité de l'Internet ainsi que les nouvelles applications aux besoins divers et évolutifs introduisent dans le trafic Internet de nombreuses caractéristiques qui sont très loin des croyances traditionnelles. En fait, les modèles basés sur des métriques simples comme le débit, le délai ou le taux de perte ne sont plus suffisants pour permettre une modélisation complète et précise des spécificités dynamiques observées dans le trafic Internet. La modélisation du trafic dans son ensemble est une tâche à réinventer. Les travaux les plus récents ont essayé de décrire la variabilité du trafic Internet, dont la dynamicité est à la base des difficultés rencontrées par les chercheurs et les ingénieurs réseaux pour mettre au point des techniques de garantie de la QoS. Ces travaux de modélisation sont parvenus à montrer que le trafic Internet est très loin des modèles simples Poissonniens et Markoviens utilisés dans le monde de la téléphonie, et que les modèles qui représentent mieux le trafic Internet sont des modèles ayant des propriétés d'auto-similarité ou de dépendance longue mémoire (LRD) [Pax 95]. La métrologie des réseaux de l'Internet - au sens littéral « la science des mesures » - doit permettre d'apporter une réponse à ces questions concernant le (ou les) modèle(s) de trafic de l'Internet qui font aujourd'hui défaut. En particulier, la méconnaissance du trafic Internet est vraisemblablement à la base des difficultés rencontrées pour la mise en œuvre de mécanismes de garantie de QoS, car il était alors impossible de confronter des solutions théoriques à des conditions réalistes de trafic.

L'évolution de l'Internet est ainsi étroitement liée à la connaissance et la compréhension des caractéristiques de son trafic car elles indiquent les types de mécanismes à déployer pour être en adéquation avec les besoins des utilisateurs et les contraintes réseaux. En conséquence, les domaines suivants doivent être approfondis : le développement d'outils basés sur la métrologie, de technologies permettant la collecte d'informations dans le trafic Internet ou encore de méthodes permettant l'analyse de ses caractéristiques. Leur utilisation permettra ainsi de faire des propositions en matière d'ingénierie et de recherche en réseau, en particulier, pour la définition et la quantification de la QoS dans l'Internet qui reste un problème ouvert.

Même si la métrologie de l'Internet n'est appliquée dans la recherche, l'ingénierie et la conception des réseaux Internet que depuis le début des années 2000, cette approche est de

plus en plus populaire et devrait tendre à se généraliser. L'étude, la caractérisation, l'analyse et la modélisation du trafic existant sur les liens de l'Internet doivent aider à comprendre les principes qui régissent le comportement du réseau par rapport à un trafic qui s'avère méconnu. C'est donc le processus de recherche et d'ingénierie des réseaux qui se trouve modifié par l'ajout d'une phase métrologique en amont permettant de collecter des données et des connaissances sur l'existant, pour permettre, ensuite, de concevoir et mettre en œuvre de nouvelles architectures protocolaires optimisées.
La nécessité d'effectuer des mesures et des analyses du trafic se justifie plus particulièrement par les besoins suivants :

- Evaluer la demande en trafic des utilisateurs, notamment dans le cadre de la fourniture à venir de classes de service différenciées (CoS).
- Dimensionner les ressources du réseau : capacité de traitement des routeurs ; débit de transmission des liens ; taille des buffers aux interfaces. Adapter la gestion opérationnelle de ces ressources à l'évolutivité temporelle de la demande en trafic. Ceci inclut en particulier tous les aspects en relation avec le routage dans le réseau.
- Contrôler la QoS offerte par le réseau : taux de perte de paquets, délai et gigue de transfert des paquets de bout en bout pour les applications à contraintes temps-réel, débit utile de transport des flux de trafic de données.
- Tester l'adéquation des modèles de performance élaborés au moyen de calculs analytiques ou de simulations, tant au niveau de la validation des hypothèses considérées que de la pertinence des résultats.

Finalement, la métrologie se trouve utilisée pour de très nombreuses fonctions dans les réseaux, dont une liste non exhaustive pourrait commencer par :

- mesure, mise en œuvre et gestion de la QoS
- gestion et administration des réseaux
- tarification et facturation
- contrôle de congestion et contrôle d'admission
- routage
- sécurité (détection d'intrusion, protection du réseau par des outils tels les firewalls, etc.)
- etc.

1.1. La QoS dans l'Internet

1.1.1. Définition et besoins

Besoins en termes de fiabilité

Les multiples applications de l'Internet, qui utilisent de nombreux médias, ont des besoins très variables. Ainsi, les médias continus (audio et vidéo) ont pour caractéristique d'être plus ou moins redondants. Ainsi deux images successives d'une transmission vidéo comportent généralement peu de différences. De cette redondance résulte la possibilité que des pertes d'information (image) soient acceptables du point de vue de l'utilisateur final. Il apparaît donc ici pour les médias les plus importants d'une application multimédia (audio et vidéo) une contrainte de fiabilité du transfert des données non plus totale mais partielle, la perte de certaines informations pouvant être acceptable. Notons cependant que l'expression d'une contrainte de fiabilité partielle est à coupler avec la façon dont sont codées les données audio et vidéo. En effet, certains codages (MPEG par exemple) introduisent une dépendance entre

les images qui peut rendre indécodables plusieurs images consécutives en cas de perte de l'une d'entre elles, plus importante que les autres. A l'inverse, un codage de type M-JPEG n'introduisant aucune dépendance entre les images, une contrainte de fiabilité exprimée en termes d'un pourcentage maximum de pertes admissibles et d'un nombre maximum de pertes consécutives s'avère alors valide.

Besoins en termes de débit

Les besoins des applications en termes de débit sont très variables. Certaines, comme les applications Web ou mail ne requièrent que quelques Kilo-octets de bande passante pour les flux qu'elles échangent. D'autres, au contraire, sont beaucoup plus exigeantes. Bien sûr, c'est cette dernière catégorie qui tend à se généraliser car de plus en plus d'applications récentes nécessitent une bande passante importante. On peut situer les applications de diffusion en temps réel comme par exemple les chaînes de télévision sur Internet. Dans ce dernier cas, il est d'ailleurs primordial de pouvoir fournir un service le plus stable et le plus régulier possible de façon à ce que l'utilisateur à l'extrémité du réseau reçoive son flux multimédia avec un niveau de qualité le plus régulier possible.

Besoins temporels

Les applications de diffusion différée de médias continus traitent leurs données de la même façon que s'il s'agissait de médias discrets. Deux types d'applications multimédias présentent des contraintes temporelles : les applications de diffusion en temps réel de médias continus et les applications multimédias interactives. Les contraintes temporelles s'expriment généralement par le biais de deux paramètres : le délai de transit des données et la gigue.

- Délai
  Pour les applications interactives (telle que la visioconférence), et à un degré moindre pour les applications de diffusion en temps réel (telles que le streaming audio ou vidéo), afin que la communication se déroule comme si elle avait lieu localement, il faut que les données soient transmises en un temps inférieur au seuil de perception humain lié au media considéré. Il apparaît ainsi une contrainte sur le délai de bout en bout du transfert des données.
- Gigue
  Les médias continus (tels que l'audio et la vidéo) présentent des contraintes temporelles dues à leur caractère isochrone. Ces contraintes s'expriment en termes de régularité dans l'arrivée des données (on suppose que la source des données émet à un débit correspondant au débit idéal de présentation). Cette régularité s'exprime par une contrainte sur le temps inter-arrivées des données, c'est-a-dire sur la différence entre les dates d'arrivée de deux données successives. Cette contrainte est appelée la « gigue ». La date d'arrivée d'une donnée étant calculée par :

  $$t_{réception} = t_{émission} + dt_{min} + \delta dt$$

  où :
  - dt_{min} désigne le temps de transmission optimal (sans attente dans le réseau) ;
  - δdt désigne le temps d'attente dans le réseau.

  On peut alors exprimer la gigue par :

  $$t_{inter\ réception} = t_{inter\ émission} + \delta dt_2 - \delta dt_1$$

  où :
  - δdt_1 et δdt_2 représentent les temps d'attente dans le réseau pour deux données successives.

1.1.2. Etat de l'art des approches pour la QoS et positionnement de nos travaux

Historiquement, et par rapport aux besoins des applications qui au début de l'Internet se contentaient d'un service de transmission fiable en guise de QoS, des études ont d'abord été menées sur les protocoles de transport afin d'en augmenter les performances et les fonctionnalités ; cela a conduit à la création et au développement du protocole de transport TCP qui a ensuite connu de très nombreuses améliorations.
Dans un second temps, avec l'arrivée des applications multimédias notamment des études ont été menées en plus au niveau IP afin de fournir aux paquets véhiculés un service différent (et meilleur) que le best effort actuel, qui n'offre aucune garantie. Dans cette mouvance, les deux principales approches qui ont été proposées sont IntServ et DiffServ.

Les solutions pour la garantie de la QoS au niveau IP

IntServ propose d'offrir des garanties de QoS par flux et définit deux types de services en plus du best effort : le CL (Controlled Load) et le GS (Guaranteed Service). Le CL propose un service de bout en bout exprimable de façon qualitative en termes de bande passante : il assure que la transmission se fera comme sur un réseau peu chargé (pas de congestion). Le GS propose un service exprimable de façon quantitative en termes de bande passante et de délai de transit maximal : il garantit que tous les paquets d'un même flux arriveront (aux erreurs dues au médium physique près) en un temps borné défini par l'application qui utilise le service. Afin de réserver les ressources réseau (bande passante et mémoire tampon) nécessaires à l'obtention de ces services, l'approche IntServ nécessite l'utilisation d'un protocole de réservation de ressources : RSVP [Bra 97]. Ce protocole propage la demande de réservation à tous les routeurs sur le chemin des données (de façon dynamique afin de s'adapter aux changements de route). Chaque routeur est en charge d'accepter ou non la réservation en tenant compte des ressources disponibles localement et de la caractérisation du trafic fournie avec la réservation.
La limite principale de cette approche concerne la surcharge induite pour les routeurs traversés par ce type de flux, étant donné que chacun doit stocker une information relative aux machines de bout en bout qui échangent ces données pour les traiter comme prioritaires par rapport au reste du trafic. Avec le grand nombre de flux émis en temps réel dans l'Internet à l'heure actuelle, la charge CPU et les limitations en termes de mémoire RAM des routeurs deviendraient rapidement impossible à supporter si l'approche IntServ était déployée à large échelle, ce qui entrainerait une rupture du service et un possible effondrement des différents routeurs traversés par ces flux. Cette limitation porte sur l'impossibilité d'une mise à l'échelle du service IntServ dans l'ensemble de l'Internet. A l'heure actuelle, IntServ n'est ainsi déployé qu'à l'échelle d'un seul domaine et quand ce dernier comporte un nombre de nœuds limité. Pour pallier cette limitation technique, l'approche DiffServ (sans signalisation) a été proposée.

L'idée de base de ***DiffServ*** [Bla 98] est de fournir une QoS différenciée aux paquets traversant un réseau tout en repoussant (le plus possible) la complexité du traitement en bordure du réseau afin de ne pas surcharger le cœur du réseau. De plus, afin d'éviter le problème de passage à l'échelle inhérent aux solutions IntServ, le choix a été fait de traiter un nombre limité d'agrégats (paquets IP n'appartenant pas nécessairement à un même flux) plutôt que des flux individuels. De plus, pour contourner le problème du passage à l'échelle de la solution IntServ, l'approche DiffServ ne génère aucun trafic de signalisation pour éviter de surcharger les routeurs de cœur. La solution DiffServ propose en fait de garantir des contrats de service

(ou SLA : Service Level Agreement) dans un domaine unique [Blake 98]. Ce comportement est donc purement local et ne tient pas compte d'un état global du réseau. Les nœuds frontières se chargent de marquer les paquets selon le code réservé à chaque classe. Ainsi, DiffServ offre aux utilisateurs des différentes classes une garantie statistique du niveau de service demandé.
Les limites des solutions DiffServ ont principalement trait :

- au manque de finesse dans le paramétrage des services, dû à la nécessité de limiter le nombre d'agrégats dans le réseau. En effet, seuls trois types de service différents sont définis dans l'approche DiffServ mais on peut néanmoins imaginer de compléter le nombre de classes de service pour affiner l'approche. Il n'est cependant pas possible de multiplier à l'infini les classes étant donné que le problème de surcharge des routeurs intermédiaires se produirait de la même façon qu'il a été mis en évidence pour l'approche IntServ.
- à la difficulté d'un accord entre administrateurs des différents domaines. En effet, les différents opérateurs sont en concurrence les uns face aux autres. Dès lors, il n'est pas dans leur intérêt de rendre transparent leur politique de gestion des services fournis à leurs clients. Ainsi, fournir une même qualité de service de bout en bout de l'Internet (i.e. en traversant différents domaines) s'avère à l'heure actuelle une tâche délicate voire même impossible.
- à la limitation de la réactivité des services qui sont proposés. En effet, toutes les classes de service reposent sur la définition de contrats de SLA eux-mêmes basés sur des métriques de QoS statiques (délai, pertes, …) et ne prennent pas en compte le caractère variable des caractéristiques du trafic Internet. Une solution à cette limitation qui sera abordée dans la partie 2.3 repose sur l'utilisation de techniques de mesure temps réel dans le réseau pour pouvoir réagir au plus tôt et de façon la plus précise aux évolutions se produisant dans le réseau.

L'adaptabilité au niveau de ressources disponibles

Ces approches qui proposent des classes de services garanties au niveau IP, notamment DiffServ (IntServ étant a priori condamné) nécessitent de gros efforts et un coût conséquent pour leur mise en œuvre à l'échelle de l'Internet. Si DiffServ devient un jour le standard pour la garantie de la QoS, ce ne sera pas avant plusieurs années. Or le besoin d'offrir des services convenables pour de nombreuses applications multimédias existe bel et bien aujourd'hui. Face à ce besoin, et à l'absence d'une solution simple, bon marché et rapide à mettre en place, la plupart des opérateurs ont basé leur stratégie sur le sur-dimensionnement de leur réseau (ou domaine) avec une politique de tarification qui repousse les problèmes, de congestion notamment, à la périphérie de leur réseau. La métrologie est donc un outil essentiel pour acquérir une connaissance du trafic qu'ils doivent transporter, et ainsi, dimensionner leur réseau en conséquence. L'objectif est donc, tout en ayant une unique classe de service qui est la traditionnelle classe « best effort », de l'optimiser de façon à ce qu'elle offre un niveau de service suffisant pour de la voix sur IP par exemple, ou toute autre application ayant des contraintes en termes de niveaux de services. Nous verrons plus loin que le sur-dimensionnement du réseau n'est pas suffisant : le trafic est intrinsèquement très variable et se caractérise par des anomalies imprévisibles qui se manifestent ponctuellement par des augmentations conséquentes du trafic. Naturellement, une connexion de voix sur IP serait alors très perturbée voire stoppée lors d'une telle augmentation de la charge de trafic sur un lien. En plus du sur-dimensionnement des ressources, il faut donc pouvoir ***s'adapter à la dynamicité des ressources disponibles*** dans le réseau lorsque le trafic est à ce point variable.
C'est dans cette optique que je conduis le travail qui est décrit dans ce mémoire : optimiser le niveau de service offert par le réseau en rendant son architecture et ses mécanismes

protocolaires capables de s'adapter aux conditions du trafic. L'objectif est de permettre d'améliorer la QoS du service « best effort » pour des applications aux contraintes très strictes, voir temps-réel (souple) comme de la téléphonie par exemple, et ce à moindre coût. Ce service s'adresse à tous les internautes qui ne sont pas prêts à payer cher un service garanti, et qui sont donc disposés, ponctuellement, à voir leurs connexions interrompues[1].
Naturellement, les outils de base pour pouvoir mettre en place ces mécanismes d'adaptabilité sont la métrologie et la supervision du(es) réseau(x) qui seuls sont capables de détecter les variations sur l'état du réseau et de son trafic et d'alerter les mécanismes nécessaires à l'adaptation au niveau de ressources disponibles. Un des éléments clés est donc la conception et le développement d'un système de métrologie global sans lequel les mécanismes d'adaptation auraient une efficacité réduite. C'est un des problèmes principaux qui vont servir de fil rouge au long de ce mémoire.

Couche Transport (étendue)

L'adaptabilité n'est pas en soi une nouveauté extraordinaire. Il y a plusieurs années, des travaux avaient déjà été menés sur cet aspect pour améliorer les performances de l'Internet « best effort ». A l'époque, l'objectif était d'éviter un très grand nombre de retransmissions qui consommaient inutilement des ressources. Cela avait conduit à l'introduction dans TCP des mécanismes qui font référence aujourd'hui que sont : slow-start, congestion avoidance, fast retransmit et fast recovery.
Plus récemment, avec l'avènement du multimédia, la même approche a été étendue pour offrir des services qui s'adaptent aux besoins de ces nouveaux médias. En particulier, au LAAS, dans le cadre du projet CESAME, un protocole de transport à ordre et fiabilité partielle a été proposé. L'utilisation de ce protocole pour transmettre les flux d'applications multimédias a fait l'objet de ma thèse de doctorat (voir [Owe96b], et mes publications de l'époque comme [Owe95] [Owe96a], [Owe98], etc.).
Récemment, de nombreux travaux se sont attachés à proposer de nouveaux protocoles de Transport pour enrichir les fonctionnalités et/ou les services des protocoles UDP et TCP, sur le même modèle de ce que nous avions fait dans le cadre de CESAME de 1992 à 1995. Les paragraphes suivants présentent les protocoles, SCTP et DCCP, actuellement développés à l'IETF, et FPTP – conçu et développé au LAAS - qui est une évolution des protocoles à ordre et fiabilité partiels conçus dans CESAME.

- SCTP
  Le protocole SCTP [Ste 00], est un protocole de transport à fiabilité totale se déployant sur un service paquet de niveau réseau sans connexion, offert par exemple par le protocole IP. Il est unicast et orienté session, une session étant définie comme une association établie entre deux hôtes. Dans le cas où un hôte dispose de plusieurs adresses IP, les adresses sont échangées lors de l'établissement de la session (on appelle « multi-homing » le fait que plusieurs adresses IP peuvent correspondre à une session). Un mécanisme de contrôle d'erreur est implémenté dans SCTP et permet de détecter les pertes, la rupture de séquences, la duplication ou la corruption de paquets. Un schéma de retransmission est utilisé pour corriger ces erreurs. SCTP utilise le principe de SACK [Mat 96] pour la confirmation de la réception des données. Les retransmissions sont faites après expiration d'un timer ou sur interprétation du SACK. Au contraire de TCP, SCTP est orienté message (ce qui le rapproche par cet aspect de UDP). Chaque paquet contient un en-tête commun et

[1] A la limite, on peut également imaginer que ces mécanismes d'optimisation puissent être couplés avec des mécanismes garantissant des niveaux de QoS statistiques (comme DiffServ). Nous n'avons toutefois pas encore abordé cette question.

une partie donnée (contenant soit des données utilisateurs soit des données de contrôle). En fait, bien qu'il soit orienté message, plusieurs données peuvent être contenues dans le même paquet, mais seront délivrées à l'application avec le format des messages initiaux. SCTP offre un service de multiplexage/démultiplexage entre flux : une application multimédia peut être découpée en plusieurs flux pouvant avoir chacun des schémas de remise des données différents. C'est donc un protocole d'ordre total au sein d'un flux et n'offrant aucune garantie sur l'ordre inter-flux, ce qui permet au protocole de délivrer les données d'un flux même si des pertes ou des déséquencements sont détectés sur un autre flux. Le type de contrôle de flux et de congestion est négocié à l'établissement de la connexion. Ces mécanismes sont construits sur la base des algorithmes de TCP : le récepteur informe l'émetteur de sa taille de buffer et la taille de la fenêtre de congestion est contrôlée au cours de la connexion SCTP. Les mécanismes de « slow-start, congestion avoidance, fast recovery et de fast-retransmit » sont les mêmes que ceux de TCP mais ils utilisent les paquets SCTP comme unités d'acquittement. SCTP peut intéresser les applications désirant un service de transport à ordre partiel. Cependant, le fait que SCTP offre un service totalement fiable entraîne une incompatibilité avec les applications multimédias ayant des contraintes en termes de débit, de délai ou de gigue. Une extension [Ste 03] de SCTP permet d'offrir un service à fiabilité partielle temporisée. Une fiabilité partielle temporisée signifie que l'utilisateur peut spécifier une durée de vie à son message. Mais ce service n'est pas adapté aux applications à temps contraint présentant des données applicatives spécifiques, comme par exemple les données des images I, P et B d'un flux vidéo MPEG.

- DCCP

  Le protocole DCCP [Han 03], offre un service de transport non fiable pour des flux en datagrammes (donc type UDP) mais intégrant plusieurs mécanismes de contrôle de congestion, ce qui permet aux applications utilisant habituellement UDP de ne pas avoir à implémenter le leur. Le but de DCCP est d'offrir l'efficacité d'UDP à certaines applications tout en respectant les autres flux (TCP) du réseau. Les mécanismes de contrôle de congestion sont négociés pour les deux sens de la connexion entre les hôtes au moyen d'un identifiant appelé CCID. Plusieurs mécanismes sont disponibles, parmi lesquels un contrôle de congestion TCP-like utilisant une fenêtre de congestion et un algorithme TFRC TCP-Friendly Rate Control [Flo 01]. DCCP peut être utilisé par toutes les applications présentant des contraintes temporelles et qui sont capables de s'adapter aux fluctuations de débit imposées par les mécanismes de contrôle de congestion. Cela, dit même si DCCP apporte un plus par rapport à TCP en termes de mécanisme de contrôle de congestion (implémentation de TFRC), il reste encore basé sur une solution de bout en bout statique. Cette solution a été évaluée dans la partie 2.2.3 de ce manuscrit dans lequel nous avons mis en évidence que même si la régularité du trafic était améliorée avec l'utilisation de TFRC, la performance globale restait légèrement en deçà de ce que pouvait mettre en œuvre TCP dans le réseau. La solution que nous proposons pour améliorer à la fois la régularité du trafic et les performances obtenues dans le réseau repose sur l'utilisation de techniques de métrologie permettant d’obtenir des informations en temps réel sur l'état du réseau de façon à réagir au plus près aux fluctuations de bande passante disponible ou encore aux phénomènes de congestion se produisant dans le réseau. En effet, comme nous allons le voir dans la partie suivante, la variabilité du trafic Internet est très importante, ce qui se traduit par une très grande dynamicité des ressources disponibles qu'il faut prendre en compte pour permettre une meilleure gestion du réseau et de la QoS que l'on peut y mettre en œuvre.

- MMPOC

  Un transport à ordre partiel [Owe 98] est un transport qui délivre les unités de données envoyées sur une ou plusieurs connexions, suivant un ordre (partiel) donné. Cet ordre est un ordre situé entre l'ordre total (TCP) et aucun ordre (UDP) et peut s'exprimer comme une composition série/parallèle d'objets ou d'unités de données. Notons que cet ordre peut, par exemple, être décrit par un Réseau de Pétri à Flux Temporels (Time Stream Petri Net – TSPN, une extension temporelle du modèle de Réseau de Pétri général), comme dans le cas de la composition série/parallèle des flux son et vidéo d'une application de visioconférence [Owe 98]. Dans ce cas, l'ordre de délivrance peut être vu comme la synchronisation logique d'objets multimédias, la synchronisation étant l'un des points-clés les plus importants des systèmes multimédias distribués.

  De plus, la possibilité de pertes dans le réseau amène à l'intéressante notion de fiabilité partielle. Cette notion est étroitement liée à la QoS du transport : elle définit une QoS nominale et une QoS minimale en dessous de laquelle le service demandé par l'utilisateur n'est plus assuré. Cette QoS minimale peut être exprimée en définissant un ensemble de pertes acceptables, par exemple un nombre maximum de pertes à l'intérieur d'une séquence, un nombre maximum de pertes consécutives... Quand une perte acceptable est détectée (c'est-à-dire quand un objet reçu a une numérotation plus élevée que prévu), l'objet manquant peut instantanément être déclaré perdu (indication de perte au plus tôt), et les données suivantes déjà reçues peuvent être immédiatement délivrées à l'application (délivrance au plus tôt). Si la perte ne peut pas être acceptée par rapport à la fiabilité demandée, une retransmission devra être effectuée. La fiabilité partielle exigée, définie dans le service de transport à ordre partiel et ayant pour résultat des indications de perte et de délivrances au plus tôt, se déduit des besoins de l'application.

  En fait, deux approches existent pour contrôler la fiabilité partielle : média par média ou par groupe de médias. Média par média signifie que l'entité de réception du flux peut seulement gérer la fiabilité partielle sur le flux qu'elle contrôle, et pas sur les autres flux de la connexion multimédia. Dans une gestion par groupe de médias, l'entité de réception peut déclarer des pertes sur d'autres flux de la même connexion multimédia, ce qui mène à un comportement plus interactif. Dans ce cas, si une perte est acceptable sur un flux, on peut déclarer une donnée perdue pour en délivrer immédiatement une autre à l'application.

- FPTP

  FPTP [Exp 03] est un protocole configurable et programmable qui fournit des services de communication capables de satisfaire les contraintes en QoS des applications multimédias distribuées. Les services de FPTP sont fournis grâce au déploiement de nouveaux mécanismes de niveau Transport et par la configuration de ceux existants. Protocole de Transport de nouvelle génération orienté QoS, il vise à fournir une ensemble de mécanismes Transport aptes à répondre aux besoins applicatifs en utilisant de manière aussi optimisée que possible les services et les ressources réseau disponibles. Il est ainsi possible de composer, étendre et spécialiser le protocole, tout en utilisant et étendant les services existants.

  Les besoins en QoS et les actions à accomplir quand on ne peut les satisfaire doivent être exprimés à l'aide d'une spécification:

  - De la QoS par flux. Un flux correspond à un media (i.e. audio, vidéo, données, etc.). La QoS du flux s'exprime par la bande passante requise pour la transmission, le délai, le taux de pertes acceptable et le "désordre" acceptable entre unités de données (niveau de déséquencements). Il est aussi nécessaire d'exprimer le niveau de synchronisation entre les différents flux d'une même session.

- De la politique de QoS, c'est à dire la tolérance du service partiellement ordonné et fiable ainsi que les actions à accomplir en cas de violation de cette tolérance.

FPTP inclut les services de négociation, la prise en compte des besoins et la mise en œuvre des mécanismes de transport requis. Il intègre aussi des mécanismes de contrôle et de gestion conçus pour garantir au mieux la QoS de la session multimédia (Contrôle de congestion, contrôle d'erreur et contrôle des contraintes temporelles). La terminaison de la session prend en charge la libération des ressources.
L'API FPTP est une extension de l'interface classique socket. Ce choix garantit le maintien de la compatibilité avec les applications multimédias existantes et permet aux nouvelles de définir explicitement leurs besoins en termes de QoS.
Les mécanismes de QoS peuvent être classés en 2 catégories: les mécanismes statiques liés à la détermination de la QoS à fournir et les dynamiques qui contrôlent la QoS pendant la phase de transfert. Le tableau 1 montre ces mécanismes classés par catégories et nous donne un aperçu de l'API (Application Programming Interface) à travers les paramètres permettant de définir les mécanismes disponibles.

Etablissement (mécanismes statiques)	
Mise en place	Dérivation ou traduction de la QoS en paramètres Transport
Admission et déploiement	Acceptation des demandes de QoS à partir de l'évaluation des ressources disponibles. Ces mécanismes assurent également le contrôle et la gestion des mécanismes de déploiement pour fournir la QoS demandée
Contrôle (mécanismes dynamiques)	
Gestion du flux	Mécanismes utilisés pour le contrôle de flux base sur la spécification de la QoS (i.e. bande passante, délai, fiabilité, ordre, synchronisation, etc.).
Contrôle des ressources disponibles	Les contrôles de flux et de congestion gèrent les émissions de données en fonction des ressources disponibles et des capacités du récepteur.
Gestion (mécanismes dynamiques)	
Surveillance de la QoS	Vérifie la QoS fournie par les mécanismes de contrôle. Les mécanismes de gestion renvoient des alertes quand un paramètre de QoS viole les limites décrites dans la spécification. Il est aussi possible d'envoyer des signaux aux mécanismes de contrôle pour leur indiquer une dégradation de la QoS

Tableau 1 : Classification des mécanismes de QoS de FPTP

1.2. Métrologie de l'Internet : un nouvel outil pour la recherche en réseaux

Suite à ce qui précède, il apparaît clairement que fournir de la QoS dans l'Internet revient à résoudre une triple problématique. La solution qui y parviendra devra :
- Etre insensible aux facteurs d'échelle ;
- Fournir une solution de bout en bout indépendamment des différents domaines et AS (Autonomous System) traversés ;
- S'adapter à la dynamicité des ressources du réseau et à la variabilité du trafic.

La métrologie est une activité en plein essor dans le domaine des réseaux IP qui est très prometteuse pour résoudre cette triple problématique. En effet, la métrologie doit permettre de mesurer en continu la QoS offerte par un réseau et donc d'adapter les mécanismes de transmission aux conditions de trafic et du réseau. Ainsi, la métrologie devra dire quels traitements appliquer à quels flux (en espérant que le nombre de flux sera réduit pour être peu sensible au facteur d'échelle). De la même façon, elle devra indiquer où les flux devront être supervisés et où ces traitements devront être appliqués. Cela suppose donc d'avoir à tout moment une connaissance assez précise du trafic et de ses caractéristiques pour pouvoir réagir en conséquence, notamment pour s'adapter à la dynamicité des ressources qui apparaît comme étant un des problèmes majeur de l'Internet dès lors qu'on veut garantir une QoS stable.

Toutefois, même si les opérateurs réseaux utilisent des techniques de métrologie depuis la mise en place des premiers réseaux de communication, cette discipline n'a jusqu'à présent jamais été utilisée comme elle aurait dû l'être. Pour l'instant, les opérateurs utilisent la métrologie, souvent passive et en ligne (à partir de SNMP et de ses MIB), pour faire de la supervision du réseau ainsi que du trafic qui circule dessus. Mais ce type de solution ne permet pas une analyse du trafic très fine, et notamment pas en rapport avec la fréquence des variations du trafic actuel. En effet, le protocole SNMP associé aux MIB ne permet pas de considérer des granularités d'observation inférieures à quelques minutes. Or il est nécessaire de considérer l'ensemble des échelles (des plus fines aux plus larges) pour une bonne analyse du trafic. Dès lors, le besoin d'outils de métrologie plus performants (capables de considérer à la fois des échelles d'analyse inférieures et supérieures à la seconde) devient nécessaire.

Nous allons donc voir dans la suite comment la métrologie peut se positionner comme un outil adéquat pour aider à dissiper une partie de cette méconnaissance des caractéristiques du trafic et des comportements réseaux et utilisateurs.

1.2.1. Métrologie active et passive

Vue l'intérêt grandissant pour la métrologie des réseaux IP, beaucoup de projets de recherche sur ce sujet sont en cours, en particulier conduits par des opérateurs Internet et des laboratoires d'études et de recherche partout dans le monde. Ces projets peuvent être répartis en deux grandes classes : ceux fondés sur les mesures actives et ceux reposant sur les mesures passives décomposées elles-mêmes en mesures passives en ligne et hors ligne. Chacune de ces deux classes permet de mieux comprendre le comportement à la fois du réseau (observation des taux de perte, des délais, …) et des applications (réactions en temps réel des applications aux pertes dans le réseau, du taux de transmission utile, …) et de mettre en lumière les interactions entre les applications et le réseau. La suite présente ces deux approches, en commençant par la métrologie active qui fut chronologiquement la première à être utilisée.

Métrologie active : principe et exemples

Le principe des mesures actives consiste à générer du trafic dans le réseau à étudier et à observer les effets des composants et protocoles – réseaux et transport – sur le trafic : taux de perte, délai, RTT, etc. Cette première approche possède l'avantage de prendre un positionnement orienté utilisateur. Les mesures actives restent le seul moyen pour un utilisateur de mesurer les paramètres du service dont il pourra bénéficier. En revanche, l'inconvénient majeur de cette approche est la perturbation introduite par le trafic de mesure qui peut faire évoluer l'état du réseau et ainsi fausser la mesure. De nombreux travaux menés actuellement abordent ce problème en essayant de trouver les profils de trafics de mesures qui

minimisent les effets du trafic supplémentaire sur l'état du réseau. C'est par exemple le travail en cours au sein du groupe IPPM[2] de l'IETF[3] [Pax 98] [Alm 99a] [Alm 99b] [Alm 99c].
Les mesures actives simples restent tout de même monnaie courante dans l'Internet pour lequel de nombreux outils de test, validation et / ou mesure sont disponibles. Parmi eux, on peut citer les très célèbres *ping* et *traceroute*. *Ping* permet de vérifier qu'un chemin est valide entre deux stations et de mesurer certains paramètres comme le RTT[4] ou le taux de perte. *Traceroute* permet de voir apparaître l'ensemble des routeurs traversés par les paquets émis jusqu'à leur destination et donne une indication sur les temps de passage en chacun de ces nœuds.

L'un des projets les plus simples en théorie était le projet ***Surveyor*** [Kal 99] de la NSF[5] aux Etats-Unis qui reposait sur l'utilisation de *ping*, amélioré par la présence d'horloges GPS[6] sur les machines de mesure. L'objectif de ce projet était donc d'étudier les délais de bout en bout et les pertes dans l'Internet.

Plusieurs projets ont actuellement pour sujet les mesures actives.

- Le projet NIMI[7] (initié par Vern Paxson aux Etats-Unis) [Pax 00] a pour objectif le déploiement d'une infrastructure nationale (au niveau des Etats-Unis) de mesures actives. Cette infrastructure est flexible et permet le recueil de diverses mesures actives. Cette infrastructure a été utilisée durant les deux ou trois années passées pour plusieurs campagnes de mesures, dont la détermination d'une matrice de distance dans Internet. L'infrastructure NIMI s'est aussi étendue en Europe, notamment en Suisse.
- En Europe, le projet RIPE (Réseaux IP Européens) TTM, tente de déployer une infrastructure semblable à l'infrastructure de NIMI en Europe. Par rapport à NIMI, RIPE fournit des services à des clients : RIPE se propose de réaliser toutes les études qui peuvent être demandées par des clients, en plus des services classiques d'accès à des statistiques globales d'utilisation des liens du réseau Européen de la recherche surveillés.
- Le projet MINC[8] [Ada 00] [Cac 99] est un client du projet NIMI. Il utilise la diffusion de sondes actives par le biais du multicast pour inférer sur la structure interne du réseau et les propriétés sur tous les liens d'interconnexion ainsi traversés. En allant plus loin, c'est le sujet de la tomographie qui est au centre de ce projet qui se focalise sur certains aspects dynamiques du trafic, comme les propriétés du routage, les pertes et les délais. Toutefois, comme le multicast n'est pas un service disponible partout, et comme il a été montré que le trafic dans l'Internet n'est pas forcément symétrique, l'intérêt du multicast dans cette tâche n'est concrètement pas évident. Aussi, le projet UINC (Unicast INC) a vu le jour et tente de reproduire le travail de MINC en unicast.
- Le projet *Netsizer* [Net 01] de Telcordia (ex Bellcore) a pour objectifs de mesurer la croissance de l'Internet, les points durs de congestion, les délais, *etc*. Pour cela, depuis un ensemble de stations situées chez Telcordia, un programme teste la présence sur le réseau de toutes les adresses IP existantes et met à jour suivant les résultats une carte de l'Internet. Un des gros problèmes de ce projet reste ainsi un problème de représentation.

[2] IPPM : IP Performance Metrics
[3] IETF : Internet Engineering Task Force
[4] RTT : Round Trip Time
[5] NSF : National Science Fondation
[6] GPS : General Positioning System
[7] NIMI : National Internet Measurement Infrastructure
[8] MINC : Multicast-based Inference of Network-internal Characteristics

- Le projet Européen INTERMON [Mil 04], qui a exploité les premiers résultats du projet européen AQUILA [Aqu 05], se propose de développer un ensemble d'outils de bout en bout pour permettre une caractérisation de la QoS dans les réseaux large échelle (Internet en particulier). L'idée est de pouvoir ainsi faciliter la définition de SLA entre les clients et les opérateurs Internet Européen. En particulier, un des objectifs de ce projet est de pouvoir détecter plus facilement quand les paramètres du contrat de service sont rompus et quelles sont les causes de ces dysfonctionnements : par exemple un simple non respect par les clients des paramètres définis dans le SLA ou à l'inverse des dysfonctionnements réseaux plus problématiques pour l'opérateur. Dans ce dernier cas, l'utilisation d'outils basés sur *traceroute* est privilégiée pour détecter par exemple les changements et ruptures dans les routes Internet.
- Le projet américain AMP[9] de NLANR[10] [Nla 01] [Mcg 00] a pour objectif de faire de la mesure active (« active probing »), et propose des télescopes de l'Internet.
- Le projet MOME [Mom 05] est une action coordonnée du programme IST de l'union européenne visant à offrir une plateforme commune pour l'échange d'outils et de connaissance dans le domaine de la mesure et la supervision des réseaux. De plus elle doit permettre la coordination des activités de métrologie et de mesure des réseaux IP entre les différents projets et acteurs européens. Ainsi, la plateforme fournit des informations pour tester l'interopérabilité des outils de mesures des différents projets. Enfin, une base de données est aussi mise à disposition ; elle contient les mesures collectées.
- Le projet *traceroute@home* a été initié en marge du projet METROPOLIS, et continue aujourd'hui avec un support du réseau d'excellence E-NEXT et en partenariat avec les universités de Boston et d'Indiana. Il a pour objectif de mettre en place des techniques de mesures actives basées sur l'outil *traceroute* pour découvrir la topologie de l'Internet [Don 05].

Métrologie passive : principe et exemples

Les projets de mesures passives sont apparus beaucoup plus tardivement que les projets de mesures actives car ils nécessitent des systèmes de capture ou d'analyse du trafic en transit relativement avancés, et développés plus récemment. Le principe des mesures passives est de regarder le trafic et d'étudier ses propriétés en un ou plusieurs points du réseau. L'avantage des mesures passives est qu'elles ne sont absolument pas intrusives et ne changent rien à l'état du réseau lorsqu'on utilise des solutions matérielles dédiées (par exemple sur la base de cartes DAG [Dag 01] présentées dans la suite). De plus, elles permettent des analyses très avancées. En revanche, il est très difficile de déterminer le service qui pourra être offert à un client en fonction des informations obtenues en métrologie passive.

D'autre part, les systèmes de métrologie passive, peuvent se différencier en fonction du mode d'analyse des traces. Ainsi, le système peut faire une analyse en-ligne ou hors-ligne. Dans le cadre d'une analyse en-ligne, toute l'analyse doit être effectuée dans le laps de temps correspondant au passage du paquet dans la sonde de mesure. Une telle approche, temps-réel, permet de faire des analyses sur de très longues périodes et donc d'avoir des statistiques significatives. Par contre, la complexité maximale pour ces analyses reste très limitée à cause du faible temps de calcul autorisé. Une analyse hors-ligne oblige, à l'inverse, la sonde à

[9] AMP : Active Measurement Project
[10] NLANR : National Laboratory for Applied Network Research

sauvegarder une trace du trafic pour analyse ultérieure. Une telle approche demande ainsi d'énormes ressources ce qui représente une limitation pour des traces de très longue durée. Par contre, une analyse hors-ligne permet des analyses extrêmement complètes et difficiles, capables d'étudier des propriétés non triviales du trafic. De plus, comme les traces sont sauvegardées, il est possible de faire plusieurs analyses différentes sur les traces, et de corréler les résultats obtenus pour une meilleure compréhension des mécanismes complexes du réseau.

L'endroit idéal pour positionner des sondes de mesures passives est indéniablement dans les routeurs. CISCO a ainsi développé le module Netflow [Net 05] pour ses routeurs, qui scrute le trafic en transit, et génère régulièrement des informations statistiques sur ce trafic. Netflow a ainsi été utilisé dans de nombreux projets présentés ci-après. L'expérience montre toutefois que les performances de Netflow restent limitées (code écrit en Java et interprété), et que l'influence sur les performances du routeur est non négligeable.

Toutefois, le premier projet connu – le projet AT&T *Netscope* [Fel 00a] – a débuté il y a environ 7 ans et repose sur ce système *Netflow* de CISCO. Ce projet de mesure passive en ligne a pour but d'étudier les relations entre le trafic transitant en chaque nœud du réseau et les tables de routage des routeurs. L'objectif final est d'utiliser ces résultats pour améliorer les politiques et décisions de routage, afin d'équilibrer au mieux la charge dans les différents liens du réseau, et ainsi améliorer la qualité de service perçue par chaque utilisateur. C'est de la tomographie afin de trouver ensuite des politiques d'ingénierie des trafics adéquates.

Vern Paxson et al. d'ACIRI ont également conduit un projet de mesure passive en ligne dont l'objectif était de proposer un modèle pour les arrivées de flux et de paquets sur les liens de l'Internet. Ce travail [Pax 95] achevé depuis 1995 a été et reste une référence dans le milieu de la recherche Internet. Cependant, aujourd'hui, avec l'apparition de nouvelles applications qui n'existaient pas à l'époque et avec les changements dans la façon d'utiliser l'Internet, ce travail doit être reconduit. Les résultats ne sont certainement plus valables aujourd'hui, et il n'existe aucune technique sûre d'extrapolation de ces résultats pour essayer de modéliser le trafic d'aujourd'hui.

De façon plus générale, le laboratoire CAIDA[11] à San Diego, Californie, est spécialisé dans l'étude du trafic Internet et mène un projet dont l'objectif est d'étudier sur le long terme l'évolution du trafic, avec l'apparition des nouvelles applications comme les jeux, le commerce électronique, etc. D'autre part, ce projet étudie aussi les variations en fonction du moment de la journée, du jour de la semaine, de la période de l'année, etc. [Cla 98] [Mcc 00]. Pour ce faire, le système de métrologie repose sur les modules OC3MON [Aps 97] et OC12MON qui permettent de traiter le trafic de liens IP/ATM dont les capacités respectent respectivement les normes OC3 (155 Mbps) et OC12 (622 Mbps). D'autre part, pour l'analyse statistique, CAIDA a développé la suite logicielle *CoralReef* [Cor 01] [Key 01] qui est complémentaire des systèmes OCxMON. D'autres études sont en cours, notamment sur les problèmes de représentation de l'Internet [Huf 01], ou d'étude des délais. Pour plus d'information, le lecteur pourra consulter [Cai 05].
A noter que les systèmes OCxMON sont aussi utilisés par Worldcom et NLANR pour faire de la métrologie sur le réseau vBNS [Vbn 01].

En France, le projet NetMet [Sim 01] a débuté il y a 5 ans environ et a été conçu et développé par et pour des administrateurs réseaux. Il repose sur la technologie CISCO Netflow et offre à

[11] CAIDA : Cooperative Association for Internet Data Analysis

ses utilisateurs deux approches passives de niveaux différents pour la métrologie. La première est une étude macroscopique du trafic comme le font la plupart des analyseurs et logiciels d'administration réseaux, notamment ceux basés sur l'utilisation des MIB SNMP. Le second niveau, plus fin, consiste en une trace de chaque flux qui a traversé le routeur. Il n'y a à l'heure actuelle pas d'outil pour analyser cette trace de flux (ils doivent être développés par les utilisateurs / administrateurs en fonction de leurs souhaits), mais cette trace est une mine d'informations à la fois pour des activités d'administration et d'opération des réseaux, mais également pour la recherche en réseau. A noter également qu'une extension de NetMet appelée NetSec [Mar 01] propose des facilités pour l'étude des attaques générées à l'encontre d'un réseau. Il repose sur les mêmes principes métrologiques que NetMet (approches macroscopique du trafic, et orientée flux).

Ensuite, SPRINT a démarré il y a 6 ans un des projets les plus ambitieux du moment basé sur des mesures actives hors ligne. Ainsi, Sprint enregistre des traces complètes de tous les entêtes de tous les paquets qui transitent en certains points de son réseau IP. Cette granularité microscopique permet d'approfondir les analyses que l'on peut faire dans la compréhension des interactions qui existent entre tous les flux, les mécanismes des routeurs, etc. A noter que le système IPMON de Sprint, décrit plus en détail dans la suite, repose sur la carte DAG [Dag 01] conçue par l'université de Waikato en Nouvelle Zélande et qui se charge d'extraire les entêtes des paquets, de les estampiller suivant une horloge GPS et de les stocker sur un disque dur [Cle 00].

Enfin, le projet français METROPOLIS, dont de nombreux résultats font plus spécifiquement l'objet de ce manuscrit, fut l'une des premières tentatives dans ce domaine en France. Il avait pour objectif de fédérer plusieurs laboratoires universitaires et de l'industrie. Ainsi, les différents partenaires étaient le LAAS, le LIP6, France Télécom R&D, l'INRIA, le GET, Eurécom et RENATER. Ce projet a été labellisé par le RNRT, a commencé en novembre 2001 et s'est achevé en février 2005. Il aborde les thèmes d'étude suivants :
- La classification du trafic et le dimensionnement du réseau ;
- L'analyse du réseau (protocoles, routeurs) ;
- La modélisation du trafic et de ses propriétés ;
- La définition de procédure de tarification et de mise en place de SLA.

La particularité de ce projet est qu'il combinait les approches de métrologie actives et passives, ce qui permettait de corréler ces deux types de mesures. Cette combinaison a apporté un plus considérable par rapport aux autres projets. Son deuxième point fort résidait dans la diversité des réseaux sur lesquels ont été effectuées les mesures. Les réseaux étudiés étaient :
- Un réseau expérimental avec le réseau VTHD ;
- Un réseau public opérationnel avec le réseau Rénater ;
- Un réseau commercial : certaines plaques ADSL du FAI France Télécom.

Il faut noter que le projet METROPOLIS a grandement contribué à l'essor de la métrologie dans la communauté de recherche académique française de recherche en réseau. Il a été pour moi un élément structurant de mon activité de recherche, et à ce titre est une des sources d'informations principale de ce manuscrit. Il sera donc souvent question, dans la suite de ce manuscrit, de résultats issus du projet METROPOLIS.

1.2.2. Caractérisation et analyse du trafic Internet

Avec tous ces projets de métrologie fournissant des traces, les chercheurs ont pu travailler à la caractérisation du trafic Internet et à sa modélisation. Nous nous attacherons ici à synthétiser les différents modèles de description du trafic qui ont été élaborés au moyen de l'analyse de campagnes de mesures. Celles-ci ne seront que peu évoquées en elles-mêmes. Il s'agira généralement d'observations réalisées à l'aide de sondes passives, plus spécialement adaptées à la fourniture de paramètres descriptifs du trafic. Les sondes actives fournissent quant à elles des informations plutôt liées à la performance du trafic et à la QoS réseau, sujets débordant quelque peu du cadre assigné à cette partie. Il est à noter que cette partie reprend, en les synthétisant et les réactualisant un état de l'art de METROPOLIS [Owe 03b] sur le sujet.

1.2.2.1. Diversité du trafic Internet

1.2.2.1.1. Caractéristiques générales du trafic IP

Un réseau de type Internet a vocation à transporter un grand nombre de types de médias possédant des caractéristiques de trafic différentes et éventuellement des contraintes de Qualité de Service (QoS) différenciées. Cependant, dans le souci d'une modélisation simplifiée autant que pour les besoins opérationnels de gestion du réseau, l'on recherche plutôt une classification grossière des différents types de trafics [Rob 00]. La plupart des auteurs s'accordent généralement pour distinguer deux grandes classes de trafics applicatifs dans les réseaux à haut débit :

- Le trafic de type « **streaming** », dont la durée et le débit ont une réalité intrinsèque bien que variable éventuellement. Souvent associé à la notion de services « orientés connexion », son intégrité temporelle doit être préservée par le réseau. Le délai de transfert des données de même que sa variation, la gigue, doivent être contrôlables, tandis qu'un certain degré de perte de paquets peut être tolérable. Les flux de trafic streaming sont typiquement produits par les services téléphoniques et vidéo (vidéoconférence ou téléchargement « on-line » de séquences).
- Le trafic dit « **élastique** », ainsi nommé car son débit peut s'adapter à des contraintes extérieures (bande passante insuffisante par exemple) sans pour autant remettre en cause la viabilité du service. Cette classe de trafic est essentiellement engendrée par le transfert d'objets numériques par nature (par opposition au transfert en mode numérique d'informations analogiques à la source) tels que des pages Web (application HTTP), des messages électroniques (e-mail, application SMTP) ou des fichiers de données (application FTP). Le respect de leur intégrité sémantique est indispensable mais les contraintes de délai de transfert sont moins fortes. Cette intégrité sémantique est la plupart du temps assurée par le protocole de transport (TCP) et ne constitue donc pas un élément de performance sur lequel l'opérateur de réseau peut agir ; en revanche, le maintien d'un certain débit effectif minimum de transfert des documents est un objectif de QoS.

Le trafic de type élastique est actuellement largement majoritaire sur les réseaux IP : on constate couramment [Tho 97] des proportions supérieures à 95% en volume (octets) et à 90% en nombre de paquets pour le trafic sous TCP, protocole sous lequel fonctionnent la plupart des applications mentionnées ci-dessus. Des proportions similaires ont été observées récemment sur les réseaux de France Télécom et Renater (cf. partie 1.2.2.1.2).

L'analyse des caractéristiques du trafic Internet s'effectue commodément en se plaçant à un niveau de représentation selon trois entités de trafic, correspondant à trois échelles de temps différentes et, quoique de manière assez grossière, à trois niveaux (couches) de la pile protocolaire des réseaux de données :

- Les « **paquets** » forment l'entité de trafic la plus fine que l'on considère dans les réseaux de données, le paquet étant l'unité élémentaire traitée par la couche « réseau ». Les paquets sont *a priori* de longueur variable dans un réseau IP et leur processus d'apparition est très complexe, en raison notamment de la superposition de services de nature très diverse et de l'interaction des couches protocolaires (dispositifs de contrôle de flux et de retransmission sur perte de paquets, tels TCP [Bla 92]). Le trafic au niveau paquet possède la caractéristique unanimement reconnue d'auto-similarité, laquelle rend très ardue l'évaluation de ses performances à ce niveau. Les échelles de temps décrivant le processus des paquets sont la microseconde ou la milliseconde, en fonction des ordres de grandeur du débit de transmission des liens.
- Les « **flots** » constituent une entité de trafic intermédiaire que l'on pense être la mieux adaptée pour effectuer les études d'ingénierie du trafic IP. Ils correspondent à des transferts plus ou moins continus de séries de paquets associés à une même instance d'une application donnée. Pour être plus précis, référons-nous en premier lieu à l'une des principales études menées de manière extensive sur cette notion [Cla 95] : nous rappelons qu'on définit un **flot** comme un ensemble de paquets IP répondant à une même **« spécification de flots »** et se succédant les uns les autres à un intervalle de temps inférieur ou égal à un seuil donné que l'on nomme **« Time Out » (TO)**. Cette notion de Time Out permet de garantir une certaine cohérence temporelle à la suite de paquets identifiée par une spécification de flots, c'est-à-dire que les flots de paquets ne présentent pas de trou trop important dans leur processus d'arrivées[12]. Par exemple, lorsqu'on traite d'ingénierie du trafic, on définit en général un flot comme étant l'ensemble des paquets dont les adresses destinations ont un préfixe commun, et délimités par un Time Out sur une période d'inactivité. Mais on peut également considérer ces flots par rapport à des propriétés applicatives. Ainsi, les flots de type streaming sont associés à des communications audio/vidéo (téléphonie sur IP, vidéoconférence) ou encore à des téléchargements en temps réel de séquences vidéo. Les flots de trafic élastique sont créés par le transfert d'un fichier, d'un message, d'un objet (ou document) au sein d'une page HTML, etc. Un flot correspond donc plus ou moins à la couche transport de la pile protocolaire Internet ; mais pas complètement puisque cette notion n'est pas nécessairement équivalente à celle d'une connexion TCP, par exemple. Une connexion TCP est un flot (on parle plutôt dans ce cas de ***flux***) pour lesquels les paquets qui le

[12] La cohérence temporelle est essentielle à maintenir pour la modélisation des performances du trafic sous TCP. Par ailleurs, l'introduction d'un TO sert pour décider qu'un flot est terminé ou non ; c'est un élément indispensable si l'on envisage l'implémentation de traitements par flots dans les routeurs du réseau : le dépassement de TO sans nouvelle arrivée de paquet liée à une spécification de flot active permet de déclarer le flot terminé et de le supprimer de la table d'états du routeur. Dans ces conditions, l'estimation d'un TO optimal revêt une importance primordiale afin d'économiser les ressources en mémoire et en temps CPU des machines. La spécification d'un TO est loin d'être triviale ; elle peut être : (i) différenciée selon le type de protocole ou d'application ; (ii) adaptative en fonction du débit des flux [Ryu 01] ; (iii) motivée par des préoccupations diverses (pour ne pas dire divergentes) telles que l'élaboration de modèles de performance du trafic, la mise en œuvre de disciplines de service par flot ou de politique de routage dans les nœuds du réseau ; (iv) etc. Sans trop entrer ici dans les détails, mentionnons que la spécification de flots peut comprendre quatre dimensions [Cla 95] : la directionalité des flots (mono- ou bi-directionalité) ; la prise en compte d'une ou deux des extrémités (origine ou destination des paquets) ; la granularité des extrémités (de la plus fine, les applications, à la plus grossière, les sous-réseaux) ; enfin, le protocole de la couche transport.

constituent ont les mêmes adresses source et destination, les mêmes ports source et destination, le même champ « protocol », et sont délimités par des paquets de début (SYN) et de fin (FIN) de connexion[13]. La différence entre un flux et une connexion a trait au caractère mono-directionnel d'un flux. Une connexion est en fait la réunion de flux de sens opposés (les adresses source et destination des deux flux qui composent une connexion sont inversées). On peut estimer que les flots/flux ont une durée s'étendant de quelques secondes à quelques minutes, voire quelques heures.

- Au plus haut niveau, on peut tenter de définir la notion de « **sessions** » dans le but de se rapprocher des périodes d'activité des utilisateurs (transposition de la notion d'appels considérée en téléphonie à commutation de circuits). Pour le trafic streaming, ce niveau ne se distingue guère de celui des flots, du moins temporellement, puisque ce dernier correspond déjà à des communications ou des appels. S'agissant du trafic élastique, les sessions peuvent être associées à des connexions Telnet, FTP, ou à des envois de messages électroniques. La notion de session est (encore) plus floue pour les connexions de type WWW (« World Wide Web ») selon le protocole HTTP : on peut par exemple la définir comme étant la durée de transfert d'une page HTML dans son ensemble (comportant plusieurs objets à transférer) ou d'une suite de pages associées à une même consultation. Les sessions sont générées par la couche application des réseaux et l'ordre de grandeur de leur durée se situe entre quelques minutes et quelques heures.

1.2.2.1.2. Répartition par protocole

Sur l'Internet, au-dessus de la couche réseau IP, les protocoles de transport de loin les plus répandus sont UDP et TCP. Le trafic TCP est largement majoritaire, comme le montre le tableau 2 où l'on donne les fourchettes dans lesquelles s'insèrent la plupart des proportions de trafic UDP/TCP reportées dans la littérature. Il est intéressant de noter que ces valeurs sont relativement stables depuis quelques années (environ 8 ou 9 ans) [McC 00]. Le protocole UDP ne transporte encore que très peu de trafic lié à des applications utilisateurs (les services de Voix sur IP ou de téléchargement audio/vidéo en temps-réel n'ont pas encore réussi leur percée).

D'autres protocoles de transport sont présents dans les observations, mais ne contribuent que pour une proportion négligeable du volume de trafic véhiculé, mesuré en nombre de paquets ou d'octets (en termes de flots, leur poids pourrait monter jusqu'à 1 ou 2% selon la définition utilisée pour identifier les flots) : ICMP (Internet Control Message Protocol), RSVP (Reservation Protocol), GRE (General Routing Encapsulation), SIPP-ESP (SIPP Encap Security Payload) et NHRP (NBMA Next Hop Resolution Protocol). On ne considère généralement pas ces protocoles lors des études de caractérisation de trafic, en particulier celles rapportées ici.

[13] La définition d'une connexion/flux peut être légèrement différente : parfois on intègre également les champs TOS et DSCP. Parfois, on peut revenir à la définition générale : on ne considère donc pas les paquets SYN et FIN comme délimiteurs, mais des périodes d'inactivité, i.e. des périodes pendant lesquelles aucun paquet de la connexion n'est transmis. Dans la suite, nous considèrerons toujours la définition suivante pour une flux, i.e. l'utilisation du quintuplé (adresse source, adresse destination, port source, port destination, protocole) et les délimiteurs SYN et FIN.

	TCP	UDP	Autres
% paquets	85 - 90	10 - 15	négligeable
% octets	94 - 98	2 - 6	négligeable

Tableau 1. Proportions de trafic par protocole de transport

1.2.2.1.3. Répartition par application

Comme cela a déjà été évoqué, il existe des différences significatives entre les trafics d'un réseau académique et d'un réseau commercial. Ce résultat intuitif, même s'il reste un secret de Polichinelle, est assez difficilement accessible de façon mesurable car peu d'opérateurs de réseaux commerciaux publient la composition de leur trafic. Pour combler le déficit en traces disponibles publiquement, dans cette partie, nous nous rabattrons donc sur le seul projet METROPOLIS. Nous présenterons la répartition du trafic par application pour ces deux types de réseaux : d'un côté RENATER, et de l'autre une plaque ADSL de France Télécom, ces deux opérateurs étant des partenaires du projet.

Pour illustrer la répartition du trafic par application sur un réseau académique, nous avons aléatoirement choisi une trace de trafic capturée sur le réseau d'accès du MAN de Jussieu à RENATER. Toutefois, les autres traces capturées sur ce lien montrent une certaine constance en termes de proportion de trafic de chaque application. A noter que la classification applicative a été effectuée en utilisant le logiciel *Traffic Designer* de la société QoSMOS. Ce logiciel utilise pour la classification une technique de « pattern matching » sur les paquets des connexions de façon à reconnaître le protocole applicatif utilisé. Le résultat obtenu est donc tout à fait fiable. En tous cas plus fiable qu'en utilisant une classification à partie des numéros de port de la classification qui sont aujourd'hui de moins en moins significatifs car de nombreuses applications utilisent des ports dynamiques non répertoriés (comme les applications de P2P par exemple), ou encapsulent leur trafic dans les protocoles applicatifs d'autres applications (par exemple les applications de streaming encapsulent souvent leur trafic dans des paquets http pour pouvoir passer les firewalls).

Trafic sur un lien d'un réseau académique

Les figures 1 et 2 présentent les différentes répartitions qui sont le résultat du processus de classification du trafic par application. La figure 1 présente pour l'ensemble des applications la quantité de trafic total en octets, paquets et flux. La même chose est présentée sur la figure 2 mais en ne considérant que les familles d'applications. Nous rappelons qu'une famille d'application est constituée de toutes les applications qui ont le même objectif : par exemple, Kazaa et E-donkey appartiennent à la même famille P2P.

Les figures 3 et 4 représentent l'évolution du trafic au cours du temps en octets / s à la fois pour les différentes applications et leurs familles associées.

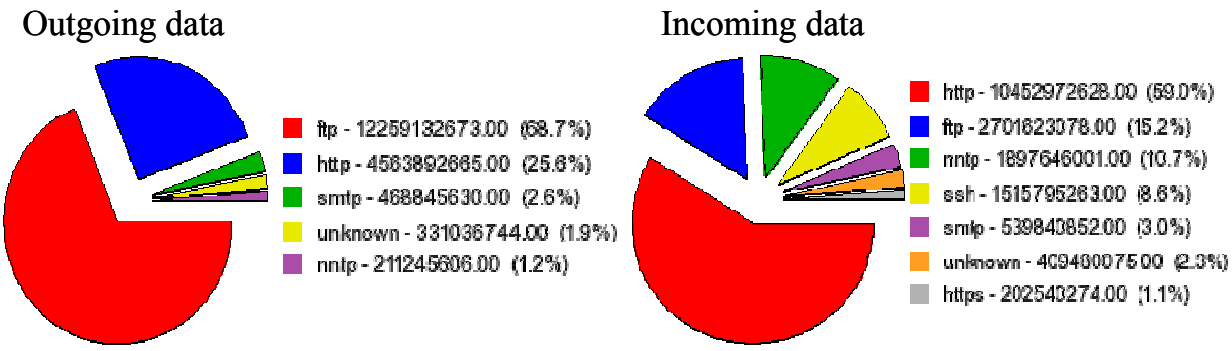

Figure 1 : Quantité globale de données par application (données sortantes et entrantes). Ces graphiques représentent la distribution du trafic par application en octets

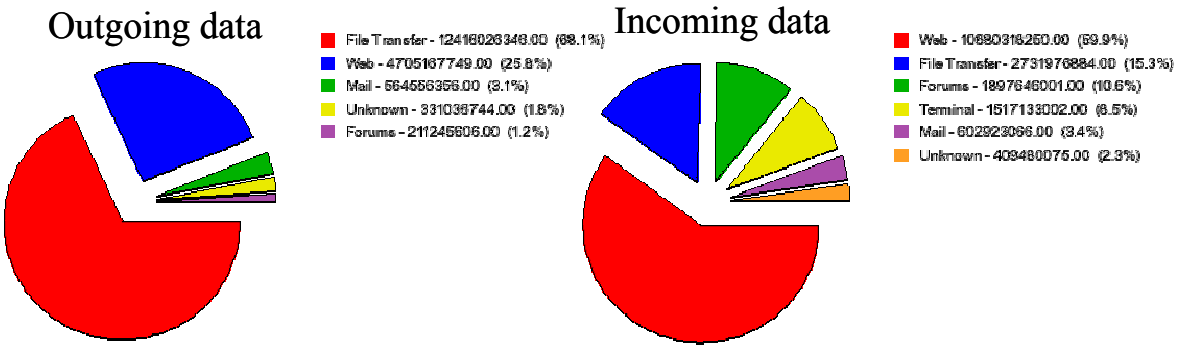

Figure 2 : Quantité globale de données par famille d'applications (données sortantes et entrantes). Ces graphiques représentent la distribution du trafic par application en octets

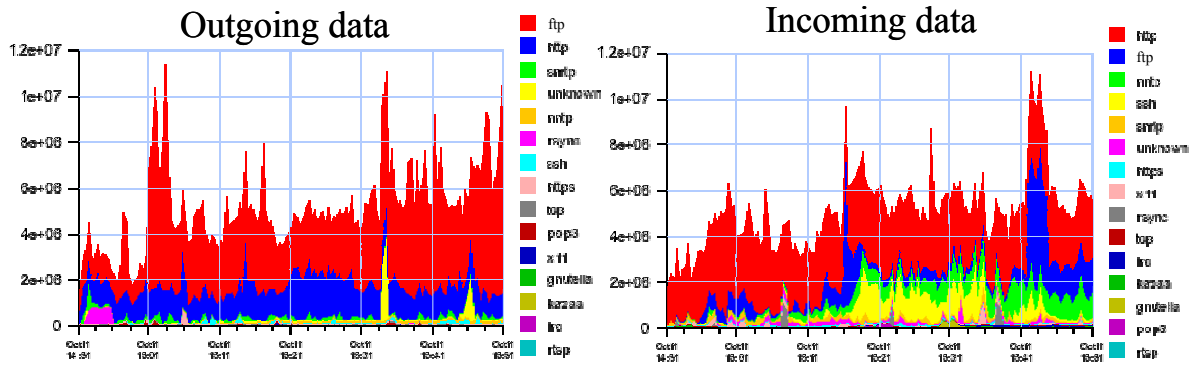

Figure 3 : Répartition du débit par application en octets / s (données entrantes et sortantes). Ces différentes répartitions représentent l'évolution du trafic octet au cours du temps pour les principales applications présentes dans le trafic de Jussieu -- les applications sont classées dans le même ordre sur la légende et dans le graphique

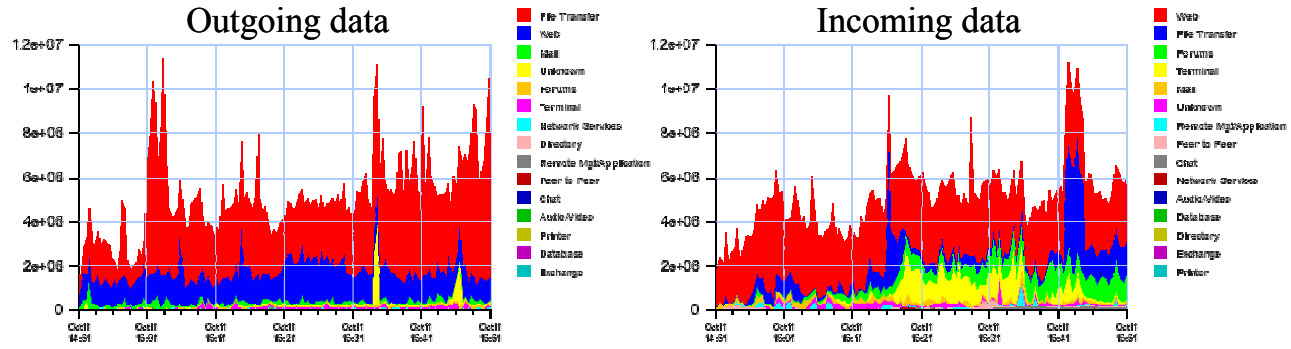

Figure 4 : Répartition du débit par famille d'applications en octets / s (données entrantes et sortantes). Ces différentes répartitions représentent l'évolution du trafic octet au cours du temps pour les principales familles d'applications présentes dans le trafic de Jussieu -- les applications sont classées dans le même ordre sur la légende et dans le graphique

Trafic d'une plaque ADSL de France Télécom

Nous présentons maintenant le même type d'analyse que celle menée pour les traces de Jussieu, mais cette fois sur une trace France Télécom collectée sur une plaque ADSL parisienne.

Les figures 5 et 6 illustrent la contribution en volume total des différentes applications et familles d'applications définies dans la section précédente. Il apparait clairement sur ces résultats que les applications P2P ont une contribution significative sur la charge totale. C'est la principale différence entre un trafic académique et un réseau commercial. Dans un trafic de campus, comme nous l'avons observé sur les traces du réseau de Jussieu, le trafic P2P est pratiquement inexistant. Dans un réseau commercial, le P2P a un impact beaucoup plus important.

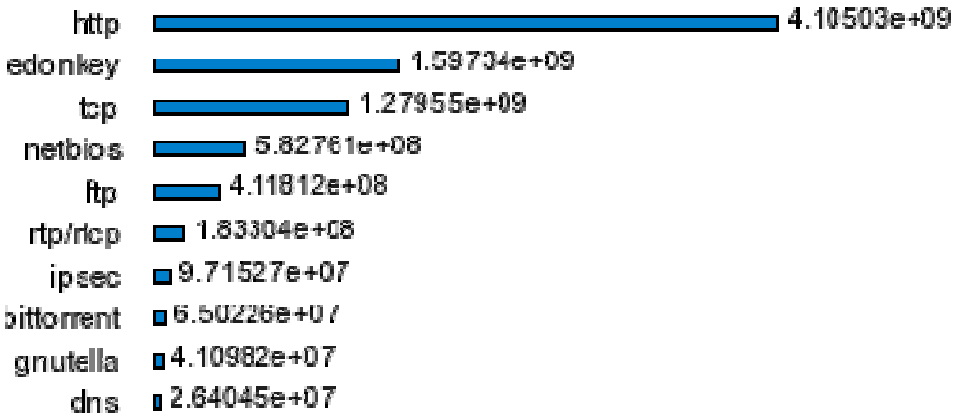

Figure 5 : Quantité total de données par application (données entrantes). Cet histogramme représente la distribution du trafic par application en octets

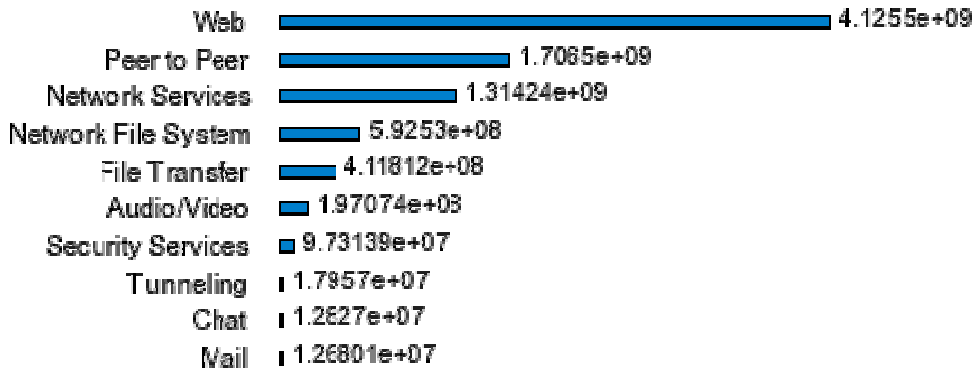

Figure 6 : Quantité totale de données par famille d'applications (données entrantes). Cet histogramme représente la distribution du trafic par familles d'applications en octets

Les figures 7 et 8 représentent le débit pour les applications et les familles d'applications. Ces figures montrent que le débit global est stationnaire dans l'ensemble ; il n'y a pas une déviation évidente dans le processus du débit. On peut aussi observer que la proportion de P2P est en augmentation ce qui implique que sa contribution à la charge globale du réseau devient de plus en plus significative. Plusieurs traces de trafic montrent que le trafic P2P domine en fin de journée (i.e. entre 21H00 et 00H00).

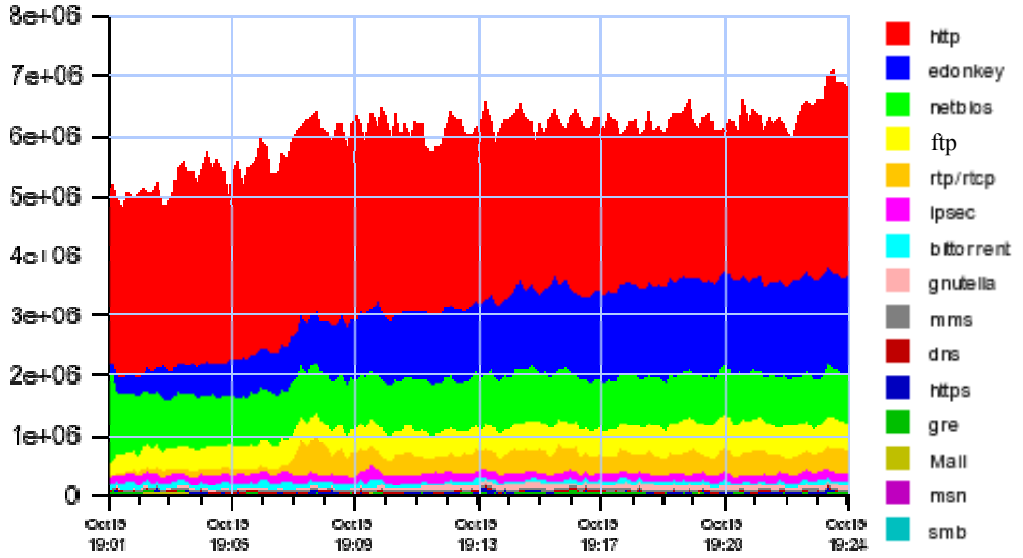

Figure 7 : Répartition du débit par application en octets / s (données entrantes). Cette répartition représente l'évolution du trafic octet au cours du temps en fonction des principales applications présentes dans le trafic France Télécom – les applications sont classées dans le même ordre sur la légende et dans le graphique

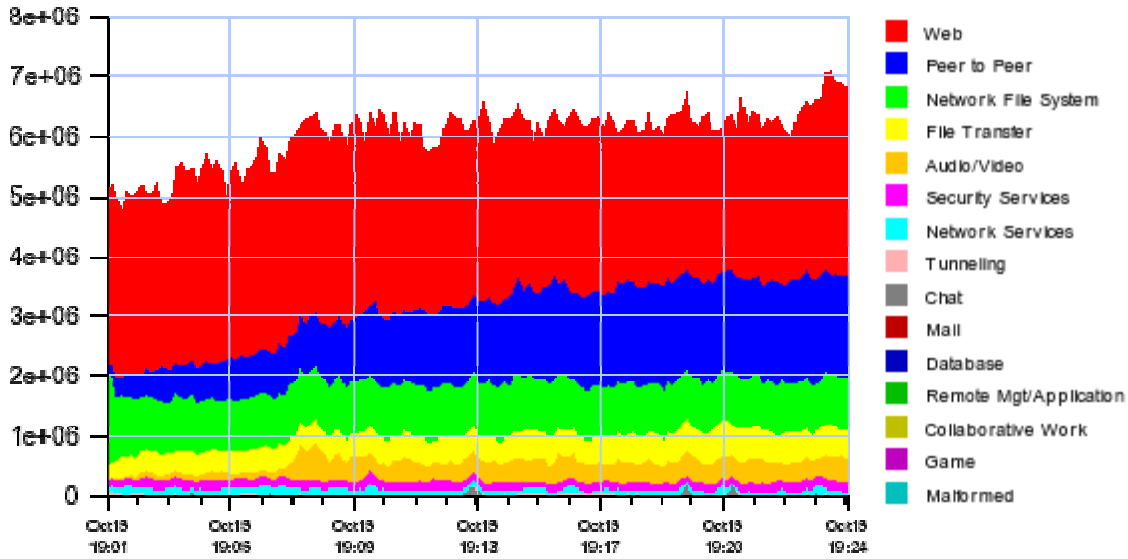

Figure 8 : Répartition du débit par famille d'applications en octets / s (données entrantes). Cette répartition représente l'évolution du trafic d'octets au cours du temps en fonction des principales familles d'applications présentes dans le trafic France Télécom -- les applications sont classées dans le même ordre sur la légende et dans le graphique

1.2.2.2. Modélisation des processus

1.2.2.2.1. Introduction sur l'auto-similarité

Les premières études métrologiques sur le trafic Internet menées partout dans le monde ont globalement montré que ce dernier est particulièrement instable, à cause des propriétés d'auto-similarité et de dépendance à long terme appelée aussi LRD [Lel 93]. Il est aussi montré que la distribution à queue lourde est très impliquée dans ces propriétés [Wil 98]. Avant de détailler dans la suite de ce chapitre toutes ces caractéristiques du trafic Internet et d'en analyser les causes, il est nécessaire d'introduire les notions mathématiques associées aux différents comportements observés dans le réseau.

Fonction d'auto-corrélation

Avant de présenter cette fonction mathématique, il faut définir les notions d'indépendance et de corrélation :

- X, Y sont deux v.a. indépendantes ssi

$$P(X<x \cap Y<y) = P(X<x).P(Y<y)$$

- X, Y sont deux v.a. décorrélées ssi

$$E(XY)=E(X).E(Y)$$

En pratique, on dispose de N mesures. La fonction d'auto-covariance se calcule comme la fonction de covariance entre deux séries. La seconde série est ici la même que la première mais décalée d'un nombre K d'éléments. La fonction d'auto-covariance C_K s'écrit alors :

$$C_K = \sum_{k=0}^{K} (\frac{1}{N-k} \sum_{t=0}^{N-k} (x_t - \bar{x})(x_{t+k} - \bar{x})$$

où $\bar{x}$ représente la moyenne de la série de points.

Processus à dépendance longue (LRD)

Un processus à dépendance longue ou à mémoire longue signifie que la dépendance entre deux variables du processus ne diminue pas trop rapidement avec l'éloignement temporel. La définition mathématique introduite par [Cox 84] est présentée ci-dessous :

Soit $X=X_t$ un processus stochastique (à covariance) stationnaire à temps discret, on dit que X_t est à mémoire longue s'il satisfait les propriétés suivantes :

- $\sum_{t=0}^{\infty} \rho(t) = \infty$ (ρ est la fonction d'auto-corrélation),
- La densité spectrale S est singulière[14] à l'origine,
- $m.varX^m \rightarrow \infty$ quand $m \rightarrow \infty$

Un processus à dépendance longue possède la propriété suivante :

$\rho(t) \xrightarrow{t \to \infty} ct^{-\beta}$ $O<\beta<1$ (ρ est la fonction d'auto-corrélation).

Ainsi la fonction d'auto-corrélation décroît hyperboliquement.

La dépendance à long terme a été découverte en premier par Hurst qui la définit comme un processus ayant une fonction d'auto-corrélation non sommable (première propriété) et caractérisée par un paramètre *H*, défini par la formule $H = 1 - \frac{\beta}{2}$ [15], et appelé paramètre de Hurst. En 1993, Leland, Taqqu, Willinger et Wilson ont mis en évidence la LRD pour des séries temporelles de paquets Ethernet. Depuis, une multitude de travaux et d'articles ont traité de la dépendance à long terme du trafic Internet (voir [Wil 98], [Ver 00b], [Par 96] et [Dow 01]). Nous y reviendrons dans les sections suivantes.

Distribution à décroissance lente

Plusieurs travaux de recherches (voir [Wil 98], [Ver 00b], [Par 96] et [Dow 01]) ont démontré que la distribution à queue lourde pour certaines caractéristiques du trafic (distribution des tailles de fichiers, des durées de transfert…) est l'une des principales causes de LRD du trafic Internet.

Une distribution est à queue lourde si sa fonction de distribution a la propriété suivante :

---

[14] Une fonction *f* est dite singulière en un point *a* si elle n'est pas explicitement définie en ce point (à cause par exemple d'une division par zéro si $x = a$ ou dans le cas d'une fonction définie sur un ensemble topologiquement ouvert, d'un point a qui est à la frontière de l'ensemble de définition de la fonction - C'est le cas de la fonction *ln(x)* lorsque $x=0$).

[15] β étant le coefficient de la fonction d'auto-corrélation [Ber 94].

$$P[X > x] \xrightarrow{t \to \infty} x^{-\alpha}, \alpha \in]0,2[$$

En d'autres termes, la forme asymptotique de la distribution à queue lourde suit une loi exponentielle avec α inférieur à 2.

On l'appelle « à queue lourde » car, comparée à la distribution exponentielle et la distribution normale, une variable aléatoire qui suit une distribution à queue lourde peut montrer pour des très grandes valeurs de *X* une probabilité *P[X]* supérieure à celle obtenue pour une distribution exponentielle équivalente. Cette variable a une variance infinie si $\alpha \in]0, 2[$ et une moyenne infinie si $\alpha \in]0, 1[$.

Processus auto-similaire

L'auto-similarité est une notion très importante dans la caractérisation du trafic Internet. En effet, la nature du trafic de données en général, celui d'Internet plus particulièrement, présente un aspect auto-similaire. Il s'agit de la manifestation du phénomène suivant : la structure des variations d'amplitude du signal analysé (par exemple le nombre d'octets transférés par unité de temps) se reproduit de manière similaire quelle que soit la finesse temporelle avec laquelle il est représenté. Ainsi, le comportement d'un trafic auto-similaire est à l'opposé de celui d'un trafic poissonnien, dont les variations d'amplitude sont filtrées au fur et à mesure que l'on augmente la taille de la fenêtre d'observation [Pax 95]. Il existe différentes définitions mathématiques de l'auto-similarité. La suivante concerne les processus à temps continu :

Un processus *X(t)* est dit auto-similaire de paramètre $H \in R$, si et seulement si pour tout $c > 0$, $c^H X(t)$ et *X(ct)* possèdent les mêmes distributions jointes à tous les ordres. Ainsi pour tout entier $n, t_1, \ldots, t_n, x_1, \ldots, x_n$:

$$P(X(t_1) \leq x_1, \ldots, X(t_n) \leq x_n) = P(X(ct_1) \leq c^H x_1, \ldots, X(ct_n) \leq c^H x_n)$$

Cette définition signifie que si l'on modifie l'échelle sur laquelle on observe le processus par un facteur positif *c* et que l'on « zoome » le même processus par ce facteur élevé à la puissance *H*, alors l'allure des deux processus obtenus est la même. Par conséquent, il n'y a pas une stabilisation vers une moyenne comme dans le cas du processus de Poisson.

Auto-similarité et trafic Internet

Une monographie entière [Par 00] est consacrée à la modélisation du phénomène d'auto-similarité du trafic dans les réseaux de données et à son impact sur l'évaluation des performances. Y figurent aussi bien des chapitres sur la description et la simulation des caractéristiques auto-similaires du trafic (streaming vidéo, connections TCP, …) et sur leur analyse au moyen de techniques sophistiquées telles que la transformée en ondelettes, que sur leur impact sur les modèles de performance basés sur les files d'attente et sur l'ingénierie des réseaux multi-services offrant de la Qualité de Service (dimensionnement, contrôle de congestion, etc.). Ce livre constitue une excellente et très complète source d'informations et de références sur ce thème ; nous donnons explicitement certains de ses chapitres dans la bibliographie figurant en fin de document. On pourra consulter aussi [Wil 96] pour une bibliographie exhaustive (à la date de parution) sur le sujet.

Les chercheurs d'AT&T ont publié de nombreux travaux sur l'auto-similarité du trafic [Lel 94], [Wil 97]. Les articles [Fel 98] et [Fel 98a] sont particulièrement intéressants car – outre la présentation de nombreux résultats mettant en avant ce phénomène – les auteurs insistent sur

la nécessité de développer un modèle structurel d'analyse du trafic. Ce type d'approche permet de mieux cerner les aspects dynamiques (processus des connexions TCP au sein des sessions applicatives, processus paquets, …) du trafic de données transporté par les réseaux longue distance (" Wide Area Networks "), et de fournir quelques interprétations " physiques " des phénomènes observés (relations entre auto-similarité et lois de probabilité à décroissance lente, par exemple). L'analyse des phénomènes liés aux échelles de temps est effectuée à l'aide d'une technique originale fondée sur la transformée en ondelettes [Abr 98] : les séries temporelles, telles que le nombre de paquets transmis par unité de temps par exemple, y sont analysées en termes d'un spectre d'énergie établi en fonction d'un facteur d'échelle temporelle.

1.2.2.2.2. Trafic au niveau paquets

Une caractéristique générale du trafic de paquets est de se présenter sous forme de rafales, ce qui est inhérent à ce mode de commutation (voir [Rob 96] et [Tra 00] et leurs nombreuses références). Il en résulte une extrême variabilité à toutes les échelles de temps des processus observés relatifs aux paquets : intervalle entre paquets successifs, nombre de paquets ou d'octets transférés par unité de temps, etc. Ceci se traduit mathématiquement par un comportement auto-similaire, voire multi-fractal selon les échelles de temps, des variables de trafic, un phénomène observé dans toutes les publications à ce sujet. Ce comportement se caractérise notamment par une décroissance lente, par exemple sous forme de loi puissance [Hey 98], de la fonction d'auto-corrélation du nombre de paquets, ou du nombre d'octets, transférés par unité de temps (typiquement 100 ms) : les processus auto-similaires sont des cas particuliers des processus à dépendance à long terme (LRD).

Concernant le trafic de type streaming, les services liés à la vidéo sont appelés à un fort développement dans le futur : vidéoconférence, téléchargements en temps réel (Video on Demand). La caractéristique LRD a été identifiée dans de nombreuses publications concernant le transfert de séquences vidéo à débit variable (VBR selon la terminologie ATM) [Ber 95], probablement due à la variabilité des paramètres de transmission liés au codage des trames (MPEG, p. ex.), à la dynamique des images, etc. On pourra consulter [Hey 00] pour une revue complète sur les caractéristiques de ce trafic et sur leur impact sur les modèles de performance. Il y est en particulier noté que la LRD n'a pas forcément une influence déterminante, contrairement aux corrélations à court terme, sur le comportement des files d'attente des routeurs.

Dans le cas particulier de la téléphonie sur IP, on pourrait supposer que les paquets sont de longueur et d'intervalle inter-arrivées constantes au sein d'une même communication. Ces paramètres fixes sont le reflet, après encodage et compression à la source, du débit constant des communications téléphoniques. Cependant, ces hypothèses semblent quelque peu simplificatrices, d'une part à cause du phénomène de gigue de transfert si l'on se place sur un lien éloigné du routeur origine, d'autre part en raison de la diversité potentielle des paramètres de codage de la voix. Quoi qu'il en soit, et il en est de même pour le trafic vidéo, nous ne disposons pratiquement pas à l'heure actuelle d'observations concrètes de ce type de trafic sur réseau réel.

Concernant le trafic de type élastique, l'identification du processus des paquets tel qu'il est offert au réseau est particulièrement délicate. En effet, les dispositifs de correction d'erreur et de perte génèrent la retransmission de paquets supplémentaires et les mécanismes de contrôle de flux (TCP notamment) régulent les débits de transmission [Bla 92]. Les analyses de trafic

doivent donc se contenter des données de trafic effectivement mesurées sur des liens, compte tenu de ces retransmissions et régulations.

Le caractère auto-similaire du trafic TCP a été largement étudié. En complément de ce qui a été dit au paragraphe précédent, notons les tentatives d'explication avancées : aux échelles de temps supérieures à un délai de transmission typique (RTT, de l'ordre de 100 ms), le comportement auto-similaire (ou mono-fractal) serait dû à l'extrême variabilité de la taille des documents transférés (la loi de distribution est de type « heavy-tailed », telle la loi de Pareto), voir le paragraphe 1.2.2.2.3 sur la caractérisation des flots ; tandis que les caractéristiques multi-fractales aux échelles de temps inférieures seraient provoquées par les mécanismes de contrôle de congestion du protocole TCP [Fel 98 et 98a]. Effectuant une analyse des phénomènes d'échelle segmentée par composante de trafic (protocole de transport ou application), [Mol 00] montre que HTTP et FTP sont les principales applications contribuant, par leur extrême variabilité, aux propriétés de LRD détectées au niveau des paquets IP.

Tout ce qui précède concerne le processus d'arrivée des paquets. La loi de distribution des tailles de paquet, quant à elle, est difficilement modélisable statistiquement car elle possède de fortes composantes discrètes correspondant à certaines tailles caractéristiques (messages de gestion, accusés de réception, etc.) [Tho 97]. La distribution des tailles de paquet peut bien sûr varier selon le lieu et l'heure d'observation, mais elle est surtout sensible généralement au sens de transmission du trafic : la plupart des liens IP présentent une dissymétrie de répartition serveurs/usagers entre les deux nœuds qu'il relie (c'est le cas p. ex. de liens internationaux Europe – Etats-Unis, de liens de collecte du trafic grand public vers le cœur de réseau, etc.). Le sens serveur vers usager a alors tendance à comporter des paquets de plus grande taille, liés au transfert des données demandées, par rapport au sens usager vers serveur, où le trafic est essentiellement composé de requêtes et d'informations protocolaires relatives à l'établissement des communications (accusés de réception, début et fin de connexion TCP…).

On observe ainsi trois modes déterministes principaux, qui se superposent bien entendu à une certaine distribution continue de poids assez variable. Les paquets de faible taille (40 octets ou guère plus), essentiellement composés des en-têtes TCP (ou UDP) et IP, sont produits par les protocoles et par de courtes requêtes (telles les commandes de Telnet générant des paquets de 1 caractère) ; ils constituent globalement presque la moitié des paquets observés, et jusqu'à 70 ou 80% des paquets dans le sens usager vers serveur. Les paquets de taille moyenne (typiquement 552 ou 576 octets) sont produits par certaines implémentations de TCP. Les paquets de grande taille (1500 octets) correspondent à la taille maximum (MTU) autorisée par la couche Ethernet et généralement reconnue par les protocoles de transport. Ces deux derniers modes comptent chacun pour environ 10 à 20% de la totalité des paquets.

1.2.2.2.3. Trafic au niveau flots

De nombreuses études ont été publiées récemment sur la modélisation du trafic au niveau des flots, motivées par les nombreuses perspectives d'application offertes par la considération de cette entité de trafic. En premier lieu, comme souligné plus haut, l'analyse des performances du trafic et l'inférence qui en découle de méthodes de dimensionnement des ressources s'effectuent plus aisément, et de manière plus adéquate, à ce niveau. Par ailleurs, les différents schémas d'architectures de routage, de « traffic engineering » (MPLS, routage orienté QoS, etc.), voire de fourniture de services différenciés (IntServ, DiffServ), qui ont été proposés ces dernières années de manière quelque peu « foisonnante » dans la mouvance de l'IETF,

prennent en compte également la notion de flots, éventuellement selon des niveaux d'agrégation très variables.

Une comparaison détaillée est malaisée à effectuer entre les différents résultats produits, en raison des définitions diverses accordées à la notion de flots : micro-flots selon la définition ci-dessus, connexions TCP, documents Web, etc.). Cependant, quelques points communs importants peuvent être dégagés dans l'ensemble : la non conformité du processus des arrivées de flot à un processus de Poisson, et le comportement général de décroissance lente des distributions statistiques de longueur de flot. A noter que la plupart des publications sur ce sujet ne traitent que des caractéristiques de flots TCP, à l'exception de [Oli 01] qui montre que les modèles de représentation des processus de flots sont similaires pour UDP et TCP, notamment pour ce qui concerne le processus d'arrivée. Cependant, ce dernier résultat est à tempérer par le fait que très peu de véritables flux de trafic temps-réel circulent à l'heure actuelle sur les réseaux IP.

Tous les résultats statistiques produits dans la littérature mettent en évidence des lois de distribution à décroissance lente (« heavy-tailed ») dès que l'on s'intéresse à un paramètre lié à la taille, au volume, à la durée, …, d'un objet à transférer sur un réseau de données (voir p. ex. [Bol 99], [Cha 00], [Dow 01], [Mah 97], [Nab 98], [Oli 01], [Pax 94a] pour le trafic IP). Ce phénomène de décroissance lente signifie que la probabilité d'obtenir des très grandes valeurs de la variable aléatoire est asymptotiquement beaucoup moins faible que pour une loi de type exponentiel. Les lois de probabilité couramment utilisées pour modéliser un tel comportement sont la loi de Pareto et la loi log-normale. Si l'on entend littéralement par « décroissance lente » une décroissance équivalente (selon une définition mathématique que l'on ne précisera pas ici) à une fonction puissance, la loi log-normale n'est pas une loi à décroissance lente [Pax 95], elle est seulement à décroissance sous-exponentielle. De même, la loi de Weibull est souvent assimilée à une loi à décroissance lente alors qu'il s'agit d'une généralisation (de même que la loi Gamma) de la loi exponentielle ; elle peut bien sûr être à décroissance plus lente que l'exponentielle en fonction des valeurs prises par l'un de ses paramètres.

La loi de Pareto est l'archétype de la loi à décroissance lente puisque sa distribution (cumulative complémentaire) est proportionnelle à $x^{-\alpha}$, $\alpha > 0$. Pour $1 < \alpha \leq 2$, la valeur moyenne est finie, mais la variance ne l'est pas. Pour $0 < \alpha \leq 1$, la valeur moyenne elle-même devient infinie. Ce comportement est significatif d'une très grande variabilité de la variable aléatoire considérée : dans le cas de la taille des documents des sessions Web, de très nombreux documents de taille modeste coexistent avec des documents très volumineux, en nombre plus faible mais non négligeable. C'est cette extrême variabilité de la taille des documents qui semble être à l'origine des phénomènes de dépendance à long terme observés aux grandes échelles de temps (typiquement supérieures à 1 s), du moins à propos du trafic de type Web ou de transfert de fichiers [Cro 97], [Par 96].

Dans la plupart des cas, seule la queue de distribution de la loi des longueurs de flot est identifiée comme étant à décroissance lente ; la loi de Pareto ne fournit en général pas un bon modèle de représentation de l'ensemble de la distribution, le corps de la distribution étant par exemple bien modélisé par une loi log-normale [Nab 98], [Oli 01]. Circonstance qui pourrait inciter à proposer de modéliser l'ensemble de la distribution par des mélanges de loi (log-normal/Pareto [Jen 00] ou mélange de plusieurs lois log-normales [Bol 99]), quoi que l'on puisse douter de l'intérêt pratique de disposer de tels modèles de représentation, certainement peu utilisables analytiquement et peu économes en nombre de paramètres, pour mener des

études ultérieures sur la performance du trafic. A l'opposé de ce caractère généralement multi-modal des distributions, on observe dans [Oli 01] un ajustement remarquablement bon (du moins visuellement, mais néanmoins selon deux modes de représentation, en échelle linéaire et en échelle logarithmique) de l'ensemble de la distribution par une loi de Pareto dès lors que l'on traite des longueurs de flots TCP mesurées en nombre de paquets, et ce à partir de diverses campagnes d'observation, aussi bien sur un réseau dorsal que sur un réseau d'accès haut débit ADSL. Dans tous les cas où il est estimé, le paramètre de puissance α de la loi de Pareto se situe entre 1 et 2, voire proche de 1, signe d'extrême variabilité comme souligné plus haut.

Les travaux publiés sont un peu moins nombreux concernant la caractérisation du processus d'arrivée des flots, malgré le fait que la plupart des modèles de performance au niveau flot supposent qu'il s'agit d'un processus de Poisson et demandent donc à être validés. Dans le cadre d'un modèle hiérarchique sessions/flots [Bon 01] où les flots correspondent à des demandes de transfert successives de documents (pages Web) ou de fractions de documents en parallèle ou en série (fichiers ou objets d'une page Web) au sein d'une même session d'un utilisateur, il est logique de s'attendre à des inter-dépendances dans le processus temporel d'apparition des flots, lequel devra alors s'écarter sensiblement du modèle Poissonnien. C'est ce que l'on vérifie expérimentalement, à l'exception de l'étude commentée au paragraphe suivant. La distribution statistique des intervalles inter-arrivée de flots est remarquablement bien représentée (y compris au vu de tests numériques d'ajustement) par une loi de Weibull [Fel 00], [Oli 01] ou par une loi Gamma (toutes deux des extensions à deux paramètres de la distribution exponentielle, mais la dernière étant moins usitée dans ce domaine). Dans la seconde de ces deux études, les flots sont des micro-flots TCP ou UDP, tandis que dans la première, ce sont des connexions TCP (identifiées par les informations de début et de fin fournies par ce protocole) ; on en déduit une certaine robustesse des résultats obtenus. Pour compléter l'étude au second ordre, des estimations de la fonction d'auto-corrélation de l'intervalle inter-arrivée mettent en évidence une corrélation persistante dans le temps (sur une ou quelques dizaines de seconde), quoi que de niveau assez faible (de l'ordre de 0,1). Poussant plus loin le caractère non Markovien du processus d'arrivée des flots, [Fel 00] met en évidence une composante de LRD concernant le nombre d'arrivées de connexions TCP par unité de temps, sur toutes les échelles de temps au delà de 1 s. Les auteurs notent par ailleurs le fait intéressant que ce phénomène est apparu graduellement au cours de ces dernières années, au fur et à mesure de l'importance croissante du trafic Web (protocole HTTP).

Se différenciant des résultats précédents, l'étude [Nab 98] montre que la loi log-normale fournit (de même que pour la statistique des longueurs) la meilleure représentation de la distribution des intervalles inter-arrivées de documents si l'on traite l'ensemble des données recueillies sur plusieurs jours consécutifs (typiquement une semaine). En se limitant à des périodes chargées de 2 heures où les composantes non stationnaires (profils journaliers déterministes) sont moins présentes, la meilleure représentation est alors fournie par la loi exponentielle. Ce résultat est surprenant, d'autant qu'il repose sur une analyse descriptive très complète des statistiques du trafic Web (jeux de données sur plusieurs semaines, en provenance de 4 sites différents). Il peut néanmoins s'expliquer par différents facteurs : les flots sont en fait des requêtes adressées vers des sites Web ; parmi les lois testées, seule la loi exponentielle n'est pas à caractère de décroissance sous-exponentielle.

En tout état de cause, il semble que les modèles de performance du trafic IP doivent tenir compte du caractère non Poissonnien sensiblement marqué du processus d'arrivée des flots, soit en intégrant explicitement, de manière exogène, les caractéristiques de représentation du

premier ordre, voire du second, soit en développant une approche de plus haut niveau prenant en compte la structuration hiérarchique des flots en sessions comme le propose [Bon 01].
A noter toutefois qu'un premier article [Cao 01], à l'origine de nombreux débats dans la communauté Internet et peut être à la base d'une nouvelle évolution dans l'approche choisie pour modéliser le trafic, défend une théorie opposée à celle de l'auto-similarité. En effet, l'étude présentée montre que plus la quantité de trafic augmente, plus le trafic devient régulier, avec des distributions d'arrivées exponentielles (et plus sous-exponentielles) et une dépendance qui diminue (évaluée à l'aide de méthodes entropiques). Le modèle de trafic ne serait ainsi plus auto-similaire à partir du moment où une certaine quantité importante de paquets et de flux s'entrelacent sur un lien haut débit.

1.2.2.2.4. Trafic au niveau sessions

Le processus des demandes de communication, qu'elles soient de type streaming ou de type élastique, a toutes les raisons de pouvoir être considéré comme Poissonnien (dans la mesure où l'on peut admettre que la population source est de taille quasi-infinie). C'est l'un des principaux « invariants » communément reconnus en modélisation du trafic Internet [Flo 01]. En effet, au niveau des sessions utilisateurs, le processus d'arrivée résulte de la superposition d'un nombre élevé de demandes élémentaires indépendantes entre elles (à opposer à la dépendance inter-flot au sein d'une même session).

Des campagnes d'observation remontant au début de la précédente décennie, époque où le trafic Internet était essentiellement dominé par les applications FTP, Telnet ou SMTP, ont montré que les arrivées de session obéissaient correctement à un processus de Poisson [Pax 95], bien que ces diverses applications aient des modes de fonctionnement très différents (au niveau des connexions TCP générées par exemple). Dans le but de caractériser les sessions Web, des observations indirectes ont été effectuées [Fel 98] par la collecte d'informations relatives aux appels par modem à destination d'un ISP : instants d'arrivée, taille et durée des appels. Bien que ces demandes de connexion ne contiennent pas uniquement des sessions Web, ces données ont été utilisées pour tenter de caractériser les processus liés à ces dernières. L'analyse, uniquement qualitative, montre que le processus d'arrivées est cohérent avec un processus poissonnien, du moins avec un processus de renouvellement (processus pour lequel les intervalles inter-arrivées sont indépendamment et identiquement distribués). En fait, peu de travaux ont eu pour objet de valider rigoureusement le caractère poissonnien du processus d'arrivée des sessions, probablement en raison du caractère naturel, presque « évident », de l'hypothèse, mais aussi certainement à cause de la difficulté d'identifier des sessions générées par les utilisateurs à partir de traces réelles. Citons seulement l'article [Nuz 00] qui obtient sur des données collectées aux Bell Labs (donc sur un réseau local) un excellent comportement, aux premier et second ordres, du modèle de représentation des arrivées de session par un processus de Poisson.

La loi des durées (ou des longueurs), quant à elle, possède des caractéristiques de distribution à décroissance lente, quoiqu'elle soit difficile à identifier (comme indiqué plus haut). Que ce soit dans [Pax 95] ou dans [Fel 98], donc avec ou sans présence prépondérante des sessions Web, la loi des durées de session (ou de taille exprimée en koctets) possède une queue de distribution caractéristique d'une loi de Pareto de moyenne finie, mais de variance infinie significative d'une grande variabilité. D'un point de vue qualitatif, les paramètres quantitatifs des modèles de représentation étant bien entendu différents, les caractéristiques statistiques des durées de session sont dans l'ensemble similaires à celles des longueurs de flot.

1.3. Conclusion

Ce premier chapitre a dressé un état des besoins en QoS dans l'Internet au vu de ses usages actuels de plus en plus variés. Il a notamment positionné la contribution de ces travaux dans le cadre de l'Internet global, sans restriction de taille ou de service. De fait, l'objectif avoué est d'arriver à satisfaire tous les besoins des utilisateurs et applications de l'Internet, sans pour autant renier les principes de base de ses techniques de communication. En particulier, la direction de recherche choisie respecte le principe de fonctionnement de l'architecture TCP/IP actuelle qui consiste à s'adapter aux ressources disponibles et à les exploiter – de façon dynamique – au mieux. Pour améliorer ce principe, la contribution introduite et défendue dans ce mémoire consiste à développer et utiliser au maximum des outils de métrologie qui permette d'avoir une vision très précise de l'état d'un réseau et de son trafic, et ce à tout moment.
Ce chapitre a donc également dressé un état de l'art des techniques et avancées en métrologie, et présenté les caractéristiques du trafic, notamment la répartition du trafic par application, ainsi que les propriétés mathématiques du trafic mises en évidence lors des tentatives de modélisation qui ont été conduites par les premiers projets de métrologie. Les exemples présentés dans ce chapitre sont pour la plupart issus du projet Métropolis, avec notamment des traces issus du réseau Renater et de plaques ADSL du réseau de France Télécom en France.

2. Eléments de contribution

Cette seconde partie de ce mémoire décrit les principales contributions de mon activité de recherche de 2001 à aujourd'hui, avec également quelques références aux travaux que j'ai menés en 2000 alors que j'effectuais une mobilité au sein des laboratoires Sprint ATL. Toute cette contribution a pour dénominateur commun l'intégration d'outils de métrologie dans le processus de recherche en réseaux. L'objectif, comme énoncé dans la partie 1.1.2, est de montrer que la mesure et la supervision du réseau et de son trafic permettent de mettre en œuvre des techniques d'adaptation aux conditions du réseau pour améliorer le niveau de performance et la QoS des réseaux IP.
Aussi, la contribution présentée va se décomposer en 4 parties :

- la première traite de la ***mise en œuvre d'équipements et d'outils de métrologie*** en périphérie de Renater, tâche indispensable pour acquérir les connaissances de base sur le trafic par exemple ;
- la seconde étudie les ***caractéristiques du trafic***, et notamment montre combien les modèles traditionnels issus des télécoms – comme Poisson ou Markov – sont éloignés de la réalité ;
- la troisième partie, qui utilise les travaux précédents de caractérisation du trafic, propose un système de ***métrologie globale*** du réseau de façon à ce que toutes les entités du réseau soient au courant de l'état du réseau en temps réel. A partir de cette connaissance, nous montrons sur un exemple – un mécanisme de contrôle de congestion – les capacités et bénéfices que l'on peut tirer d'un système adaptatif aux conditions des réseaux ;
- Enfin, la dernière partie, utilise les résultats de caractérisation du trafic Internet pour proposer un mode de ***simulation / émulation de scénarios réalistes***. Le but est de pouvoir reproduire des conditions de trafic réalistes pour arriver à des résultats de simulation ou d'émulation qui soient proches de la réalité (ce qui n'est pas le cas aujourd'hui lorsque l'on utilise des modèles de trafic traditionnels issus du monde des télécoms et pour lesquels il a été montré dans la partie 2 qu'ils ne s'appliquaient pas au trafic Internet actuel). Nous proposons donc une méthode de rejeu de traces de trafic et montrons que le résultat est statistiquement très proche de la réalité. D'ailleurs ce mode de génération de trafic réaliste a été utilisé dans toutes nos expériences, que ce soit en simulation ou en émulation, et notamment dans les travaux présenté dans la partie 3.

2.1. Instrumentation sur Renater

Depuis que METROPOLIS a commencé, et encore aujourd'hui, le problème crucial des chercheurs en réseau est de disposer de traces de trafic à étudier et analyser, et / ou de pouvoir en capturer à volonté. Une des principales contributions de METROPOLIS a donc été de mettre en place sur les réseaux RENATER, VTHD et de France Télécom des équipements de mesure et de capture de trafic. J'étais en charge dans METROPOLIS de conduire la mise en place des équipements de mesure passive sur RENATER. Je suis toujours chargé de cette tâche dans le projet MétroSec, qui continue d'exploiter et étend l'infrastructure mise en place dans le cadre de METROPOLIS. La suite décrit la conception, la validation et la mise en place de cette infrastructure de mesure en fonction des objectifs et besoins.

Naturellement, les types des informations qui sont collectées peuvent être de natures très diverses, allant de quelques statistiques sur la quantité de trafic qui passe en ce point (vision macroscopique du trafic) jusqu'à la collecte d'une trace d'information de tous les événements se produisant sur le réseau, c'est-à-dire garder une trace du passage de tous les

paquets individuellement (vision microscopique du trafic). Le type d'informations collectées a une influence capitale sur le mode d'analyse qui peut être réalisé. Dans le premier cas, les analyses sur quelques paramètres précis peuvent se faire en temps-réel et permettre des réactions très rapides aux événements observés. Dans le second cas, en revanche, l'analyse ne pourra se faire qu'a posteriori, et permettra des analyses en temps différé, en théorie sans limite de complexité. Dans le cadre de METROPOLIS qui initiait cette thématique de recherche dans le secteur académique en France, avec des objectifs ambitieux notamment dans le domaine de la caractérisation et la modélisation du trafic, il est apparu judicieux d'observer le trafic avec ces deux angles de vue, micro et macroscopique. Pour l'analyse microscopique, la solution retenue est basée sur les cartes DAG [Cle 00]. Pour l'analyse macroscopique la solution retenue est basée sur les sondes QoSMOS[16].

2.1.1. Premières contraintes et besoins

La principale contrainte qui se pose pour l'installation de sondes de mesure est due à la nature opérationnelle du réseau dont nous souhaitons analyser le trafic, et au besoin de laisser le réseau continuer à fonctionner sans aucune dégradation du service qu'il offre, lorsque la sonde est installée. Le premier besoin pour le système de mesure à mettre en place est donc une transparence totale pour le réseau et son trafic. Cela signifie que pour être non intrusif, cet équipement ne devra pas provoquer de pannes, d'erreurs de transmission et ne pas introduire de délais pour ne pas modifier le profil du trafic.

Le second besoin lors du choix des sondes de mesure passive concerne sa précision et la validité des traces qu'elle produira. Ainsi, il est essentiel de ne pas « manquer » de paquets transitant sur le réseau, et d'avoir des informations précises sur le passage de ces paquets, notamment au niveau temporel, qui représente aujourd'hui une des difficultés majeures avec les systèmes actuels. Le système devra donc être bien dimensionné et offrir une horloge précise qui ne dérive pas.

Enfin, le troisième besoin qui apparaît concerne la possibilité de corréler des événements de plusieurs traces, par exemple de suivre un paquet en plusieurs points du réseau, ou d'analyser de façon croisée le passage des paquets et de leurs acquittements, etc. Pour pouvoir finement analyser de tels événements se produisant en des points géographiquement distants et à des instants distincts mais faiblement éloignés temporellement, il est nécessaire de disposer d'une base temporelle commune et universelle pour toutes les sondes.

2.1.2. La solution DAG

Pour répondre à ces besoins (transparence, précision temporelle, temps universel), la solution existante la mieux adaptée est indéniablement une solution basée sur les cartes DAG conçues et développées à l'université de Waikato en Nouvelle-Zélande et, à l'heure actuelle, commercialisées, maintenues et améliorées par la société ENDACE. Le principe de fonctionnement des sondes DAG est décrit sur la figure 9. Le premier avantage de cette carte est de pouvoir travailler en dérivation du lien à analyser. Ainsi, dans le cadre de réseaux sur fibres optiques, le principe de branchement de la sonde consiste à insérer un « splitter » optique qui laisse passer 80 % de la puissance optique sur la fibre originelle (chemin normal), et récupère 20 % de cette puissance à destination de la sonde DAG. Ainsi, le trafic n'est absolument pas perturbé, aucun délai n'est introduit au niveau du « splitter »[17] et le trafic

[16] Voir http://www.qosmos.net.

[17] D'ailleurs, le « splitter » est un élément complètement passif basé sur des jeux de miroirs qui ne sont même pas alimentés électriquement, garantissant ainsi un fonctionnement normal même en cas de panne d'électricité.

conserve donc les mêmes caractéristiques et profils. Le système de mesure est ainsi totalement transparent.

De son côté, la carte DAG est une carte dédiée qui réalise, en temps-réel, l'extraction des entêtes de tous les paquets qui passent sur le lien. La taille de l'entête est précisée au moment de la configuration de la carte pour la capture. Dans notre cas, nous souhaitons pouvoir capturer les entêtes IP et TCP. Enfin, pour chaque paquet capturé, la carte ajoute une estampille codée sur 64 bits à l'entête capturée. Le tout est ensuite stocké sur disque. Il est à noter que les traces ainsi constituées deviennent rapidement très volumineuses, surtout sur les réseaux à hauts débits, et nécessitent donc d'utiliser des disques de grandes capacités et en nombres suffisants.

Pour la même raison, le trafic qui transite entre la carte DAG et le disque dur de la station hôte est très élevé, et pour les réseaux aux capacités les plus fortes, les bus PCI classiques des ordinateurs habituels ne suffisent pas. Il est nécessaire dans ce cas d'utiliser des bus PCI à 64 bits et à 66 MHz. Tous ces éléments (carte dédiée temps-réel, bus haute capacité, mémoire importante et disques durs de grandes capacités) sont les éléments indispensables pour garantir un système bien dimensionné capable de capturer une trace de tous les paquets ayant transité sur le lien mesuré.

En ce qui concerne l'estampille de passage de chaque paquet, stockée avec l'entête du paquet, une référence GPS est utilisée. La carte est en effet directement reliée à une antenne GPS. Ainsi, l'horloge de la station qui héberge la carte DAG est resynchronisée chaque seconde sur un signal GPS qui transporte le temps universel venant des horloges atomiques de référence. Ainsi, la dérive de l'horloge est quasiment inexistante, garantissant une grande précision des mesures temporelles, ainsi que le temps universel, car les sondes seront effectivement synchronisées sur le temps de référence universel.

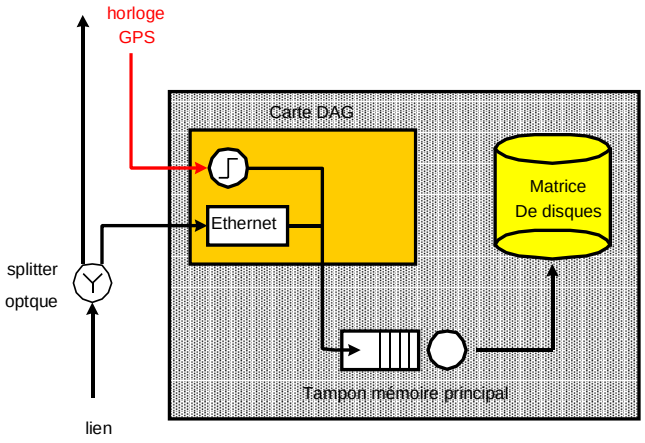

Figure 9. Principe opératoire des cartes DAG

Pour analyser les traces capturées par les sondes, une plate-forme de stockage des traces et d'analyse a été conçue et mise en place. Cette plate-forme est hébergée au LAAS à Toulouse et ouverte aux partenaires de METROPOLIS et MétroSec. Les besoins de cette plate-forme sont donc essentiellement une grande capacité de stockage, et une grande capacité de traitement (processeurs et mémoire essentiellement).

2.1.3. Déploiement des sondes DAG

Nous avons demandé à plusieurs responsables des réseaux académiques français l'autorisation de déployer nos équipements de mesure sur le réseau qu'ils opèrent. Notre objectif était de pouvoir déployer ces sondes sur des réseaux de natures différentes, soit sur le réseau de cœur, sur les réseaux régionaux et à la sortie des laboratoires. Toutes les autorisations ne nous ont pas été accordées pour des raisons sur lesquelles nous reviendront plus loin. Toutefois, aujourd'hui, 5 sondes DAG ont été déployées et respectent quasiment le schéma que nous nous étions fixé. Ainsi, trois sondes en Fast-Ethernet ont été positionnées à la sortie du LAAS, du LIP6 et de l'IUT de Mont-de-Marsan. Deux sondes Giga-Ethernet ont été positionnées à la sortie du réseau de l'ENS Lyon et surtout de Jussieu sur RAP, nous permettant ainsi d'avoir, dans ce dernier cas, accès aux traces du trafic d'un réseau à très haut débit.

Ce choix de positionnement est aussi stratégique par rapport au positionnement des sondes de métrologie passive macroscopique et des sondes de métrologie active dont un exemplaire de chacune d'entre-elles a été placé également au LAAS et au LIP6. Ainsi, il sera possible, pour un même trafic de corréler les analyses micro- et macroscopiques, ainsi que les mesures actives et passives, et ce en plusieurs points du réseau sur leur chemin entre Toulouse et Paris.

Au final, la plate-forme de mesure passive a été déployée (même si nous aurions souhaité mettre en place une à deux sondes de plus). Tous les problèmes soulevés ont été résolus, qu'il s'agisse des problèmes techniques liés à ce matériel (installation, câblage, développement de logiciels), ou aux contraintes d'anonymisation demandées par nos partenaires administrateurs de réseaux.

Sur le plan de nos besoins, ces sondes remplissent parfaitement leur cahier des charges : elles sont totalement transparentes, extrêmement précises et la base de temps GPS (horloges atomiques de référence universelles) est précise à moins de 2 μs près pour nous permettre de corréler les traces capturées en différents lieux. Enfin, il existe une base de données de traces, et des logiciels d'analyse de ces traces que nous allons présenter ci après.)

2.2. Caractérisation et analyse du trafic

Ainsi, face à la quantité de traces capturées dans METROPOLIS au début et MétroSec aujourd'hui, nous avons décidé de concevoir et développer un logiciel d'analyse des traces de trafic Internet. Ce logiciel a été baptisé Zoo[18] car il analyse les flux souris, éléphants, libellules, tortues, etc. présents dans le trafic [Lar 05c]. En effet, dans l'optique d'optimiser le niveau de service fourni à tous les flux transportés par le service « best effort », il apparaît judicieux de ne pas se baser sur des classes de services dépendant des types d'applications, mais plutôt sur la taille des flux TCP ou UDP qui – nous allons le voir – a un impact significatif sur le comportement des protocoles et des réseaux, ainsi que sur leur niveau de performance et la QoS qu'ils offrent. La coutume veut que l'on associe un nom d'animal à chaque type de flux. Ainsi, le « Zoo » de la métrologie comprend essentiellement des souris et des éléphants : les souris sont des flux qui ne comportent qu'un petit nombre de paquets (en général moins de 10). Les éléphants sont des flux qui – a contrario – se composent d'un grand nombre de paquets (en général plus de 100). Souris et éléphants sont actuellement les types de flux les plus étudiés car – nous allons le voir – ce sont eux qui ont le plus d'impact sur les

[18] Voir http://www.laas.fr/~owe/ZOO.

caractéristiques du trafic et le niveau de performance des réseaux. Dans la suite, nous allons d'ailleurs focaliser notre étude uniquement sur ces deux types de flux. Toutefois, on trouve dans la littérature de nombreux autres animaux, comme les buffles (des flux qui démarrent en groupe), des tortues (qui sont des flux long bas débit), etc. Le logiciel Zoo permet de réaliser toutes les analyses de base de ces flux, et en donne diverses statistiques, sur leur taille (en nombres octets et paquets), leur durée, le nombre de pertes expérimentées, leur débit, etc. Toutefois, la motivation principale pour développer un tel outil était naturellement de lui adjoindre des fonctionnalités d'analyse plus avancées. En particulier, notre objectif était de pouvoir analyser les comportements architecturaux et protocolaires qui engendrent les phénomènes de variabilité et de dynamicité du trafic, variabilité qui est néfaste à la mise en œuvre d'une QoS stable (et à laquelle les mécanismes protocolaires et architecturaux que nous allons proposer vont devoir d'adapter). Ainsi, par rapport à la plupart des travaux actuels et dont les résultats sont décrits dans la partie 1.2.2.2, notre objectif n'est pas de trouver un modèle mathématique décrivant le trafic. Au contraire, nous voulons analyser finement ses variations pour comprendre comment les composants de l'Internet, et notamment ses protocoles de transmission, ont pu arriver à générer un trafic au profil si problématique pour l'évolution du réseau vers la QoS. La contribution principale de cet outil est donc d'analyser la variabilité du trafic, la dynamicité des ressources du réseau, pour ensuite pouvoir proposer de nouvelles architectures protocolaires à QoS, adaptées à la réalité du trafic et du réseau.

Par rapport à la variabilité du trafic, les premiers résultats de caractérisation du trafic obtenus dans METROPOLIS sur un réseau académique comme RENATER ou commercial comme une plaque ADSL de France Télécom (cf. partie 1.2.2.1.3) montrent d'ailleurs que la grande majorité du trafic est du trafic élastique, susceptible d'engendrer des variations importantes dans les caractéristiques du trafic notamment au niveau du débit paquets ou octets. Le trafic « stream », même si sa quantité augmente fortement, a une proportion qui tend à décroître par rapport au trafic global. L'augmentation incroyable du trafic Internet actuel est en particulier liée à l'avènement des réseaux P2P comme Gnutella, E-Donkey, Morpheus, etc. Le P2P est devenu depuis quelques années la « killing application ». Il représente environ 85% du trafic global sur les réseaux commerciaux, et il faut toute la vigilance de leurs administrateurs pour que les réseaux académiques ne suivent pas le même chemin (ce type de trafic est le plus souvent hors charte de RENATER). Il est à noter également que le type de fichiers échangés – musiques, films, jeux vidéo essentiellement – ont des tailles importantes allant de quelques Mégaoctets pour les musiques à plusieurs giga-octets pour les films ou les jeux, ce qui renforce le phénomène déjà observé : les distributions des tailles de flux dans l'Internet ne sont plus exponentielles, mais à queues lourdes, induisant les phénomènes d'auto-similarité et de LRD (cf. partie 1.2.2.2).

Plusieurs études ont commencé à étudier les causes de la LRD et de l'auto-similarité du trafic sur les performances du réseau et sa capacité à alors fournir un certain niveau de QoS, mais ces études sont restées embryonnaires [Par 97]. Or, c'est ce type de résultats qui nous intéresse ici par rapport au problème de la garantie de la QoS dans un environnement dynamique, la dynamicité des ressources à laquelle nous sommes confrontés nous semblant intuitivement liée aux différents niveaux de dépendance qui apparaissent dans le trafic à différentes granularité. Une large part de notre travail ces dernières années a donc consisté à montrer le lien qui pourrait exister entre les caractéristiques du trafic, les performances du réseau, et la QoS obtenue dans ces conditions. Pour cela, il a fallu savoir évaluer la dépendance dans le trafic à toutes les échelles de temps.

2.2.1. L'impact de la dépendance à long terme dans le trafic

En revenant à l'évolution majeure du trafic Internet qui consiste en un de plus en plus grand nombre de flux longs, la figure 10 illustre les modifications que nous pouvons observer. Pour cela, elle compare le trafic Internet actuel avec un trafic qui suit un modèle de Poisson. Ces deux trafics sont observés à différentes granularités (0,01 s, 0,1 s et 1 s) et il est facile de remarquer que le trafic Internet ne se lisse pas aussi vite que le trafic Poissonnien.

L'analyse a montré que ce résultat est totalement dû aux éléphants présents dans le trafic Internet. En effet, la transmission d'éléphants crée dans le trafic l'arrivée d'une grande vague de données qui a la particularité de durer un temps relativement long (plus d'une seconde[19]). C'est pour cela que l'on observe cette différence entre les deux types de trafics : la transmission des éléphants induit des oscillations persistantes dans le trafic actuel.

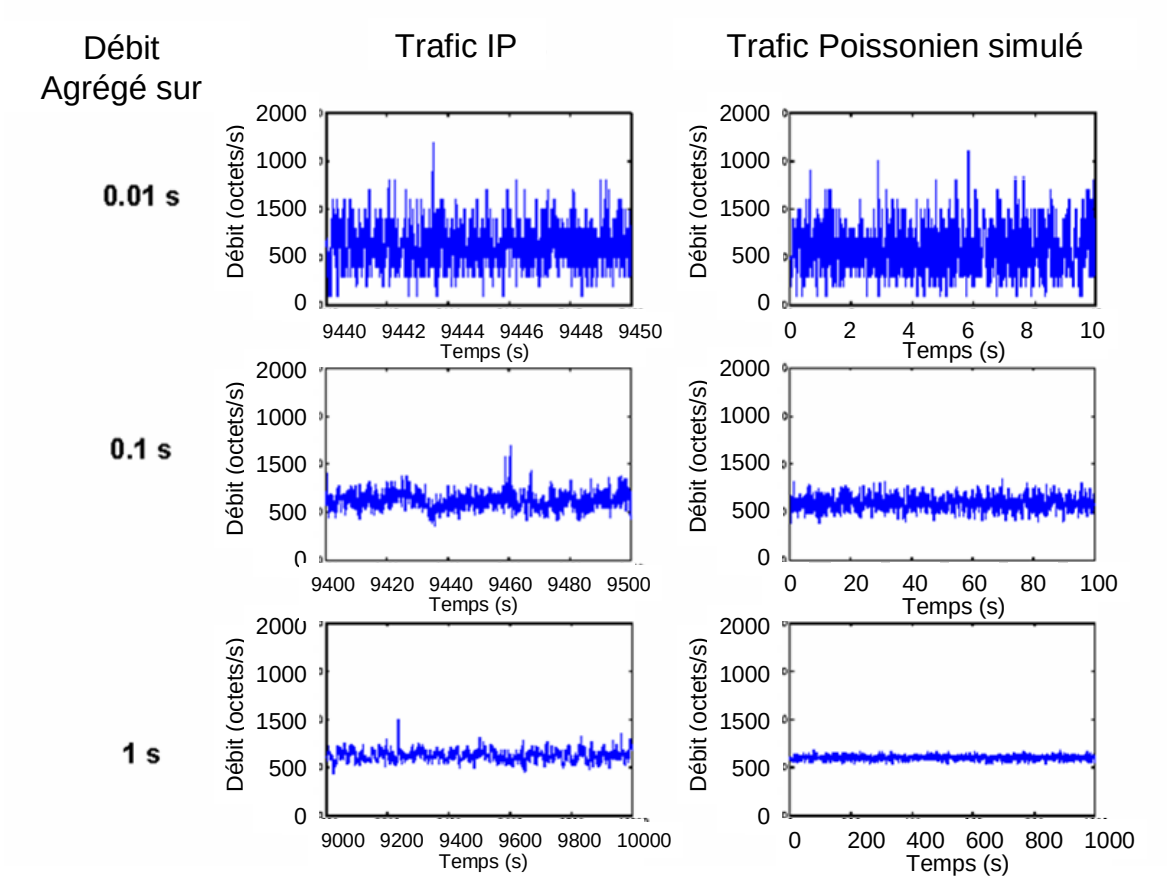

Figure 10 : Comparaison entre les oscillations observables dans un trafic Internet et un trafic Poissonnien. Cette étude réalisée dans le cadre de METROPOLIS se base sur du trafic d'une plaque ADSL de France Télécom.

De plus, les connexions TCP utilisées pour transmettre les flux éléphants plus volumineux durent plus longtemps et la dépendance qui existe entre les paquets d'une même connexion se propage ainsi sur des échelles de temps plus longues. C'est ce phénomène que l'on nomme traditionnellement LRD. On lui attribue plusieurs causes dont la principale est imputable aux mécanismes de contrôle de congestion de TCP (le protocole dominant de l'Internet). Parmi tous les mécanismes de TCP, il est évident que celui basé sur un contrôle en boucle fermée introduit de la dépendance à court terme, étant donné que les acquittements dépendent de l'arrivée d'un paquet, et que l'émission de tous les paquets suivants de la

[19] Les flux web sont traditionnellement transmis en moins d'une seconde dans l'Internet actuel.

connexion sont conditionnés par cet acquittement. De la même façon, les deux mécanismes de TCP (« slow-start » et « congestion avoidance ») introduisent de la dépendance à plus long terme entre les paquets de différentes fenêtres de congestion. Ainsi, en généralisant ces observations, il est évident que tous les paquets TCP d'une connexion sont dépendants les uns des autres. En plus, l'augmentation des capacités des liens de l'Internet en permettant la transmission de flux de plus en plus longs, augmente le phénomène de LRD. C'est pourquoi on observe sur la figure 10, la persistance d'un comportement oscillatoire dans le trafic Internet qui reste très marqué même avec une granularité d'observation importante (1 s).

Etant donné que le phénomène de dépendance de TCP se propage dans le trafic par l'intermédiaire des flux (i.e. les connexions TCP) [Ver 00], l'augmentation de la taille des flux induit une augmentation de la portée de la dépendance qui peut atteindre des échelles très importantes. Ainsi, une oscillation au temps t induit alors d'autres oscillations à d'autres instants qui peuvent être potentiellement très éloignés de t. D'autre part, il est évident que les éléphants, en raison de leur durée de vie très importante dans le réseau et des grandes capacités de ce dernier (la plupart du temps les liens étant sur-dimensionnés), ont le temps d'atteindre de grandes valeurs pour leur fenêtre de contrôle de congestion. Ainsi, une perte induit pour le flux qui la subit une importante diminution, suivie par une importante augmentation de son débit. L'augmentation de la taille des flux favorise donc les oscillations avec une forte amplitude et un phénomène de dépendance à long terme.

Bien sûr, les oscillations sont très néfastes pour une utilisation optimale des ressources globales du réseau étant donné que la capacité libérée par un flux subissant une perte ne peut pas être immédiatement utilisée par un autre (en raison de la phase de slow-start notamment). Ceci se traduit par un gaspillage de ressources et induit une diminution de la QoS globale du réseau. En fait, plus le trafic oscille, moins les performances sont importantes [Par 97].

2.2.2. Analyse multi-échelle du trafic

Ainsi, ces premiers résultats de caractérisation du trafic Internet confirment la nature de nombreux phénomènes se produisant avec des granularités différentes (e.g. l'auto-similarité), et nécessitent donc de mettre en œuvre une méthode d'analyse multi-échelles. La technique qui est aujourd'hui la plus utilisée pour une telle analyse multi-échelle nous vient du domaine du traitement du signal. Il s'agit d'analyse à base d'ondelettes que nous allons décrire et illustrer dans la suite.

Rappelons d'abord le principe des ondelettes (voir [Mal 99] pour une introduction complète). ψ_0 représente l'ondelette-mère. $\psi_{j,k}(t) = 2^{-j/2}\psi_0(2^{-j}t - k)$ représente sa forme dilatée et translatée et $d_X(j, k) = \langle \psi_{j,k}, X_0 \rangle$ les coefficients d'ondelette correspondants. L'ondelette-mère ψ_0 est aussi caractérisée par un entier $N \geq 1$, le nombre de moments évanescents qui joue un rôle clé dans l'analyse pratique et théorique de la longue mémoire. Pour tous les processus X stationnaires au second ordre, son spectre $f_X(\nu)$ peut être exprimé à l'aide de ses coefficients d'ondelette par l'équation :

$$E(d_X(j,k)^2) = \int f_X(\upsilon) 2^j \left| \Psi_0 2^j \upsilon \right|^2 d\upsilon$$

où Ψ_0 est la transformée de Fourier de ψ_0 et E l'espérance mathématique. Si X est un processus dépendant à long terme de paramètre d, cela implique que :

$$E(d_X(j,k)^2) \propto C 2^{j(2d+1)}, \text{ si } 2^j \rightarrow +\infty$$

De plus, il a été prouvé que $\{d_X(j, k), k \in Z\}$ forment une séquence dépendante à court terme si $N > d + 1/2$. Cela signifie qu'ils ne souffrent pas des difficultés statistiques dues aux

propriétés de longue mémoire. En particulier, les moyennes temporelles $S_j = 1/n_j \sum_{k=1}^{n_j} |d_X(j,k)|^2$ peuvent être utilisées comme des estimateurs efficaces et robustes pour $E(d_X(j,k)^2)$. Ceci conduit à la procédure d'estimation suivante : une régression linéaire pondérée de $log_2 S_j$ par rapport à $log_2 2^j = j$, réalisée à la limite de la granularité d'étude la plus grande, fournit une estimation de $2d+1$, et par conséquent de d. Les représentations graphiques de $log_2 S_j$ en fonction de $log_2 2^j = j$ sont communément qualifiées de diagrammes logarithmiques (LD : logscale diagrams) d'estimation de la LRD, comme par exemple le diagramme de la figure 12. La possibilité de faire varier N apporte de la robustesse à ces procédures d'analyse et d'estimation. La définition complète ainsi que les performances de cette procédure d'estimation sont détaillées dans [Abr 00] [Abr 98] [Vei 99].

Pour visualiser le principe de l'analyse du trafic par décomposition en ondelettes, nous l'illustrons sur la figure 11. Nous rappelons que la propriété d'auto-similarité du trafic signifie que le schéma oscillant du trafic Internet se produit à toutes les échelles de temps. Il est donc important pour analyser le trafic de disposer d'un outil capable d'analyser le comportement du trafic, et notamment ses variations, à toutes les échelles de temps, i.e. pour toutes les granularités. La figure 11 illustre bien que la fonction en ondelettes représente bien les variations du trafic, et ce, quelles que soient leurs durée dans le temps. Le principe de cette analyse consiste à extraire du trafic toutes les ondelettes possibles. Pour cela, nous utilisons plusieurs fonctions en ondelettes, chacune de fréquence différente afin d'obtenir les différentes granularités temporelles d'observation. Les fonctions avec les périodes les plus larges représentent les plus longues vagues, c'est à dire celles générées par les flux éléphants.

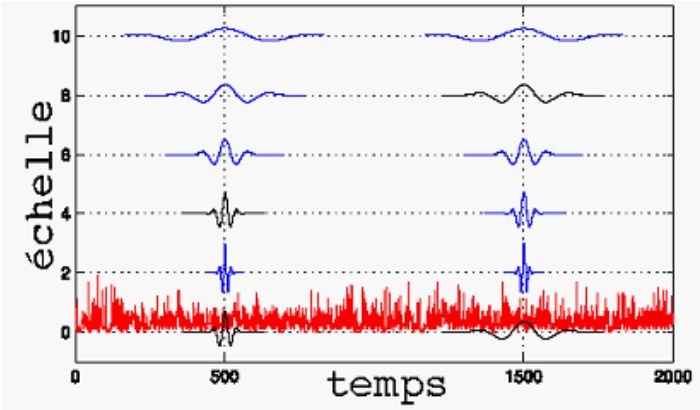

Figure 11 : Analyse en ondelettes de la LRD d'une trace de trafic Internet (Renater)

La courbe de la figure 12 a été obtenue en utilisant l'outil LDEstimate [Abr 98] estimant la LRD qui se manifeste dans le trafic à toutes les échelles temporelles. Le résultat produit par cet outil est une représentation graphique des lois qui régissent le niveau de dépendance du trafic à différentes échelles temporelles. Il représente le niveau de variabilité des oscillations (écart-type de l'amplitude des variations en ordonnées – ici en kbps) en fonction de la granularité d'observation (l'octave i correspond à $2^i \times \Delta$ unité de temps, ou Δ est la granularité d'agrégation de base de la série temporelle utilisée – ici 1 ms). Le facteur de Hurst (caractéristique des processus auto-similaires qui se retrouvent dans le trafic Internet, cf. [Par 00]) est obtenu directement sur la courbe de LRD à partir de la mesure de sa pente. La figure 12 montre un comportement différent pour deux échelles temporelles (appelé phénomène de « bi-scaling »). La frontière entre ces deux niveaux de LRD se trouve autour de

l'octave 8 et met en évidence des niveaux de LRD différents pour les échelles de temps courtes et longues, ceci se traduisant par différentes lois de puissance. Pour les échelles petites (octave < 8), c'est à dire les paquets proches les uns des autres, la dépendance est peu marquée. Par contre, pour les échelles plus grandes octave > 8), c'est à dire des paquets appartenant à des fenêtres de congestion consécutives, la dépendance est beaucoup plus importante. Evidement, ce phénomène existe pour l'ensemble des fenêtres de congestion d'un même flux. Ainsi, la présence dans le trafic de très long flux introduit un phénomène de dépendance à très long terme qui est visible sur la figure 12 pour les octaves très grands (> à 12). Ce niveau de LRD dans le trafic devient un problème majeur étant donné que chaque oscillation se produisant à un temps t peut se reproduire à n'importe quel temps t' qui est dépendant de t (en raison de la LRD qui existe entre les paquets échangés par le biais des protocoles traditionnels : ici TCP sur les longs flux). Il est intéressant de noter que nos expériences ont montré que le coude présent sur la courbe de LRD correspondait à la taille moyenne des flux, la partie droite de la courbe correspondant donc à l'impact des flux éléphants.

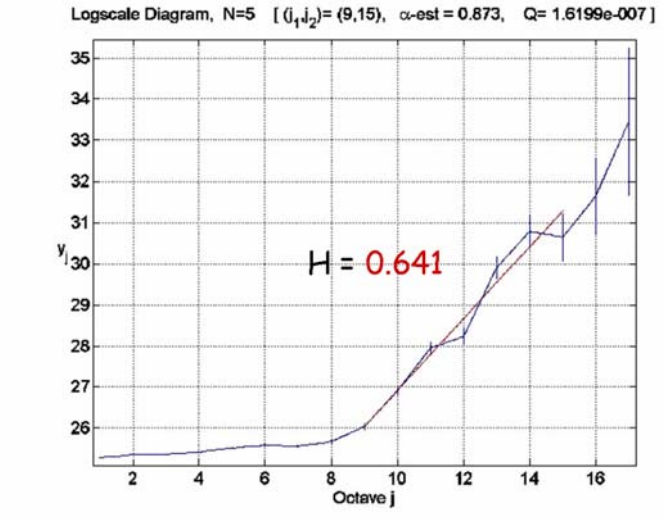

Figure 12 : Evaluation de la LRD dans le trafic Internet

2.2.3. Etude quantitative de la relation existant entre oscillations et LRD dans le trafic Internet

2.2.3.1. Evaluation de l'impact de TFRC sur la QoS

Ces observations et analyses, associées à la littérature dans le domaine amènent à penser que la LRD est un bon moyen de caractériser la variabilité du trafic, en particulier dans sa persistance. Toutefois, ce problème n'a, à notre connaissance, jamais été vraiment abordé dans la littérature existante. Aussi, l'expérience qui va être décrite dans la suite a pour objectif, sur un exemple, de montrer l'existence de ce lien entre les deux aspects variabilité et LRD. Pour ce faire, l'expérience menée s'est proposée de comparer au travers de simulations NS le trafic réel avec le même trafic re-simulé[20], mais pour lequel le mécanisme de contrôle de congestion

[20] Le principe de la technique de rejeu est présentée dans [Owe 04a], ainsi que, sommairement, dans le paragraphe 2.4 de ce manuscrit. Son objectif est de reproduire statistiquement le processus d'arrivée des paquets. Les résultats obtenus avec cette méthode sont très probants au point d'éliminer toute divergence entre trafic réel et trafic simulé. Le trafic simulé est quasiment équivalent statistiquement au trafic réel. Du moins, il en a toutes les propriétés importantes pour nous.

du protocole de transmission TCP a été remplacé par TFRC [Owe 04b] [Flo 01]. L'objectif de TFRC par rapport à TCP est de fournir des sources de trafic beaucoup plus lisses et régulières, c'est-à-dire des sources qui ne présentent pas ou peu d'oscillations. Ce mécanisme a été aussi défini pour permettre un meilleur transfert du trafic généré par les applications de streaming dans l'Internet qui nécessitent naturellement un maximum de régularité pour leurs débits d'émission et de réception. La formule qui donne la quantité de trafic à envoyer par intervalle de temps de durée RTT est la suivante (elle correspond au débit d'un flux TCP [ALT 00]) :

$$X = \frac{s}{R \times \sqrt{2 \times b \times \frac{p}{3}} + \left(t_{RTO} \times \left(3 \times \sqrt{3 \times b \times \frac{p}{8}} \right) \times p \times \left(1 + 32 \times p^2 \right) \right)}$$

Où :

- X est le débit en émission en octets/seconde,
- s est la taille des paquets en octets,
- R est le temps d'aller retour en secondes (aussi appelé RTT),
- p est le taux de perte (entre 0 et 1.0),
- t_{RTO} est la valeur du timeout de retransmission de TCP en seconde,
- b est le nombre de paquets acquittés par un seul acquittement.

On montre ainsi que lorsque l'on emploie TFRC, et donc quand on génère un trafic régulier et lisse, la LRD qui apparaît dans le réseau est très réduite par rapport au cas où TCP est utilisé.

Cette expérience décrite plus précisément dans [Owe 04b] a pour objectif de fournir une étude comparative des caractéristiques globales du trafic suivant que les éléphants sont transmis en utilisant TCP ou TFRC. Cette expérience vise aussi à fournir des résultats dans un environnement réaliste (cf. partie 2.4). L'étude comparative porte sur la trace originale d'une part et sur la trace simulée d'autre part dans laquelle les flux éléphants sont transmis en utilisant TFRC.

Par rapport au thème de cette étude comparative qui vise à étudier les effets de TFRC sur le caractère oscillant du trafic, les paramètres qui vont être évalués sont les paramètres traditionnels de débit, mais aussi des paramètres statistiques du trafic comme la LRD, et quelques paramètres mesurant le niveau de variabilité du trafic. Pour cela, nous utilisons un coefficient de stabilité (SC) qui est défini par le quotient :

$$Coefficient\_de\_stabilité(CS) = \frac{trafic\_moyen\_échangé}{écart\_type\_du\_trafic\_échangé(\sigma)}$$

La figure 13 présente le trafic dans les deux cas d'étude soit le cas réel et le cas simulé (avec TFRC). Visuellement, comme cela a déjà été montré dans la littérature abondante sur TFRC, il apparaît clairement qu'en utilisant TFRC pour transmettre les éléphants à la place de TCP, le trafic global est bien plus lisse et régulier, et que tous les grands pics de trafic que l'on peut voir sur le trafic réel ont disparu du trafic simulé avec TFRC.

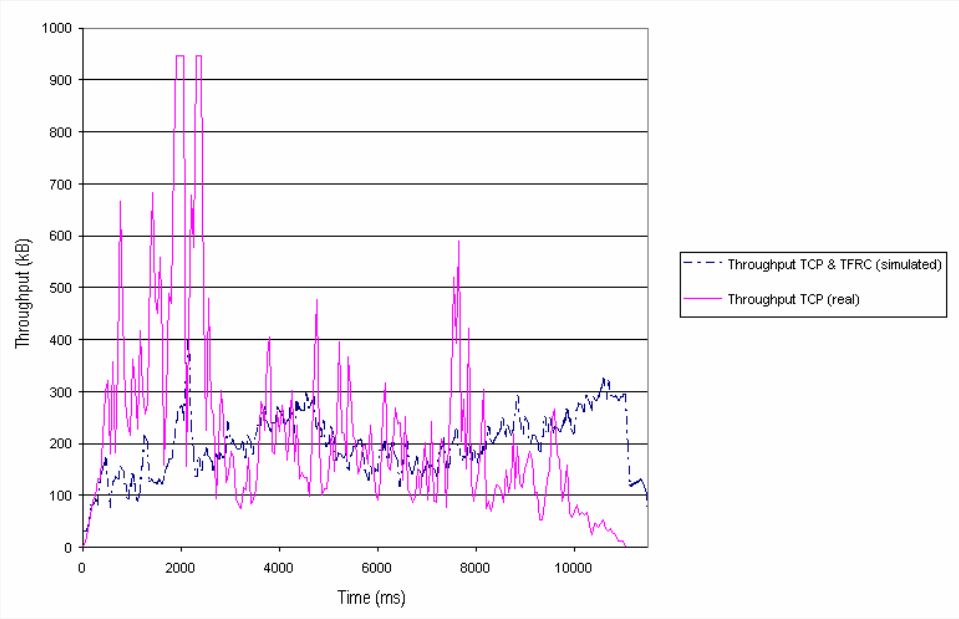

Figure 13 : Evolution du débit au cours du temps

Les résultats quantitatifs sont présentés dans le tableau 3. Ils confirment que la variabilité du trafic dans le cas du trafic réel (utilisant TCP pour transmettre les éléphants) est bien plus importante par rapport au cas simulé dans lequel les éléphants sont générés avec le protocole TFRC (voir les différences sur les écarts types et les coefficients de stabilité).

En ce qui concerne le débit global, nous avons mesuré des débits assez proches dans les deux cas. Ce résultat est excellent pour TFRC qui est, par définition, borné par le débit théorique de TCP. Il n'est, de plus, pas conçu pour consommer rapidement une grande quantité de ressources [Owe 03a], et même si TFRC est donc moins agressif que TCP, il est capable d'atteindre quasiment le même niveau de performance que TCP. Ceci confirme l'importance de la stabilité du trafic pour obtenir des performances de haut niveau et optimisées pour les réseaux de communication [Par 97].

Protocole	Débit moyen (ko)	σ (ko)	CS
TCP New Reno (NR) : cas réel	82,335	157,959	0,521
TCP NR & TFRC : cas simulé	77,707	102,176	0,761

Tableau 3 : Caractérisation du débit pour les protocoles TCP et TFRC

En ce qui concerne la LRD, et c'est là la contribution originale de ce travail, la figure 14 montre que dans le cas simulé la propriété de bi-scaling disparaît et la courbe, même pour les grandes octaves a une pente peu marquée (puisque c'est bien la pente qui est importante pour évaluer les phénomènes de dépendance). Cela signifie que toutes les formes de dépendance, et en particulier celles à long terme ont été réduites de façon drastique. Les valeurs pour la LRD, qui s'exprime à l'aide du facteur de Hurst, sont: H(trafic réel) = 0.641 et H(trafic simulé) = 0.194 (ce qui dans ce dernier cas est non significatif – à cause du niveau d'incertitude du calcul sur cette série – mais marque bien l'absence de LRD).

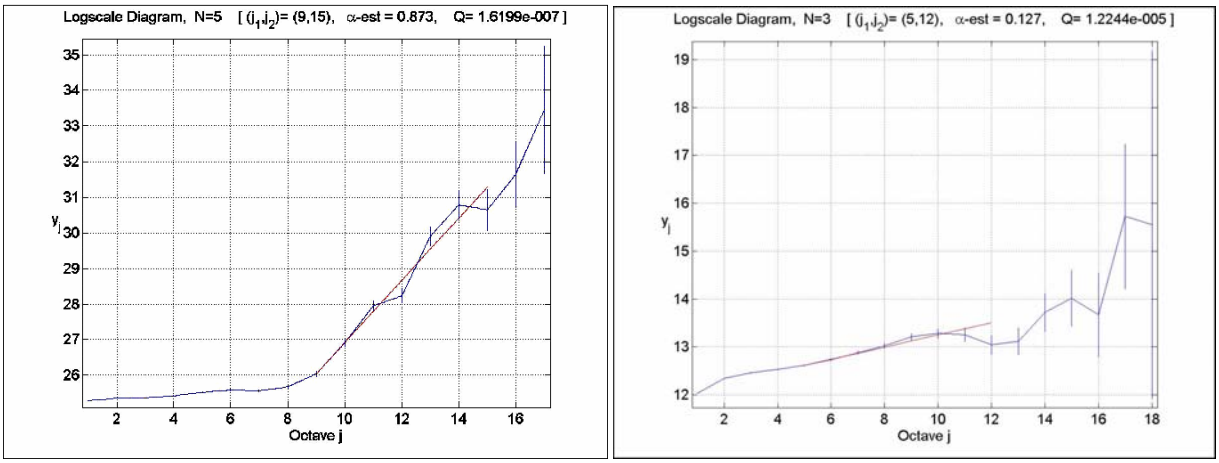

Figure 14 : Evaluation de la LRD pour le trafic simulé incluant des éléphants TFRC

2.2.3.2. La LRD : une métrique caractéristique de la QoS

Sans en donner une preuve formelle, cette expérience a permis de mettre en évidence le lien étroit qui existe entre la caractéristique oscillante du trafic et la LRD. En effet, à partir du moment où on utilise pour transmettre les flux éléphants un protocole qui ne crée pas d'oscillations (TFRC) et qui brise le modèle de dépendance lors de la récupération des pertes (les pertes inter-dépendantes se produisant en général dans la même période de RTT et étant donc toutes récupérées par TFRC en une seule fois), la LRD disparaît quasiment du trafic.

Ce résultat d'analyse est important car il donne un outil pour caractériser qualitativement et quantitativement un des phénomènes caractéristiques du trafic Internet, qui est de plus un élément dégradant de la performance du réseau. Surtout, il permet de donner des directions de recherche pour trouver des parades à ce phénomène, en particulier concernant les protocoles de transport et leurs mécanismes de contrôle de congestion.

Ce travail de caractérisation – par rapport à ce qui se fait dans le domaine et qui a juste pour vocation de trouver un modèle mathématique décrivant le trafic Internet – a donc bien permis d'analyser tous les phénomènes de variabilité du trafic de l'Internet et de les expliquer, mettant en cause notamment le comportement de TCP (sans TFRC) lorsqu'il est utilisé pour transmettre des flux éléphants sur des réseaux à hauts débits. En sachant maintenant quels sont les mécanismes de TCP qui engendrent cette dynamicité dans son débit d'émission (conduisant à une inefficacité et une instabilité dommageable), nous avons les cartes en main pour proposer des solutions pour éviter la variabilité du trafic.

2.3. MBN : Une nouvelle architecture Internet adaptative basée sur un système de métrologie global

L'analyse des lacunes des solutions existantes pour la mise en œuvre de la QoS dans l'Internet (IntServ, DiffServ, …), ajoutée aux connaissances sur les caractéristiques du trafic actuel obtenue grâce aux nouveaux outils de métrologie, montrent clairement les 3 problèmes majeurs qu'il faut résoudre pour une architecture à QoS – telle que définie dans la partie 1.1.2, i.e. optimiser la QoS offerte par le service « best effort » – dans l'Internet :

- Elle devra être insensible aux facteurs d'échelle ;

- Elle devra fonctionner de bout en bout indépendamment des différents domaines et AS (Autonomous System) de l'Internet ;
- Et surtout, elle devra s'adapter à la dynamicité des ressources du réseau et à la variabilité du trafic.

Dans ce qui précède, nous avons montré que la métrologie répond au dernier point de cette triple problématique, avec des solutions aussi simples que de positionner une sonde de mesure du trafic sur le lien considéré. Pour pouvoir répondre au deux autres points de la problématique, il faut concevoir et mettre en œuvre un système de métrologie global, à l'échelle de l'Internet, qui permette à tout équipement actif du réseau – routeurs, proxies, etc. – d'avoir une connaissance instantanée de l'état du réseau partout dans le monde[21]. C'est grâce à un tel système de métrologie global que nous pourrons développer des mécanismes réseaux adaptatifs pour optimiser le niveau de QoS du service « best effort » actuel.
Nous avons donc aussi proposé une nouvelle architecture adaptative qui utilise les outils de mesure et de supervision du trafic et de la QoS, ainsi que les résultats de caractérisation et d'analyse du trafic. Cette approche s'appelle MBN (« Measurement Based Networking »). Elle repose sur une architecture orientée mesure : MBA (« Measurement Based Architecture ») qui inclut le système de métrologie global. La suite de cette partie va détailler les différents composants du système de métrologie global, son utilisation, ainsi que l'architecture MBA.

2.3.1. Retour sur la problématique de la QoS dans l'Internet

Dynamicité / variabilité du trafic et des ressources réseaux

Les résultats de caractérisation et d'analyse du trafic présentés dans la section 2.2 illustrent la grande variabilité du trafic Internet, dont les pics sont responsables des problèmes d'instabilité de la QoS réseau, ainsi que d'une dégradation importante des performances dans l'Internet. Ce résultat est en particulier dû aux gros flux qui transportent une quantité importante d'information. D'ailleurs le nombre de plus en plus important de ce type de flux ne fait qu'augmenter l'amplitude et la persistance des variations du trafic (caractérisées par une augmentation du phénomène de LRD). Or, la LRD et les variations sont néfastes pour la QoS du réseau car elles induisent des congestions, des variations de délai, ou plus généralement une grande variabilité dans la disponibilité des ressources de communication dans les réseaux, comme la bande passante, les mémoires tampon, etc., et ne permettent pas en conséquence de fournir un service stable aux utilisateurs [Par 97].

Les analyses ont d'ailleurs montré l'inadéquation de TCP au transport de flux éléphants sur des réseaux à hauts débits. Ce dernier a des réponses trop brusques et tardives par rapport à la dynamicité du réseau. De plus, les niveaux de service et de performances mis en œuvre dans l'Internet peuvent être très dégradés dans le cas d'un trafic non stationnaire. Or, le trafic ne peut être considéré comme stationnaire que pour des périodes de temps relativement courtes (quelques heures tout au plus). Au delà, il est aisé d'observer des différences entre les trafics mesurés au cours de la journée, de la nuit ou au moment des

[21] Un tel objectif est certainement trop ambitieux et surtout inutile étant donnée la spatialité le plus souvent restreinte des communications : beaucoup de communications restent très locales, avec des miroirs de sites web ou serveurs FTP, l'utilisation de caches, etc. Cependant, avoir des informations sur son domaine et les domaines alentours (à quelques sauts de là) est vraiment essentiel. Comme, il existe tout de même des connexions inter-continentales, avoir des informations sur tous les domaines que cette connexion va traverser peut également être une source d'informations très bénéfiques à sa gestion.

pauses déjeuner : les applications sont différentes (les applications professionnelles sont plus visibles pendant les périodes de travail alors qu'il y a plus d'applications de jeu en ligne par exemple en soirée) ainsi que le volume d'informations échangées. De la même façon, le trafic au moment de la pause déjeuner est moins important qu'aux heures de pointe, le trafic le week-end est moins important qu'en semaine, etc. D'autre part, des variations peuvent avoir lieu en raison d'évènements populaires dans l'Internet comme la diffusion d'un événement sportif ou culturel exceptionnel ou encore la mise à disposition de documents très attractifs sur un serveur web qui vont attirer un maximum de curieux. Ainsi, en raison des variations importantes du trafic Internet mesurables d'un lien à un autre, ou encore sur un même lien mais à des instants différents, il est très difficile de proposer un protocole de transport qui fonctionne de façon optimale dans tous les cas. Ainsi, une solution purement statique (pour la gestion du trafic) n'est absolument pas adaptée à un tel niveau de variabilité et d'instabilité du trafic (le nombre de flux et leur profil évoluant continuellement en fonction du temps).
Dès lors, les techniques de métrologie, qui permettent une quantification en temps réel de nombreux paramètres du trafic et du réseau, doivent permettre de mieux appréhender leur dynamicité.

Les structures administratives et topologiques de l'Internet

La figure 15 illustre la topologie et la structure administrative de l'Internet actuel. L'Internet est généralement représenté comme une interconnexion de réseaux. C'est évidemment vrai, mais cette définition est incomplète. En fait, l'Internet est surtout divisé en plusieurs domaines (aussi appelé AS pour « Autonomous System »), administrativement indépendants et dont la gestion est réalisée de façon isolée. Chaque réseau de chaque AS met donc à disposition des utilisateurs différents services et différents niveaux de QoS. En particulier les nouveaux types de réseaux, reposant sur de nouvelles technologies sans fil (WIFI, GPRS, UMTS, etc.) ou le satellite, proposent des niveaux de service très différents. Dans un tel contexte, assurer une QoS de bout en bout est un challenge ardu étant donné que la QoS finale obtenue par les utilisateurs sera celle du réseau rencontré sur le chemin entre la source et la destination dont le niveau de service sera le plus faible. En particulier, les liens connectant les différents AS (i.e. « peering links ») sont généralement sous-dimensionnés, et à l'origine d'importantes dégradations de la QoS et des performances pour les communications de bout en bout[22].

Ainsi, la structure administrative de l'Internet fait apparaître différents réseaux proposant chacun des services et un niveau de performance différents. Cette variabilité des services offerts est aussi à l'origine d'une forte dégradation des performances des mécanismes de niveau transport étant donné que dans une transmission de bout en bout le niveau de service offert aux utilisateurs est conditionné par le réseau qui offre la QoS la plus faible.

Toutefois, Il est évident pour nous que les techniques de métrologie peuvent dans ce cas apporter aux entités situées aux extrémités du réseau un ensemble d'informations permettant de s'adapter à cette hétérogénéité et dynamicité des ressources disponibles dans l'Internet. Ces mesures seront d'un grand intérêt pour adapter les mécanismes réseaux en temps réel aux évolutions du trafic et par exemple à l'évolution du niveau de congestion du réseau.

[22] Depuis quelques années, ce problème a mobilisé de nombreux efforts de la part des opérateurs et des Fournisseurs d'Accès Internet (FAI) qui ont progressivement augmenté la capacité de ces liens, ceci s'étant traduit par une augmentation du niveau de QoS pour les communications inter-domaines.

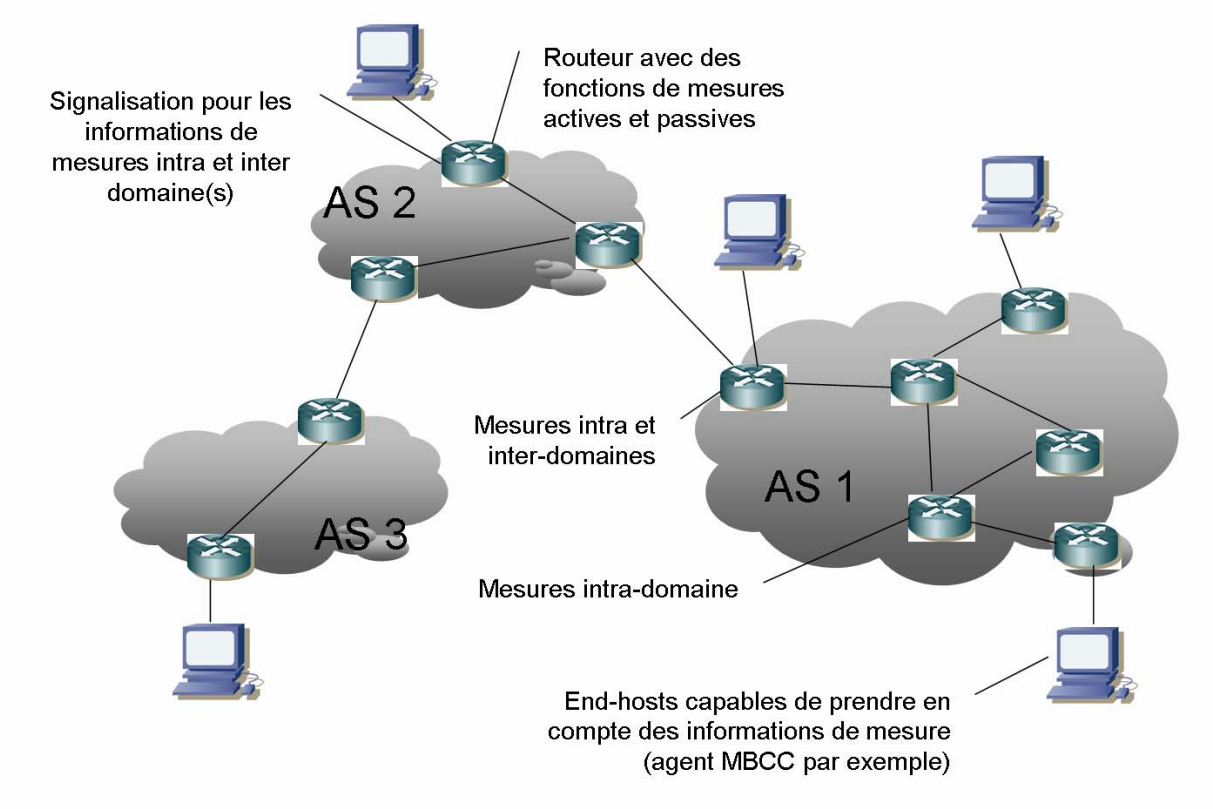

Figure 15 : Entités nécessaires dans le réseau pour permettre le déploiement de l'approche MBN

2.3.2. Principes de l'approche MBN et l'architecture MBA

Etant donnée la structure topologique de l'Internet et l'ensemble des problèmes concernant l'instabilité du trafic, son absence de stationnarité, sa nature fortement oscillatoire, son haut niveau de corrélation ou encore sa forte variabilité au cours du temps, il est aisé de comprendre qu'il est impossible de trouver une solution statique optimale qui s'appliquerait pour toutes les connexions dans l'Internet. Ce constat nous a amené à proposer l'approche MBN dans le but de pouvoir réagir en temps réel à des évènements particuliers du réseau. En effet, TCP, par son mécanisme de boucle de contrôle de bout en bout, ne peut pas réagir assez vite à des changements se produisant au milieu du chemin entre la source de la connexion et sa destination. De plus, TCP est aussi limité par les paramètres qu'il considère et sa façon de les interpréter. Pour MBN et son architecture MBA associée, nous avons donc été amenés à faire les choix suivants :

- ***Prise en compte de l'hétérogénéité de la topologie Internet :***
  La première caractéristique de l'approche MBN est d'utiliser les informations sur les changements du trafic. Pour cela, il est nécessaire de mesurer les paramètres de trafic et de QoS localement et sur des longues distances lorsqu'une connexion traverse plusieurs domaines. La figure 15 représente la politique avec laquelle les systèmes de métrologie peuvent être déployés dans l'Internet. Précisons que nous sommes fermement persuadés que les équipements de métrologie et de mesure qui sont de plus en plus populaires et de plus en plus déployés dans les réseaux opérationnels devraient se généraliser dans un avenir proche. De plus, même s'il est impossible de dire que tous les liens et tous les routeurs de l'Internet seront « monitorés » un jour, nous défendons l'idée que la prise en

compte des résultats apportés par les outils de métrologie et de mesure effectivement déployés dans l'Internet seront d'un grand intérêt pour améliorer le comportement et la gestion de l'Internet. MBN repose donc sur le principe suivant : permettre une augmentation des performances et du niveau de QoS dans le réseau en tirant parti des informations de mesure disponibles. De plus, dans le cas où les informations de mesure ne sont pas présentes en certains points, le réseau doit continuer à fonctionner avec de bonnes performances et un niveau de QoS acceptable.

- ***Utilisation de mesures intra-domaine :***
  Ainsi, en ayant étudié la topologie administrative de l'Internet, nous proposons d'utiliser différentes techniques de mesure pour ce faire. Les mesures intra-domaine de paramètres comme le taux de perte, la bande passante utilisée et disponible, le nombre de flux, etc. peuvent être réalisées grâce à des équipements passifs (par exemple à l'aide d'outils NetFlow ou basés sur le protocole SNMP ou encore de systèmes DAG). Cette tâche est rendue possible car la plupart des domaines sont administrés et gérés par une entité unique et que la plupart des outils de métrologie ou du moins de gestion du réseau sont déjà présents. De plus, les outils de mesures passives apportent des informations sur le trafic avec le point de vue de l'opérateur du réseau[23] qui est le point de vue le plus adapté pour connaître l'état général d'un système autonome (ou AS). En fait, seules les mesures de délai seront réalisées de façon active pour des raisons de commodité (mesurer le délai par l'intermédiaire de techniques passives est plus difficile étant donné qu'il est nécessaire de pouvoir suivre les paquets tout au long de leur parcours).

- ***Utilisation des mesures inter-domaines :***
  D'autre part, pour les mesures inter-domaines, il est impossible d'utiliser les techniques passives étant donné que les autres domaines ne sont pas gérés de la même façon et que leurs administrateurs peuvent potentiellement ne pas utiliser des techniques de mesure, ou pas nécessairement les mêmes techniques. De plus, même si des mesures sont réalisées sur leur domaine, les FAI étant en concurrence les uns avec les autres, ils n'accepteront pas forcément de partager de telles informations de mesure[24]. D'un autre côté, si des informations de mesure sont mises à disposition, on peut ne pas forcément leur accorder un niveau de confiance maximal à cause de cette concurrence entre opérateurs. Ainsi, dans ce dernier cas, il est nécessaire d'utiliser des techniques de mesures orientées utilisateur. Plus précisément, pour obtenir des informations sur d'autres domaines, la meilleure solution consiste à mesurer les paramètres requis par l'intermédiaire de techniques actives, c'est à dire en envoyant des paquets à travers les autres domaines et en mesurant ce qui arrive à ces paquets sondes (ce trafic de sondes devant naturellement rester faible et non intrusif).

- ***« Reporting » des mesures :***
  Ainsi, l'ensemble de ces mesures réalisées en temps réel et signalées aux sources de trafic (i.e. les utilisateurs du service), leur apporte une connaissance de l'état du réseau et du trafic, et leur permet d'adapter leur débit d'émission aux ressources disponibles. Il est important de noter cependant qu'un autre aspect important de l'architecture MBA et de son système de métrologie global concerne le développement d'un protocole de « reporting » des informations de mesure. Ce dernier devra nécessairement fonctionner en intra-

[23] Les mesures passives sont généralement considérées comme une catégorie d'information plus facilement exploitable par les opérateurs.
[24] Il est indispensable pour les FAI de se différencier les uns des autres, en fournissant des services de meilleure qualité que les concurrents, afin d'attirer les clients.

domaine, mais aussi être étendu à une configuration de « reporting » inter-domaines. Cependant, étant donné qu'il est difficile de savoir si une information apportée par un FAI « partenaire » est correcte, nous recommandons de conserver l'utilisation des méthodes de mesures actives pour une telle action. Rappelons aussi que les informations de mesure peuvent manquer, par exemple si un utilitaire de mesure connait une défaillance, si certains liens sont congestionnés entrainant une perte des paquets de signalisation, ou si votre FAI « partenaire » décide soudainement de ne plus coopérer avec vous. Nous avons ainsi défini l'approche MBN pour permettre de continuer à fonctionner, même si les informations de mesure sont totalement ou partiellement manquantes.

2.3.3. MRP : un protocole de « reporting » pour un système global de métrologie

Le principal challenge à relever pour MBA est donc de concevoir un système de métrologie global afin qu'une source de trafic puisse disposer de toutes les informations utiles sur l'état du réseau et de son trafic, pour pouvoir réagir et s'adapter à ses évolutions. Un système de métrologie global pour l'Internet devra donc remplir deux fonctions :

1) réaliser des mesures, superviser le trafic et analyser les résultats locaux ;
2) diffuser ses rapports d'analyse à tous les équipements du réseau ou aux hôtes, qui eux réaliseront une analyse globale à partir de tous les rapports reçus des différents points de mesure.

Le mécanisme de « reporting » reste un des points durs à résoudre pour pouvoir disposer d'un système de métrologie global dans l'Internet. Dans un tel contexte, le mécanisme de « reporting » devra :

1) Etre réactif. En effet, pour que le système de métrologie global soit utile pour des fonctions comme le contrôle de congestion, le contrôle de trafic ou la gestion de la QoS, il faudra que les informations qu'il rapporte soient de « toute première fraîcheur ». Pour les exemples cités ci-dessus, les délais ne doivent pas excéder quelques dizaines de millisecondes.
2) Etre scalable, i.e. fonctionner avec de bonnes performances même si des millions de machines interviennent dans le système. Dans le cadre du mécanisme de « reporting » cela se traduit par le besoin de limiter la quantité de trafic de reporting au maximum.

MRP est un protocole de « reporting » qui a été conçu de façon à satisfaire ces 2 besoins. Il faut noter que pour l'instant, dans la littérature existante, les mécanismes de « reporting » se sont essentiellement focalisés sur la propriété de scalabilité. Considérer en même temps le niveau de réactivité est une caractéristique originale de MRP qui apparaît cependant comme indispensable pour que le système de métrologie global puisse servir à améliorer des fonctions réseaux qui nécessitent des temps de réactions aux changements très courts. C'est le cas, par exemple, de fonctions comme le contrôle de congestion. Jusqu'à présent, les mécanismes de « reporting » qui ont été conçus ne ciblaient que des fonctions réseaux n'ayant pas besoin de réagir très vite aux événements observés, comme par exemple l'ingénierie de trafic ou le routage adaptatif, pour lesquels des actions ne seront lancées que si le changement dans l'état du réseau est persistant (et ce, afin d'éviter les mécanismes de « route flapping »). Ainsi, en faisant un tour d'horizon de la littérature sur les mécanismes de « reporting » entre sondes de mesure, il semble que seules 2 approches génériques se distinguent :

1) le polling [Sal 01] qui consiste à interroger périodiquement les équipements de mesure ;
2) le monitoring réactif dans lequel l'équipement de mesure diffuse, périodiquement ou lorsqu'un changement survient, le nouvel état local du réseau [Dil 01].

Le problème majeur de ces approches est la production excessive de trafic de « reporting » alors qu'il faudrait concilier passage à l'échelle et réactivité du protocole. Les travaux actuels montrent une orientation pour des approches abordant l'aspect scalabilité mais au détriment de la réactivité ([Asg 02], [Asg 04], [Dil 01] et [Els 05]). Par exemple, AMoS (Autonomous Monitoring of Streams) est un mécanisme de « reporting » adapté aux grands réseaux, car il génère peu de trafic [Els 05], mais a contrario présente de forts délais entre la détection d'un évènement et son « reporting ». Pour résoudre un problème de contrôle de congestion ou de détection d'intrusion, AMoS n'est pas satisfaisant. A l'inverse, [Dil 01] propose un mécanisme réactif mais générant une surcharge de trafic conséquente. Ainsi, l'objectif de MRP est d'être un protocole de « reporting » qui allie réactivité et scalabilité.

Le protocole de reporting MRP : principe

Vu ces résultats de caractérisation et d'analyse du trafic, il nous a semblé judicieux de coupler MRP à la transmission des flux éléphants, et d'en signaler les grosses variations pour que, dans un premier temps, leurs sources s'auto-régulent. MRP est un protocole que nous avons construit à partir de RSVP [Bra 97] : MRP étant couplé à la transmission des éléphants, il est donc orienté connexion de bout en bout. En utilisant le principe de RSVP, un premier paquet découvre le chemin de la source à la destination et ensuite un paquet de retour revient à la source en remontant le chemin aller. La différence avec MRP est que le paquet de retour (qui est un paquet de réservation dans RSVP) transporte des informations de mesure. D'autre part, les paquets de « reporting » sont envoyés chaque fois que nécessaire, alors que dans RSVP, le paquet de réservation n'est envoyé qu'à l'ouverture de la connexion. En fait, MRP utilise juste le principe de RSVP qui consiste à trouver un chemin et à revenir le long de ce même chemin. Cette méthode permet à MRP d'identifier parfaitement quels sont les composants réseaux (les routeurs, que nous appellerons routeurs MRP) rencontrés sur le chemin et de limiter le nombre de sources et de destinations pour les messages de « reporting ».
Le fait de ne considérer que les flux éléphants permet aussi de répondre au problème de scalabilité : seuls 3% des flux sont des éléphants (même s'ils représentent plus de 60% de la quantité de trafic dans le réseau [Owe 06]). MRP n'aura donc à gérer qu'un tout petit nombre de flux. Ainsi, les routeurs MRP n'ont besoin de ne conserver qu'une information sur les flux éléphants les traversant. Cette technique permet de limiter le nombre d'entrées dans la table de connexion. D'autre part, le « reporting » MRP ne se fera qu'à partir des routeurs MRP traversés par des éléphants et selon la matrice des flux éléphants. A priori cela peut exclure certaines zones du réseau du « reporting » et nuire à l'aspect global souhaité avec MRP. Toutefois, dans un réseau maillé comme l'Internet, et possédant des propriétés de petit monde [Fal 99], nous avons toujours observé que les informations de mesure se propagent dans tout le réseau, même si elles ne sont pas transmises en mode multicast ou broadcast. Cela a été montré par les simulations décrites ci-après.
Enfin, pour encore améliorer la scalabilité de MRP, nous avons choisi de n'envoyer les informations de « reporting » que lorsqu'une rupture est détectée dans le trafic. Cette technique permet de ne générer du trafic de « reporting » que quand les conditions du réseau changent. Etant donné son principe de réaction basé sur la détection de ruptures, ce mécanisme va donc limiter la quantité de données de « reporting » et permettre aux émetteurs et aux routeurs de disposer très rapidement d'informations importantes sur l'évolution du réseau et du trafic. En procédant de la sorte, nous répondons aux problèmes de scalabilité et de réactivité de MRP.

Evaluation

Le but de cette évaluation est de mesurer la quantité de trafic de « reporting » généré par MRP ainsi que le temps de réaction entre l'apparition d'une variation de trafic ou de QoS et la réception de cette information dans tout le réseau. Pour ces évaluations, nous avons utilisé NS-2. Pour disposer d'une topologie réaliste, nous nous sommes basés sur la carte du réseau d'AT&T incluse dans Rocketfuel ([Spr 02a] et [Spr 02b]) et utilisée par [Els 05] pour évaluer AMOS. Au niveau du trafic de fond, la solution proposée pour simuler du trafic réaliste est présentée dans la partie 2.4 et est détaillée dans [Owe 04a]. Cette méthodologie recrée un trafic simulé statistiquement équivalent à un trafic réel. Dans cet environnement de simulation, nous avons évalué MRP (trafic de « reporting » et délais) pour de nombreuses valeurs de ses paramètres de configuration. Ces paramètres sont :

1) La granularité du système de mesure. Pour expliquer ce paramètre, on peut, par exemple, citer le mode de calcul pratique du débit instantané du débit qui est calculé comme le débit moyen sur de courtes périodes de temps (période P que l'on appelle aussi granularité). Ce paramètre a un impact fort étant donné que plus la granularité est importante, plus le débit semble lisse. En conséquence, cette granularité va agir sur le volume de trafic de « reporting » généré par MRP (plus la granularité choisie sera faible, plus la détection des variations se fera de façon précise et plus le volume de trafic de « reporting » sera important). Plusieurs périodes de 0,2 à 5 secondes ont donc été testées.
2) Le seuil de détection des changements dans le trafic : il s'agit de la variation minimale (seuil) entre deux mesures consécutives pour lequel nous pouvons considérer que les conditions du réseau ont changé et qu'il est donc nécessaire de diffuser cette information. Ce seuil est exprimé en pourcentage de la capacité totale du lien.
3) La valeur de « Time Out » (TO) qui correspond à l'introduction d'un « reporting » périodique dans MRP nécessaire pour informer les routeurs MRP concernés des évolutions lentes du trafic, sans aucune rupture, mais qui peuvent néanmoins conduire à des tendances non stationnaires. Cette valeur est définie par rapport au paramètre P. Elle doit donc être beaucoup plus importante que P. En suivant ce principe, nous avons sélectionné empiriquement les couples (P, TO) : (P = 0,2s et TO = 2s), (P = 0,5s et TO = 4s), (P = 1s et TO = 5s), (P = 2s et TO = 8s) et (P = 5s et TO = 10s).

Les résultats d'évaluation sont représentés sur la figure 1 qui montre le ratio entre la charge de trafic de « reporting » et le trafic total en fonction de la granularité du système de mesure et le seuil de détection des ruptures. Il apparaît que le pourcentage de trafic de « reporting » MRP n'excède jamais 1% du trafic global, ce qui amène à dire que le protocole MRP peut fonctionner à grande échelle. Sans surprise, cette quantité de trafic de « reporting » avec MRP est un peu supérieure à celle obtenue avec AMoS. A contrario, en termes de réactivité, MRP est infiniment meilleur. Les délais avec MRP sont peu différents de la période P (au délai de transmission près, qui reste faible par rapport à P). Dans le cas d'AMoS, les délais peuvent être 20 fois plus importants que ceux obtenus avec MRP. Si la conséquence d'un évènement est une congestion, la réactivité d'AMoS est donc difficilement acceptable.

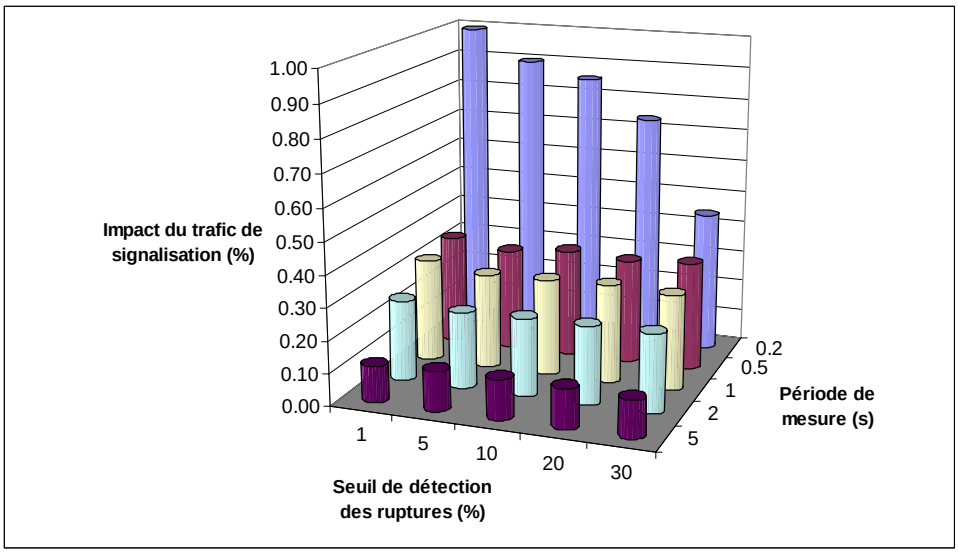

Figure 16 : Surcharge du trafic de signalisation par rapport au trafic total

Discussion

MRP est donc un protocole de « reporting » scalable et réactif pour un système de métrologie global. Il peut paraitre surprenant de se servir de RSVP comme protocole de base pour MRP alors que RSVP a justement conduit à la perte de l'approche IntServ par son manque de scalabilité. Il est important de noter ici que l'utilisation de RSVP n'a été décidée qu'après une étude et une analyse des caractéristiques du trafic Internet qui incriminait les flux éléphants. En se limitant aux flux éléphants, on réduit du même coup le nombre de flux qu'il faudra gérer avec MRP, et comme les flux éléphants sont peu nombreux en nombre, cette solution devient très scalable.
On peut également légitimement comparer MRP et l'approche ECN [Flo 94]. En fait, nous avons adopté le même principe de segmentation des connexions pour permettre des réactions plus rapides. Toutefois, nous avons étendu le concept ECN de façon significative en permettant l'utilisation d'un système de métrologie complet, et en le rendant capable de réagir à tous types d'événements. De plus, les routeurs MRP qui possèdent une base de données contenant des informations provenant des quatre coins du réseau permet de diffuser des informations sur l'état global du réseau (et pas seulement local comme avec ECN).
Enfin, même s'il est vrai que AMoS est plus scalable que MRP nous pensons que la réactivité est un élément essentiel sans lequel un système de métrologie global n'aurait guère plus d'intérêt que SNMP et ses MIB. MRP a d'ailleurs montré tout son potentiel dans le cadre d'un mécanisme de contrôle de congestion adaptatif appelé MBCC (Measurement Based Congestion Control) qui nécessite une grande réactivité et de pouvoir fonctionner dans un réseau à large échelle. MBCC fait l'objet de la partie suivante

2.3.4. MBCC

MBCC est un mécanisme de contrôle de congestion pour l'Internet qui est le fruit des réflexions qui ont fait suite aux résultats de caractérisation et d'analyse du trafic et de la QoS des réseaux de l'Internet que nous monitorons. Ces résultats avaient conduit à la définition de l'approche MBN et de son architecture associée MBA. MBCC repose donc sur cette architecture et cette approche. D'autre part, comme la partie 2.2 a montré les méfaits de TCP sur le trafic lorsqu'il est utilisé pour transporter les flux éléphants, et la partie 2.2.3 les

bienfaits de TFRC qui lisse le débit de ses sources de trafic, c'est tout naturellement que MBCC a été proposé comme une version de TFRC utilisant MBN/MBA, i.e. capable de profiter des résultats de mesures venant des différents points du réseau grâce à MRP.
Le principe de MBCC consiste à utiliser l'algorithme de TFRC pour calculer le taux d'émission nominal de chaque connexion et de corriger cette valeur grâce à la connaissance du niveau de bande passante disponible et consommée dans le réseau. Ainsi, si une fraction de la bande passante est disponible, les sources pourront générer plus de trafic qu'indiqué dans l'équation de TFRC (qui correspond au débit d'un flux TCP [Alt 00]) sans pour autant créer des pertes et des congestions dans le réseau. Ainsi, le niveau de congestion du réseau devrait être significativement réduit en déployant des sources de trafic «pro-actives», capables d'adapter en temps réel leur débit d'émission en fonction des ressources disponibles. Un tel mécanisme devrait aussi aider à augmenter l'équité entre les flux, étant donné que la correction réalisée sur le débit d'émission ne devrait pas dépendre de la valeur du RTT mais de la réelle fraction de bande passante disponible équitablement partagée entre les flux concurrents. MBCC sera uniquement utilisé pour les flux éléphants qui sont les flux qui génèrent le plus de perturbations dans le réseau. A l'opposé, comme le trafic «souris» représente un bruit blanc Gaussien [Ben 03], il n'induit pas de problème de transfert important et il n'est donc pas nécessaire de modifier leur protocole de transport. Ainsi, pour une période normale (quand les informations de mesure sont correctement reçues, qu'il n'y a pas de congestion et que de la bande passante est disponible dans le réseau), chaque flux éléphant peut utiliser une fraction supplémentaire des ressources qui sont disponibles. Cette fraction est calculée en divisant la bande passante totale disponible par le nombre de flux moyens éléphants dans le réseau à ce moment (ces informations étant fournies par les équipements de mesure rencontrés tout au long du chemin). Il est logique de diviser la bande passante disponible par le nombre moyen de flux actifs N traversant ce lien car il a été démontré que les arrivées de flux éléphants sont proches d'un processus Poissonien [Ben 03]. En effet, pour un processus de Poisson, comme la moyenne est égale à la variance, le nombre moyen est significatif car les valeurs du processus ne seront jamais très éloignées de cette valeur moyenne. A l'inverse pour une période de congestion, les émetteurs MBCC devront réduire leur débit d'émission pour résorber la congestion et ceci en essayant d'être aussi équitable que possible. Dès lors, les sources MBCC envoient la valeur minimale entre le débit TFRC et le débit effectif obtenu par un flux à ce moment au niveau du goulot d'étranglement sur son chemin. Ainsi, les équations de cet algorithme peuvent être résumées de la façon suivante :

$$Si\_pas\_de\_congestion(p=0), X_{MBCC} = X_{TFRC} + \frac{bande\_passante\_totale\_disponible}{N}$$

$$Si\_congestion(p \neq 0), X_{MBCC} = \min(X_{TFRC}, bande\_passante\_consommée)$$

Ce nouveau mécanisme de contrôle de congestion a montré tout son potentiel et ses bienfaits lors de son évaluation basée sur l'utilisation du simulateur NS-2 et des techniques de rejeu décrites dans la partie 2.4.1, à même de fournir des simulations réalistes. Une des topologies utilisées (la plus simple) est décrite sur la figure 17 (Des simulations sur des topologies plus complexes sont décrites dans à [Lar 05a] et [Lar 05b]). Elle représente deux réseaux de bordure avec une bande passante très élevée et un réseau d'accès avec une capacité beaucoup moins importante que celle des liens de bordure. Ce lien représente le lien le plus « congestionné » sur le chemin considéré, c'est à dire celui qui aura le plus d'impact sur le débit d'émission de MBCC. Cette différence de capacité devrait induire des périodes de congestion importante où les apports de MBCC pourront être analysés, et son niveau de

performance comparé avec les autres mécanismes de contrôle de congestion en particulier ceux des deux versions de TCP : TCP New Reno et TCP SACK[25].

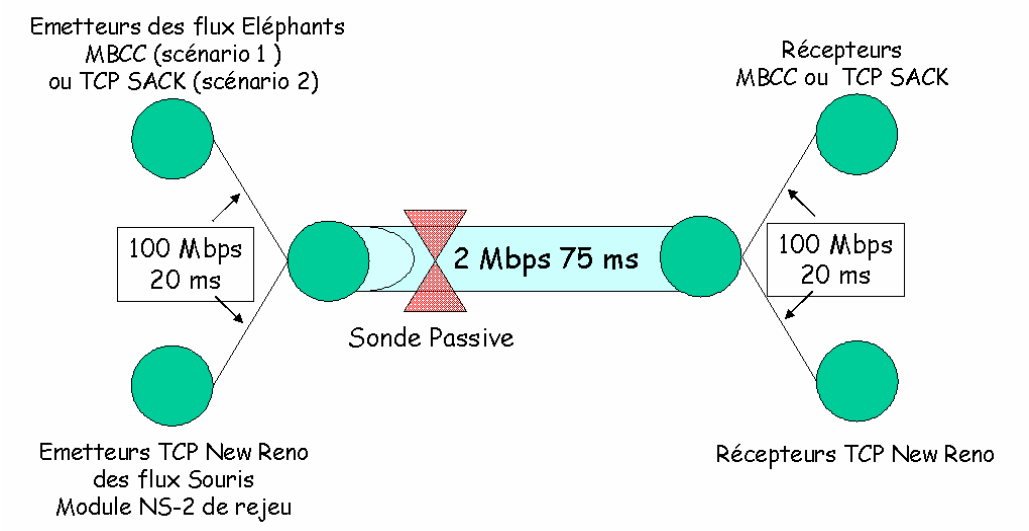

Figure 17 : Topologie du réseau utilisé dans les simulations NS-2

L'objectif principal de cette étude est de comparer les possibilités d'adaptation de MBCC au regard des augmentations (et diminutions) de charge du réseau ainsi que des autres mécanismes de contrôle de congestion. Les paramètres qui seront mesurés et calculés à partir de ces mesures sont les mêmes que pour la partie 2.2.3.
Deux scénarios ont été définis : dans le premier, les flux éléphants sont transmis en utilisant MBCC alors que dans le deuxième scénario, les éléphants sont transmis en utilisant TCP SACK. Dans ces deux scénarios, les flux souris sont émis en utilisant TCP New Reno. Ces deux expériences ont permis de comparer les contributions respectives de TCP et MBCC sur le niveau de congestion dans le réseau.

Dans un premier temps, on peut remarquer que les performances globales de MBCC sur le trafic sont meilleures (cf. tableau 4) : le coefficient de stabilité pour MBCC est plus élevé que pour TCP SACK, de même que le débit moyen. Ceci démontre que MBCC est capable de consommer la bande passante disponible qui ne peut pas être utilisée par TCP. Ce résultat montre que toutes les ressources ont été consommées de façon efficace. De plus, l'écart-type de TCP SACK est beaucoup plus important que celui de MBCC. En conclusion, ces résultats montrent un plus haut niveau d'adaptation de MBCC qui lui permet, contrairement à TCP, d'optimiser l'utilisation de la bande passante disponible, en gardant le niveau d'oscillation très bas, et ainsi conserver un service stable. De plus, en permettant une diminution des oscillations du trafic, MBCC libère une part de la bande passante habituellement utilisée en raison des oscillations engendrées par TCP SACK. Ainsi, ces ressources libres peuvent être, dans un deuxième temps, utilisées pour échanger des données utiles. Dès lors, avec MBCC l'utilisation des ressources du réseau est optimisée par rapport à ce qu'elle peut être avec TCP SACK.

[25] A noter que, par construction, MBCC est plus performant que TFRC [Lar 05b].

	Flux Souris TCP New Reno	Flux Eléphants	
		MBCC (scénario 1)	TCP SACK (scénario 2)
Débit moyen (A) (B/s)	10348.7	243738.2	242014.2
Ecart-type du débit (σ) (B/s)	6898.3	16350.5	19585.5
Coefficient de stabilité (SC)	1.500	14.907	12.357

Tableau 4 : Analyse de la variabilité du trafic

Cette meilleure optimisation des ressources disponibles est rendue possible car MBCC crée moins de congestion que TCP dans le réseau. La figure 18 montre le nombre de pertes cumulées à la fois pour le trafic MBCC et TCP SACK. Il est ainsi clair que MBCC induit moins de pertes dans le réseau que TCP SACK, le nombre de retransmissions et la consommation inutile de bande passante seront moindre. Ces ressources pourront ainsi être allouées pour la transmission du trafic utile.

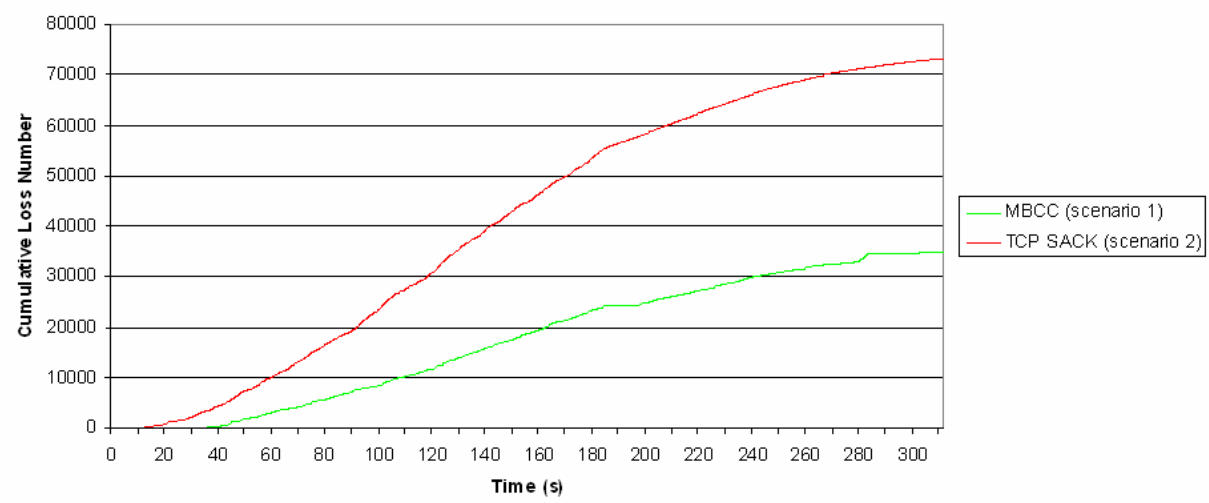

Figure 18 : Processus de perte

En dernier lieu, MBCC a un impact très important sur la LRD du trafic. En fait, grâce à MBCC, la LRD est beaucoup plus réduite dans le trafic global avec MBCC pour lequel H = 0,66 en comparaison du trafic de référence TCP où la LRD est très élevée (H = 0,88).

2.3.5. Conclusion

Cette partie vient de présenter notre proposition d'architecture adaptative MBA pour permettre d'améliorer la QoS du service « best effort » et le rendre capable de fournir des services satisfaisants (sans garantie toutefois) pour toutes les applications qui utilisent aujourd'hui l'Internet, y compris celles qui nécessitent du temps réel (souple). Cette architecture utilise un système de métrologie global, déployable à l'échelle de l'Internet, qui est à la fois compatible avec de grands réseaux et très réactif. L'élément clé de ce système de métrologie global est le protocole de « reporting » MRP.

Comme nous l'avons déjà vu, l'approche MBN s'inspire de l'approche ECN (Explicit Congestion Notification) [Flo94] dont elle reprend le principe de supervision au milieu du chemin emprunté par les connexions, pour des réactions plus rapides et plus sûres par rapport à ce que TCP peut faire. Toutefois, MBN est plus générique qu'ECN : les outils de métrologie

du réseau ne se cantonnent pas à observer le niveau de congestion des files d'attente des routeurs. Ils peuvent mesurer et superviser toutes sortes de paramètres du trafic, du routeur, de la QoS, etc. pour permettre la mise en place de n'importe quelle forme de politique de gestion du réseau, du trafic ou de la QoS. De fait, MBN n'a pas pour but de ne fonctionner qu'avec TCP, mais au contraire il est à la base proposé comme une alternative à TCP dans l'Internet (dont les méfaits ont été analysés dans la section 2.2).

Nous pensons que l'approche MBN peut être une solution universelle pour la gestion de l'Internet et de son trafic pour optimiser le niveau de QoS de la classe « best effort », mais sans doute aussi n'importe quelle classe de service définie dans une approche à la mode DiffServ. En particulier, l'approche MBN a été définie pour être capable de fournir une solution adaptée quel que soit le type de réseau, la nature du trafic ou des conditions réseaux. Pour l'instant, le concept MBN a été appliqué seulement sur une étude de cas précise : le mécanisme de contrôle de congestion MBCC (« Measurement Based Congestion Control »). Cet exemple a montré tout le potentiel et les bénéfices que l'on peut obtenir avec des méthodes adaptatives. Nous pensons également qu'une telle approche peut être bénéfique pour de très nombreuses fonctions réseau parmi lesquelles : l'optimisation de la QoS, la gestion du trafic, la détection et la prévention contre les intrusions, etc.

2.4. La métrologie dans les expérimentations réseaux

La recherche et l'ingénierie réseaux sont des activités qui ont des besoins expérimentaux très forts, et ce, afin de tester, vérifier, valider le comportement des réseaux, de leurs protocoles et mécanismes, et s'assurer qu'ils remplissent bien leurs missions avec les performances attendues. C'est le cas par exemple de l'approche MBN présentée plus haut, du protocole MRP et du mécanisme de contrôle de congestion associé MBCC que nous proposons. Pour ce faire, et avant de tester ces solutions en environnement réel, il existe deux types d'outils : les simulateurs (qui font tourner – sur une machine – un modèle du réseau, de son architecture, de ses composants et de ses protocoles), et les émulateurs (pour lesquels les protocoles et applications aux extrémités sont exécutés en vrai sur leur machines, et pour lesquels les éléments du cœur du réseau sont reproduits selon un modèle).
Les deux lacunes principales aujourd'hui avec les simulations et les émulations sont :

- L'échelle limitée des scénarios : les simulateurs couramment utilisés aujourd'hui en réseau, appelés simulateurs événementiels, ont des capacités assez réduites, et il est impossible de simuler de grands réseaux avec des capacités de communication importantes. De même, en émulation, c'est le coût de la plate-forme, dont le nombre de machines la composant est forcément limité qui interdit des scénarios à grande échelle.
- Le manque de réalisme des scénarios testés, et qui conduisent la plupart du temps à des résultats optimistes.

C'est d'ailleurs pour corriger ce second point que nous avons proposé et développé une méthode utilisant la métrologie en simulation et émulation.

2.4.1. Problématique de la simulation des réseaux de l'Internet

2.4.1.1. Pourquoi est-il si difficile de simuler l'Internet ?

Les caractéristiques des trafics observés sur les différents liens que nous avons étudiés et la littérature sur ce sujet montrent bien que le problème de la modélisation des trafics de

l'Internet reste pour le moment une tâche ardue. Comme nous l'avons déjà dit, les nombreuses approches reposant sur des modèles connus comme les modèles Poissonniens, Markoviens, les modèles ON/OFF [Lel 94], les modèles de files d'attente, M/G/1/N, Mk/Gk/1/N [Gar 01], les mouvements fractionnels Browniens caractéristiques des comportements auto-similaires, ou même les modèles à base de fractales [Fel 98] ne parviennent pas à représenter toutes les caractéristiques du trafic Internet sur un lien. Cette difficulté dans la modélisation des trafics engendre également des difficultés pour réaliser des simulations réalistes de l'Internet. C'est ce qui est mis en évidence dans [Flo 01] qui montre qu'il est extrêmement complexe de simuler de tels trafics, en particulier à cause des caractéristiques d'auto-similarité, LRD ou multi-fractalité qui ont pu être mises en évidence lors des premières analyses de trafic des liens de l'Internet. Cette difficulté est une réalité, déjà sur un seul lien. Or, il apparaît également que les caractéristiques, et donc le modèle pour les représenter, sont différents d'un lien à un autre, sans qu'il soit aujourd'hui possible de connaître les règles de dépendance d'un lien à l'autre. L'ingénierie des réseaux de l'Internet à partir de modèles formels du trafic est donc une activité à développer, et qui prendra certainement de nombreuses années. Pour pouvoir continuer à développer et améliorer l'Internet actuel, il est toutefois essentiel de mettre en place des techniques de simulations et d'expérimentations réalistes. Cette notion de réalisme est un problème majeur des outils de simulations actuels. Par exemple, dans les simulateurs actuels, les sources de trafic sont généralement des sources régulières comme des générateurs constants ou respectant des processus d'émission markoviens, soit, dans tous les cas, des sources de trafic plus régulières que le trafic de l'Internet. Cette régularité est assez dommageable pour le réalisme des simulations actuelles car les protocoles à étudier ne sont pas confrontés aux contraintes réelles du trafic, mais à des contraintes moins dures. Souvent, les protocoles ou nouvelles architectures issues de ces simulations, et qui donnaient satisfaction lors des simulations, ne fournissent pas les mêmes résultats lors des déploiements en environnement réel. Nous nous sommes donc attachés à utiliser la métrologie pour améliorer le réalisme des environnements dans lesquels sont faites les simulations (dans un premier temps) Internet.

2.4.1.2. Les deux approches de simulation

De façon évidente, la métrologie modifie le processus d'ingénierie réseau en ajoutant en amont une phase de caractérisation et d'analyse du trafic, comme cela a été développé dans ce manuscrit. D'autre part, vu les difficultés à modéliser le trafic, les approches entièrement formelles qui pouvaient être utilisées jusqu'à présent dans l'ingénierie des réseaux et des protocoles (et représentées sur la figure 19 comme l'approche 1), sont aujourd'hui difficilement applicables et le resteront tant qu'un modèle formel du trafic ne sera pas trouvé. De fait, nous sommes forcés de nous rabattre sur une approche de simulation informelle, avec un simulateur comme NS-2 par exemple, qui est le simulateur recommandé par l'IETF. Avec ce type de simulateur, comme avec des simulateurs utilisant des approches formelles, il est difficile d'obtenir des résultats réalistes pour les mêmes raisons que précédemment : les sources de trafic ne prennent pas en compte toutes les caractéristiques d'irrégularité du trafic Internet, ni qualitativement, ni quantitativement. Pour cela, l'approche que nous proposons (et représentée comme l'approche 2 sur la Figure 19) consiste à utiliser la métrologie en rejouant les traces capturées par les équipements de métrologie dans le simulateur, de façon à avoir des sources de trafic réalistes et reproduisant les comportements des utilisateurs et de leurs applications. La suite va donc présenter comment fonctionne la méthode de rejeu de traces de métrologie que nous avons développée.

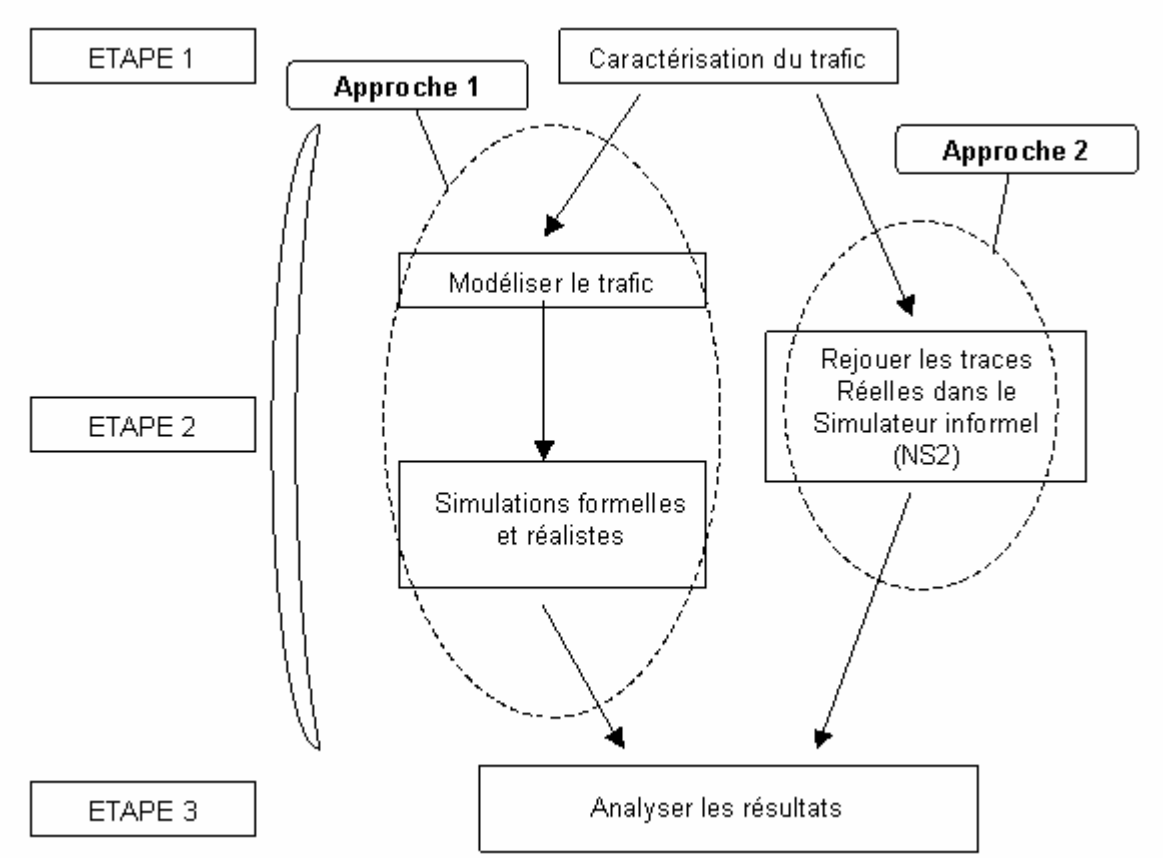

Figure 19 : Processus de recherche en réseau

2.4.1.3. Principe de la méthode de rejeu de trafic

L'environnement de simulation a la lourde tâche de mettre en forme le profil d'émission ; il est très important de le créer de façon à générer du trafic ayant les mêmes caractéristiques que le trafic réel. Le rôle des agents d'émission et de réception du simulateur qui vont injecter dans le réseau les flux aux moments opportuns et selon les tailles des paquets lus dans la trace réelle est primordial. En particulier, pour rejouer intégralement une trace les éléments caractéristiques du trafic réel qui doivent intervenir sont :

- les dates relatives des débuts de flux qui représentent le comportement réel des utilisateurs et applications ;
- les tailles des paquets à l'intérieur de chaque flux ; il a été en effet montré que c'est un des éléments qui peut être à l'origine de l'auto-similarité du trafic, propriété que l'on souhaite reproduire dans les simulations.

D'autre part, dans le cadre de flux UDP, dont les émissions des paquets sont dues aux requêtes des utilisateurs ou des applications, chaque paquet sera émis conformément à son estampille dans la trace. Pour TCP, par contre, l'émission des paquets dépend d'événements venant du réseau et de la mécanique du protocole qui va réagir en conséquence. Les dates d'émission des paquets TCP dépendent donc de l'environnement dans lequel le protocole fonctionne. La définition de la topologie de simulation nécessaire pour rejouer du trafic de façon réaliste est donc essentielle. Nous avons vu dans la partie 1.2.2.2 que le trafic Internet possédait des propriétés de LRD, et d'auto-similarité qui étaient dues à TCP et ses mécanismes de contrôle de congestion [Par 96] [Ver 00]. Comme les mécanismes sont basés

sur une réponse pré-définie aux pertes, il apparait que les principales caractéristiques du trafic réel à reproduire dans les simulations sont associées au processus de pertes. De plus, on sait que le RTT est un paramètre important pour les mécanismes de contrôle de congestion. En effet, il joue un rôle primordial pour les performances de TCP et le profil du trafic. Ainsi, notre méthode de rejeu propose de respecter ces paramètres pour les flux simulés.

De façon à construire une topologie capable de reproduire les taux de perte et RTT pour les différents flux, il est nécessaire d'extraire des traces originales, pour chacun des flux, les paramètres suivants :

- le taux de perte expérimenté par chacun des flux pendant leur transfert sur le réseau ;
- le RTT expérimenté par chacun des flux ;
- le débit moyen de chacun des flux ;
- la durée de chaque flux.

A partir de ces données, l'objectif consiste donc à faire emprunter à chacun des flux un chemin sur lequel il va subir, en simulation, le même taux de perte et le même RTT que dans le réseau réel. Ces informations sur les flux nous permettent de calculer la bande passante du lien et la taille de la file d'attente du routeur par lesquels le flux va passer, de façon à introduire statistiquement le taux de perte original. Pour limiter la complexité de la topologie de simulation, et en se basant sur les analyses des taux de pertes, nous avons décidé de définir seulement six classes de taux de pertes différentes (cf. tableau 5 pour détails).

classe	Taux de perte des flux de la classe (%)
C0	0
C10	0-10
C20	10-20
C30	20-30
C50	30-50
C100	50-100

Tableau 5 : Classes de flux utilisées pour rejouer les traces de métrologie

Au final, la topologie expérimentale pour une source qui permettra rejouer la trace considérée en reproduisant taux de perte et RTT est assez simple. Elle est représentée sur la figure 20 dans laquelle :

- QL_{Ci} est la taille de la file d'attente pour les flux de la classe i ;
- BW_{Ci} est la capacité du lien pour la classe Ci ;
- RTT_{Ci} est le RTT moyen des flux de la classe Ci.

QL_{Ci}, BW_{Ci} et $RTT_{Ci,}$ les paramètres de la topologie de simulation, sont ainsi facilement calculés à partir des paramètres mesurés pour chacun des flux de la trace originale.

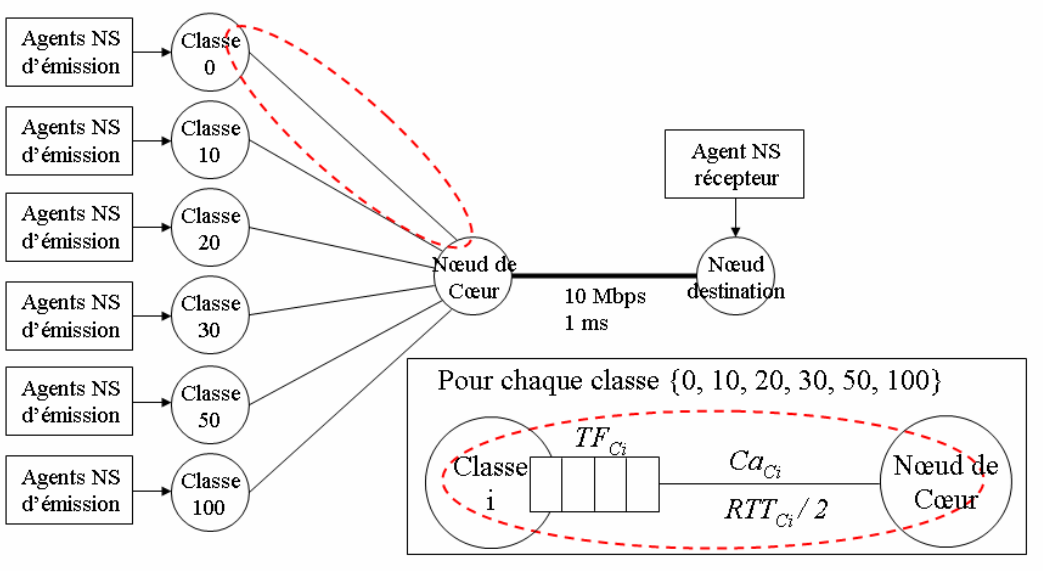

Figure 20 : Topologie expérimentale

2.4.1.4. Evaluation de la méthode de rejeu

L'évaluation de la méthode de rejeu est faite en comparant le trafic réel qui a été capturé et le « même » trafic rejoué dans le simulateur (NS-2 dans le cas présent). Les paramètres qui sont comparés sont bien évidemment les paramètres traditionnels du trafic (débit, nombre de paquets,…), mais aussi tous les paramètres qui sont en relation avec la dynamique du trafic, en particulier les moments statistiques d'ordre un et deux comme l'autocorrélation du trafic, et bien sûr la LRD. Théoriquement, pour vérifier que les deux processus qui génèrent les deux traces (réelle et simulée) sont identiques, il faudrait montrer qu'ils ont les mêmes moments à tous les ordres statistiques. D'un point de vue pratique, le troisième ordre et au delà ont très peu d'influence. Dans de telles évaluations expérimentales, il est généralement admis qu'il est suffisant de faire la vérification pour les deux premiers ordres.

Au final, les résultats obtenus en simulation sont très proches de ce qui a été observé sur les traces originales. Tout d'abord, nous avons bien observé que la moyenne du taux de perte que nous avons obtenu en simulation est la même que le taux réel pour chacune des classes considérées. Mais, et c'était le point essentiel, la mise en forme des paquets en simulation est statistiquement similaire à ce qu'elle était dans le cas réel.

La figure 21 présente la représentation Q-Q-Plot des deux séries d'inter-arrivées de paquets : pour la trace originale et pour la trace rejouée dans le simulateur. La correspondance entre les séries simulée et réelle est très bonne pour l'ensemble des valeurs, à l'exception des très grands quantiles pour lesquelles un petit nombre de points de la courbe s'éloignent de la première bissectrice. En effet, les deux analyses montrent que la seule différence vient de la proportion de paquets très proches temporellement qui est plus importante dans la trace réelle que dans celle simulée. Dans le cas réel, les paquets séparés par des durées très courtes sont celles des flux qui expérimentent un RTT très bas. En simulation, étant donné que nous avons défini pour tous les flux d'une classe le même RTT, les flux avec des RTT courts ne sont pas très bien rejoués. A l'ordre 2, la figure 22 représente la fonction d'auto-corrélation pour les deux cas. Il apparait clairement que notre simulation basée sur le rejeu de traces donne de très bons résultats pour les statistiques de second ordre, ce qui est un des problèmes principaux quand on souhaite rejouer du trafic.
Pour compléter notre analyse, il est nécessaire de calculer la fonction de LRD du trafic dans

les deux cas. Les résultats obtenus avec l'outil LDestimate sont présentés sur la figure 23. Il apparait que les LRD pour notre trace rejouée et pour la trace réelle sont très proches.

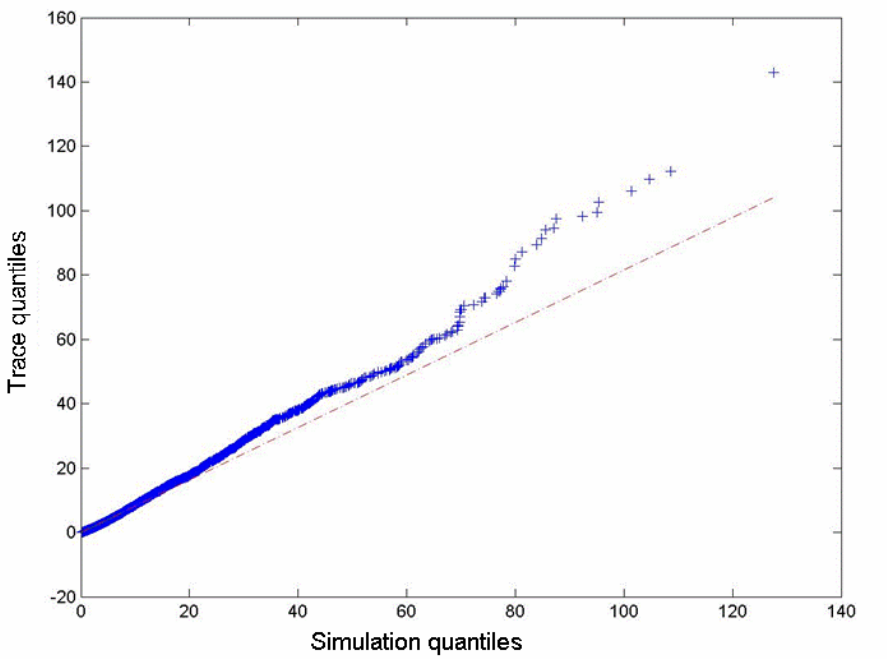

Figure 21 : Q-Q Plot des instants d'inter-arrivées des paquets (ms) des données de la trace (axe des Y) et des données de la simulation (axe des X)

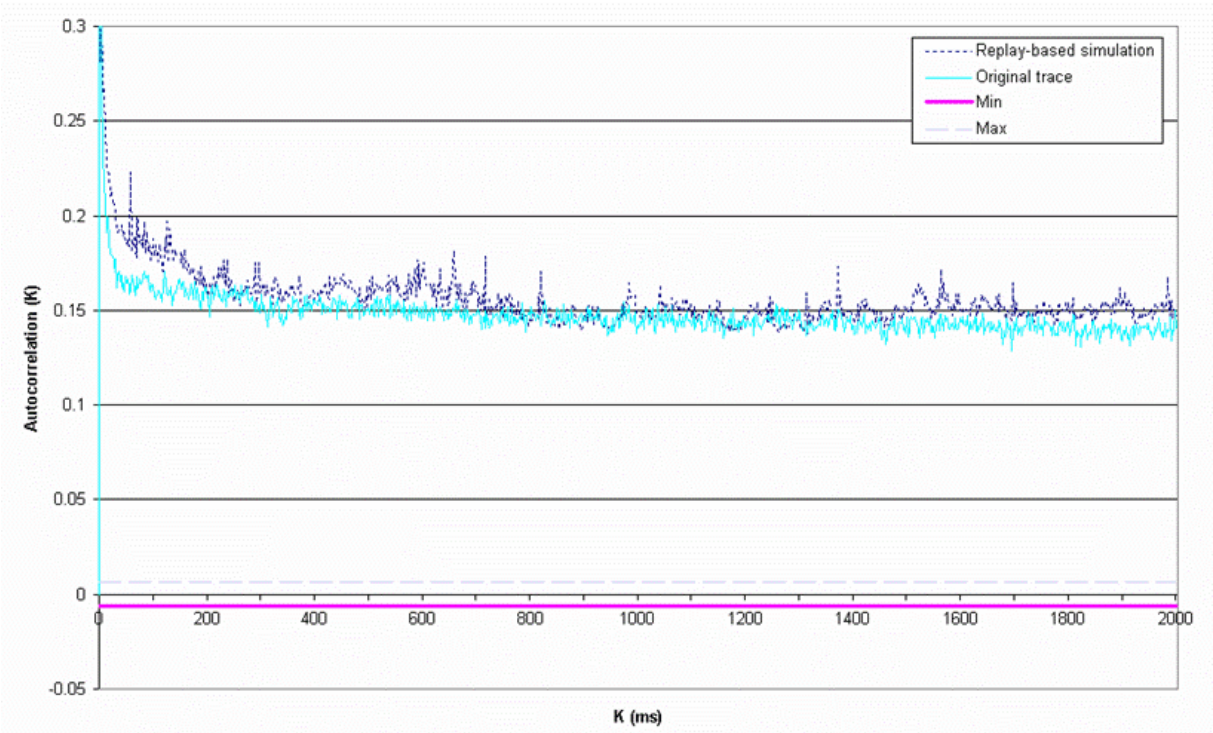

Figure 22 : Fonction d'autocorrélation des instants d'inter-arrivées des paquets

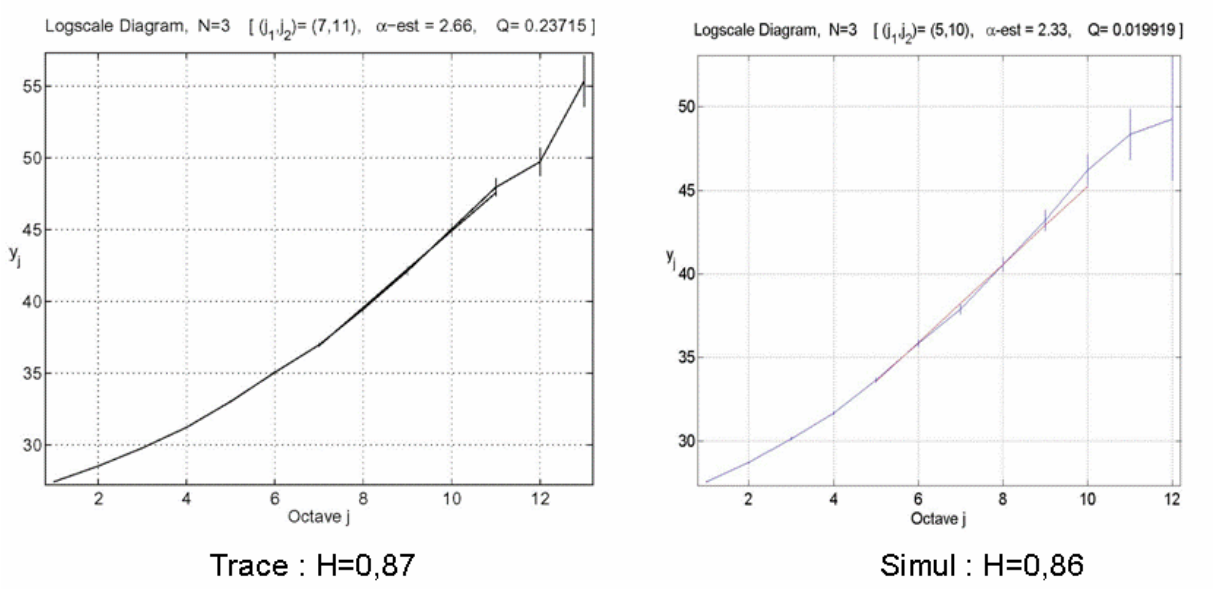

Figure 23 : Diagrammes LDEstimate des instants d'inter-arrivées des paquets (ms)

Au final, notre nouvelle approche basée sur le rejeu de traces de trafic capturées par un système de métrologie passif satisfait à ses objectifs. Elle a l'avantage important de construire des sources de trafic simulées possédant des caractéristiques et spécificités réalistes en terme de processus d'arrivée (de flux, de sessions) en accord avec ce qui est observé dans l'Internet. On a d'ailleurs montré qu'elle était un bon moyen pour arriver à obtenir des simulations réalistes, et ceci tant qu'un modèle complet du trafic Internet ne sera pas disponible.

Nos résultats de simulation sont vraiment encourageants et montrent que la simulation profite grandement de l'analyse métrologique du réseau. Cependant, nous avons aussi vu quelques petits défauts notamment en ce qui concerne les paquets séparés par des durées très courtes. Ce point devra être abordé lors de travaux futurs. Nous essaierons pour cela de définir une méthode permettant de construire une topologie de simulation qui se base à la fois sur des taux de pertes variables mais aussi des RTTs différents à l'intérieur d'une même classe de perte.

Toutefois, dans le cadre du projet STM (Sources de Trafics et Métrologie), interne au LAAS et financé sur fonds propres, nous essayons de trouver à partir d'études métrologiques du trafic, des modèles simples du trafic en fonctions de granularités d'observations pré-définies, pour pouvoir concevoir des générateurs de trafics fonctionnant à partir de ces modèles (cf. approche 1 de la figure 19). Nous reviendrons sur ce projet dans la partie 3.2.

2.4.2. Les projets de plates-formes

Comme cela a déjà été énoncé, la recherche en réseau est indissociable d'expérimentations, que ce soit dans des simulateurs ou sur des réseaux réels. C'est un des besoins forts que l'on rencontre dans presque tous les projets, et notamment au niveau du groupe de recherche OLC du LAAS. En particulier, après avoir évalué notre approche MBN et ses mécanismes protocolaires MRP et MBCC au travers de simulations, il faut, pour continuer son développement en vue d'un déploiement, l'implémenter et la valider sur des plates-formes d'émulation et d'expérimentation en environnement réel.

Dans cette optique, la stratégie que j'ai conduite pour le groupe OLC a consisté à s'investir sur deux plates-formes – Grid Explorer et laasnetexp.fr – décrites ci-après.

Grid Explorer

L'un des grands problèmes pour l'expérimentation vient de la quasi-impossibilité à franchir les facteurs d'échelle : par exemple, pour les simulateurs c'est impossible car cela nécessiterait des machines aux performances phénoménales et des capacités mémoires inimaginables aujourd'hui. Pour les expérimentations en environnement réel, il semble complètement impossible d'avoir un contrôle total sur un grand nombre de machines de l'Internet, en même temps qu'un contrôle total du trafic qui transite sur les réseaux de communications que toutes ces machines utilisent pour communiquer entre elles. Cette notion d'échelle est pourtant de première importance dès lors que l'on aborde des questions relatives à l'Internet. C'est pourquoi la solution qui semble la plus simple pour permettre de réaliser des expérimentations réalistes et exploitables est certainement l'émulation de réseaux combinée avec des techniques issues, en particulier, de la métrologie du trafic Internet pour pouvoir émuler des conditions réalistes. Par exemple, l'approche Planetlab, qui ouvre un réseau de stations de travail de par le monde aux expériences de la communauté de recherche en réseau mondiale, ne satisfait pas ce besoin de maîtrise du trafic sur le réseau qui interconnecte ces stations. De plus, [Ban 04] a montré que les stations de Planetlab sont généralement situées sur des réseaux académiques dont les trafics sont non représentatifs de ceux des réseaux commerciaux.

Dans ce contexte, les communautés de recherche en réseau, GRID computing, calcul intensif, … se sont fédérées autour du Projet GdX (Grid Explorer) financé par l'ACI Masse de Données et labellisé fin 2003. L'objectif de ce projet est de mettre en place une plate-forme d'émulation de réseaux (au sens large) à grande échelle. La cible est une plate-forme de 1000 processeurs (500 machines bi-processeurs). Aujourd'hui, la plate-forme comporte 640 processeurs et est opérationnelle. Des extensions de financement permettent de penser que l'objectif des 1000 processeurs sera atteint d'ici à la fin du projet, ce qui en fera la plus grande plate-forme d'émulation réseau au monde (loin devant les petits clusters que nous déployons dans nos laboratoires avec 10 ou 20 machines ou emulab).

GdX doit permettre de mettre en œuvre toutes sortes d'expérimentations. Cela signifie qu'il faut pouvoir mettre en place sur les mêmes équipements des topologies qui conviennent à des expérimentations sur chacun de ces domaines, et ce sans introduire des travaux de migration trop lourd, voire même permettre si possible de mener deux expériences en simultané, et isolées l'une de l'autre, sur la même plate-forme. Cela signifie par exemple qu'il nous a fallu mettre en place des solutions pour émuler différents domaines du réseau Internet, ayant des capacités différentes et offrant des services différents. Cela signifie donc intégrer des mécanismes de séparation des domaines émulés, ainsi que la possibilité de limiter la capacité utilisable sur chacun d'eux et sur les liens entre eux. Cela est aujourd'hui possible car la plate-forme est construite sur la couche 2 d'un réseau Ethernet commuté et que l'on peut utiliser pour cela les VLAN 802.1q et les mécanismes de limitation du trafic qui transite sur un port. De plus, ces mécanismes sont facilement configurables et re-configurables.

D'autre part, pour émuler les composants du réseau, c'est-à-dire les routeurs, proxies, caches, stations des utilisateurs, etc. – et ainsi créer des structures logiques sur lesquelles effectuer les émulations pour les différents projets de recherche proposés – nous disposons d'un certain nombres de machines et de logiciels d'émulations comme Dummynet ou Nistnet par exemple, qui ont pour fonction de recréer des conditions de fonctionnement réalistes du réseau à émuler sur la plate-forme, et ce en terme de délai, taux de pertes, disponibilité, etc.

Par exemple, dans le cadre des études sur les réseaux satellites, un émulateur peut recréer de façon fine les conditions particulières de transmission, de délais, de pertes, etc. d'un lien satellite.

A noter que nous sommes en train de finaliser le portage des outils développés pour mettre en œuvre notre méthode de rejeu pour le simulateur NS-2 pour l'émulateur GdX. Nous en espérons des résultats aussi bons que ceux obtenus sous NS… En attendant les résultats du projet STM.

Laasnetexp.fr

Toutefois, l'émulation n'est pas tout, et même si elle est une étape indispensable dans le processus de validation de nos propositions de nouvelles architectures, protocoles ou mécanismes réseau, il faut absolument finir par une validation en environnement réel pour laquelle le réseau et son comportement ne seront pas reproduits selon des modèles pouvant parfois dévier de la réalité. Par exemple, dans les thématiques de recherche qu'il conduit, le LAAS est s'investit dans de nombreux projets. En particulier, le LAAS est fortement impliqué dans un nouveau projet européen du 6ème FP du programme IST, appelé EuQoS (http://www.euqos.org/), dont le but est de concevoir, construire et démontrer au niveau européen une plate-forme multi-technologies multipoints fournissant à tous ses réseaux d'accès une Qualité de Service garantie. Pour cela, notre plate-forme locale doit être connectée aux 12 autres plates-formes du projet. Dans ce projet, les réseaux de cœur (pour nous Renater, GEANT et les autres RNR) sont vus et utilisés comme des réseaux sur-provisionnés, avec le service PIP (Premium IP – équivalent de EF dans la terminologie DiffServ). Ils servent ainsi de support de transfert transparent entre les différents réseaux d'accès des différents partenaires, réseaux d'accès sur lesquels porte la recherche de la garantie de QoS. Notre plate-forme doit alors, en particulier, mettre en place et tester toutes les solutions, protocoles et mécanismes de QoS proposés par le projet EuQoS, qui sont basés sur une nouvelle architecture composée d'extensions de protocoles existants et basée sur une décomposition multi-niveaux de nouveaux protocoles de signalisation..

Nous utilisons aussi cette plate-forme dans un autre projet (MetroSec : http://www.laas.fr/METROSEC) dont l'objectif est de développer des études sur la détection de problèmes de sécurité à l'aide d'outils de métrologie. Nous mettons en œuvre dans ce cadre des méthodes d'attaques distribuées de notre plate-forme et nous développons des approches de détection basées sur les analyses obtenues à partir des traces de ces attaques. Il faut ainsi à la fois générer de telles attaques, et voir comment ces attaques peuvent être caractérisées notamment au niveau des statistiques sur la dynamique du trafic.

Lors de la définition de ces expérimentations, il nous est apparu qu'il n'était pas possible d'utiliser le réseau général du LAAS, car d'une part il ne peut pas nous permettre de mettre en place les solutions de bout-en-bout pour la garantie de QoS proposées par EuQoS, et d'autre part nos expérimentations (notamment les attaques) perturbent très fortement le réseau et son environnement.

En conséquence, nous avons déployé une plate-forme d'expérimentation tout à fait distincte et séparée du réseau général du LAAS (laasnetexp.fr), qui est directement connectée au nœud d'accès régional de Renater.
D'un point de vue pratique :

- Cette plate-forme est raccordée directement au nœud Renater par un lien d'une capacité d'un Gbps.
- La plate-forme est composée de 3 réseaux physiques avec des adresses publiques appartenant à 3 réseaux différents.
- La plate-forme accède au service IPv6 et peut fonctionner en IPv6.
- La plate-forme accède aux services multicast en IPv4 et IPv6.

De plus, la plate-forme intègre pour la mise au point de nos architectures protocolaires et de nos applications une plate-forme d'émulation privée (de petite taille). Après avoir mis au point nos solutions sur cette plate-forme d'émulation, elles seront testées à large échelle sur Grid Explorer, avant de revenir sur laasnetexp.fr pour les dernières expérimentations (avant déploiement).
Le schéma général de cette plate-forme est détaillé sur la figure 24.

C'est donc sur ces deux plates-formes – Grid Explorer et laasnetexp.fr – que seront conduites les prochaines expérimentations des propositions que nous avons faites dans la partie 2.3, à savoir notre méthode de métrologie globale reposant sur le protocole de « reporting » MRP, et les mécanismes d'adaptation que nous proposons sous le terme MBN (notamment le mécanisme de contrôle de congestion MBCC). Ces solutions seront dans un premier temps évaluées par rapport à un réseau à large échelle sur Grid Explorer, puis déployées sur laasnetexp pour être expérimentées sur le « réseau » EuQoS.
D'autres projets du groupe utilisent GridExplorer et laasnetexp.fr, notamment les projets qui traitent de communications satellites, de QoS multi-domaines, etc. Cette plate-forme sera également étendue prochainement pour satisfaire aux besoins en expérimentations d'autres groupes de recherche (comme MRS) et des partenaires du LAAS.

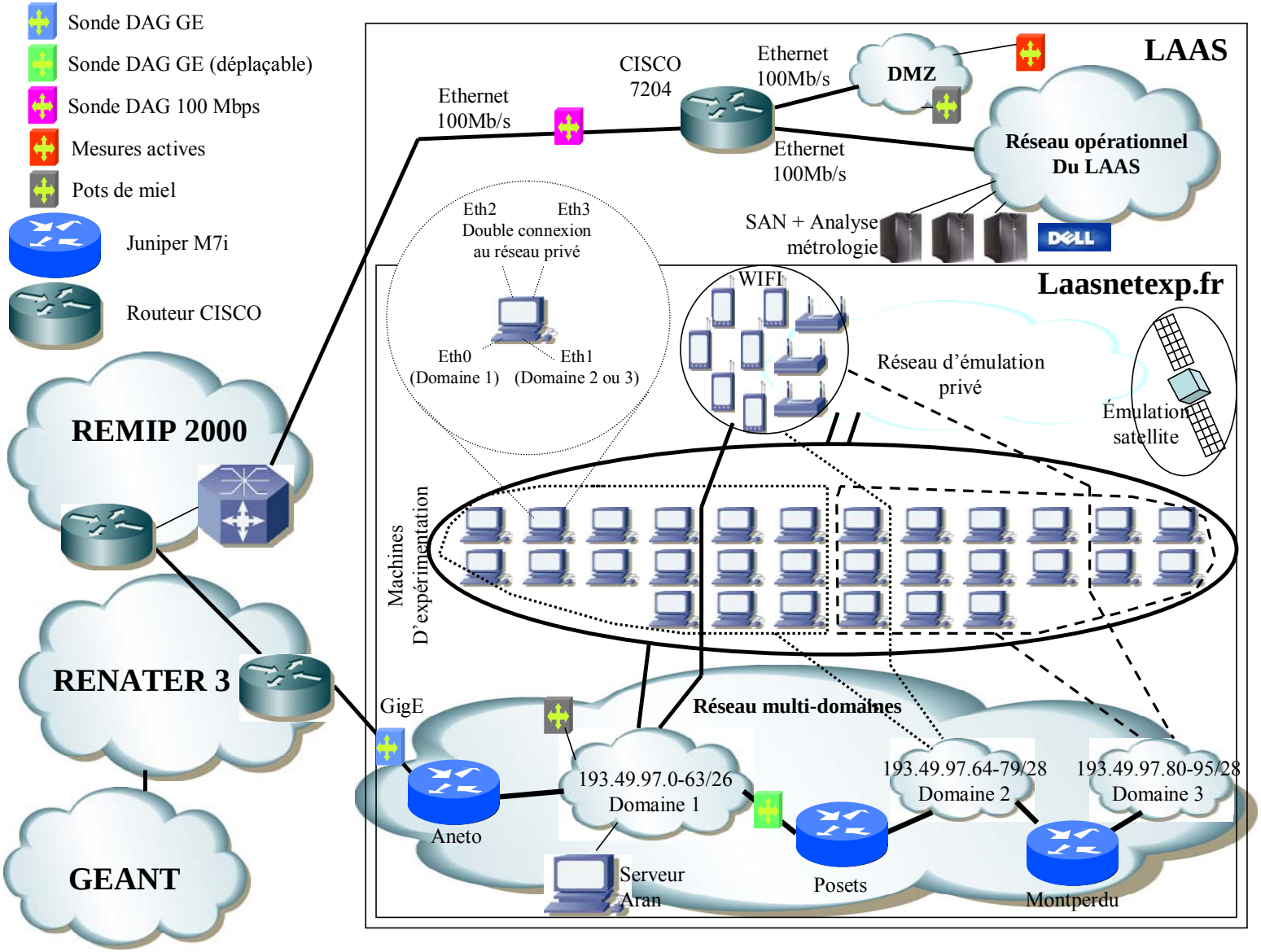

Figure 24. Plate-forme d'expérimentation réseau au LAAS

2.5. Synthèse

Ce chapitre vient de décrire mes travaux récents autour de la métrologie, ces derniers se décomposant en 4 contributions principales entièrement reliées entre elles.
La première de mes contribution a consisté à conduire la mise en place de sonde de métrologie (essentiellement de capture du trafic – DAG) sur le réseau Renater.
Grâce aux traces de trafic capturées, des travaux de caractérisation et d'analyse ont été menés. Le trafic Internet reste extrêmement variable d'un réseau à l'autre, mais sa forte variabilité due aux nouveaux usages (et en particulier le transfert de gros fichiers par des applications P2P) semble être une constante. Il a été montré que cette variabilité était dommageable pour la QoS offertes par les réseaux, et mis en évidence que TCP n'était pas adapté au transfert de gros fichiers sur des réseaux à hauts débits : lors de la transmission de ces gros fichiers, le débit généré par TCP est extrêmement variable, créant des vagues de trafic de très forte amplitude et de très longue durée. Ce chapitre a également montré que la dépendance longue ou les fonctions de corrélation caractérisaient bien ce phénomène et pouvaient donc être utilisées pour évaluer le niveau de performance d'un réseau face à un trafic donné.
Ces analyses du trafic ont également confirmé notre point de vue et nos directions scientifiques par rapport au problème de mise en œuvre de la QoS, i.e. que pour optimiser les performances et la QoS du réseau, il fallait mettre en œuvre des mécanismes d'auto-adaptation au niveau des ressources disponibles. Une nouvelle architecture de communication orientée mesures (MBA) a ainsi été proposée. Elle repose sur un système de métrologie globale et un mécanisme de « reporting » (MRP) en temps réel pour informer instantanément tous les composants du réseau de l'état du réseau, des caractéristiques du trafic et des ressources disponibles. Grâce à cette architecture de métrologie globale qui fonctionne pour des réseaux à grande échelle, il est possible de mettre en œuvre des mécanismes de gestion du réseau, de son trafic, de sa QoS, etc. qui réagissent très rapidement et avec une connaissance précise des conditions de communication. L'intérêt et les possibilités de cette nouvelle architecture de communication orientée mesure a été mise en évidence au travers d'un nouveau mécanisme de contrôle de congestion (MBCC) qui permet de réguler la transmission des flux éléphants (et de tous les autres flux) du réseau, de limiter la LRD et d'optimiser l'utilisation des ressources.
Enfin, à partir des résultats de caractérisation et d'analyse du trafic, il a été facile de voir que les techniques d'ingénierie et d'expérimentation en réseau (simulation et émulation notamment) n'étaient pas réalistes et particulièrement optimistes. Ainsi, un nouveau protocole dont les évaluations de performance par simulation étaient excellentes se trouvait en fait, au moment de sa mise en œuvre, complètement poussif. Il a donc été proposé d'exploiter les traces de trafic capturées par les outils de métrologie, et de les rejouer dans les simulateurs et émulateurs afin de reproduire les conditions réelles d'un vrai réseau lors des expérimentations / évaluations. Une méthode de rejeu de traces a donc été proposée et validée, et surtout utilisée lors de toutes les expérimentations que nous avons conduites depuis, et notamment celles décrites dans ce mémoire. A noter que pour mener à bien des expérimentations réalistes et à grandes échelles, nous avons mené à bien la mise en place de deux plates-formes pour l'émulation et l'expérimentation réseau : nous avons contribué à la mise en place du cluster GdX dont un des objectifs et de pouvoir émuler des réseaux à grande échelle (400 nœuds environ aujourd'hui). Nous avons également mis en place une plate-forme expérimentale au LAAS pour mener à bien des émulations (40 nœuds environ) et des expérimentations en réseau longues distances avec nos partenaires.

3. Programme de recherche

Le programme de recherche que je propose pour les prochaines années sera une suite logique des travaux menés ces 6 dernières années : il inclura des suites logiques aux travaux démarrés dans le passé et non encore terminés, mais également un certain nombre de ruptures par rapport à de nouveaux besoins, de nouvelles fonctions dont l'importance devient aujourd'hui prépondérante dans la recherche en réseaux.

3.1. Architecture MBA et utilisations

Comme nous l'avons vu dans la partie 2.3, nous sommes convaincus que la métrologie utilisée en temps réel pour superviser le réseau et son trafic, sa QoS, etc. amène une solution pour régler les problèmes liés à la dynamicité des ressources dans le réseau et à la variabilité du trafic, qui posent tant de problèmes pour garantir et gérer des services stables. L'approche MBN, son architecture de mesure associée MBA et les mécanismes d'adaptation au contexte des réseaux et de leurs trafics sont donc un domaine de recherche phare dans notre activité actuelle et à venir. Pour l'instant, seuls les grands principes de base ont été définis, et des applications – parfois ad hoc seulement – pour certaines fonctions des réseaux ont été proposées. Nos travaux futurs ont donc pour objectif de proposer des solutions plus génériques et universelles de cette architecture, et de l'appliquer à d'autres grandes fonctions des réseaux.

Adaptation et utilisation de MBA dans le projet européen EuQoS

En premier lieu, l'architecture MBA est en cours d'intégration dans l'architecture de fourniture de QoS proposée et développée dans le cadre du projet EuQoS. Le projet EuQoS – *End-to-end Quality of Service support over heterogeneous networks* – est un projet intégré du 6ème PCRD qui a pour objectif de concevoir et déployer la première architecture de communication à QoS garantie sur les réseaux de la recherche européens (GEANT et de nombreux NRN : National Research networks). Dans ce projet, les fonctions de base d'un réseau à QoS – comme le contrôle d'admission et de congestion, l'ingénierie des trafics, l'optimisation des ressources, la gestion des fautes, etc. – font appel à un système de mesure et de supervision (MMS : Monitoring and Measurement System) [Bur 05]. MMS est ainsi en charge de collecter un maximum d'informations sur les trafics qui transitent sur les liens des réseaux interconnectés, de mesurer en permanence l'état du réseau et le niveau de QoS qu'il fournit, et de diffuser ces informations entre les différents points de mesure et vers les équipements en charge de la mise en œuvre des différentes fonctions réseaux citées pour la gestion et la mise en œuvre de la QoS. Ce travail, réalisé en partenariat entre le LAAS, l'université de Catalogne à Barcelone, Telefonica I+D (Madrid) et l'université de technologie de Varsovie, reprend les concepts de l'approche MBN et de l'architecture MBA présentés dans la partie 2.3, et adapte les codes et protocoles conçus et développés pour l'instant pour le contrôle de congestion (MRP et MBCC) au problème plus général traité dans EuQoS. Il les enrichit également en intégrant les outils de mesure de la QoS et de supervision du trafic développés à Barcelone, et qui combinent mesures actives et passives, et respectant en cela les recommandations que nous avons faites pour MBA. De la même façon, Telefonica I+D a défini et nous sommes en train de développer toutes les interfaces nécessaires aux échanges entre les différentes entités. L'objectif est de finaliser cette architecture orientée mesure pour

fournir de la QoS garantie, de la mettre en œuvre sur les réseaux européens de la recherche et de la valider avant Septembre 2007.

Le « reporting » des mesures dans MBA

Un des composants essentiels de l'architecture MBA et qui n'a été que très partiellement abordé dans la thèse de Nicolas Larrieu [Lar 05b], dans la partie 2.3 de ce manuscrit ou dans EuQoS concerne les mécanismes et protocoles de « reporting » de mesures. Le « reporting »des mesures a donné lieu dans [Lar 05a] ou [Lar 05b] à la conception d'un protocole appelé MRP (Measurement Reporting Protocol) inspiré de RSVP, mais qui n'a été conçu que dans l'optique de satisfaire aux besoins de MBCC, i.e. basé uniquement sur une approche point à point liée à chaque connexion MBCC, la globalisation se faisant au niveau des nœuds intermédiaires traversés par plusieurs connexions MBCC pour une diffusion que rien ne garantit comme étant complète. Une telle solution présente donc de nombreux asynchronismes (liés aux multiples connexions MBCC nécessaires pour la diffusion des informations de mesure) et doit donc être améliorée pour fournir une solution globale et générique qui sera plus performante pour des fonctions globales au niveau d'un réseau entier, voire d'une interconnexion de réseaux. De la même façon, dans EuQoS la diffusion des informations de mesure du système MMS se fait selon une approche 'Pull' qui, a priori, doit induire des délais importants et donc des performances des mécanismes de « reporting » non optimales.

Il est clair, qu'autant dans le cadre de MBCC que dans celui d'EuQoS, l'effort consenti sur les mécanismes de « reporting » des mesures a été faible. Pour MBCC, qui n'était là que pour démontrer les bénéfices de l'approche MBN, la signalisation n'était pas au cœur de l'étude, et seule une solution rapide a été proposée. De même, dans le cadre d'EuQoS, la contribution totale est planifiée sur 36 mois, et les 18 mois du projet contractuel actuel n'incluent pas la conception et le développement d'un protocole de « reporting » de mesures universel et générique.

Ce sujet est donc un des éléments à aborder dans la suite de la conception et du développement de l'architecture MBA. En particulier, il faudra étudier et analyser les performances des différentes solutions : les approches Pull ou Push, l'établissement de sessions entre outils de mesures (MMS dans le cadre d'EuQoS) à la mode BGP ou de diffusion ouverte, etc. C'est un des sujets sur lequel notre action de recherche à long terme va se focaliser.

MBA et l'ingénierie des trafics

Un autre aspect à développer dans le cadre de l'approche MBN est son adéquation avec d'autres fonctions des réseaux. Aujourd'hui, seul le contrôle de congestion a été abordé pour montrer les bénéfices de l'approche basée sur l'utilisation en temps réel des mesures. De même, dans le cadre d'EuQoS, l'objectif de la première partie du projet ne se focalise que sur un petit nombre de fonctions, et de plus avec des hypothèses réductrices. Il faut donc montrer que MBN et MBA peuvent s'appliquer pour d'autres fonctions des réseaux. En particulier, dans le cadre du réseau d'excellence européen E-NEXT, Silvia Farraposo a commencé une thèse co-encadrée entre l'université de Coimbra et le LAAS, dans laquelle le LAAS amène ses compétences en matière de métrologie et l'université de Coimbra ses compétences sur le routage et l'ingénierie du trafic. L'idée consiste à définir de nouvelles politiques de répartition du trafic entre les différents chemins entre une source et une destination en fonction de la QoS requise pour les flux en question. En particulier, le problème se pose lorsque le trafic présente des anomalies, i.e. de fortes variations soudaines et qui nécessitent de changer la répartition du

trafic entre les différents liens sous peine de voir l'un d'entre eux avoir une brusque réduction de ses performances. Parmi ses anomalies, les attaques de déni de service (DoS) sont particulièrement sensibles au niveau de l'ingénierie des trafics, et il faudra utiliser au mieux la connaissance de la topologie du réseau (obtenue grâce à des mesures) et à la QoS offerte par chacun des liens à un instant t pour annihiler ses effets négatifs sur le réseau. C'est d'ailleurs un des points qui va être décrit dans la partie suivante.

3.2. Sécurité

3.2.1. Contexte

Comme nous l'avons déjà dit, le grand dessein de l'Internet est de pouvoir garantir un niveau de service suffisant pour toutes les applications qui l'utilisent, et ceci en toutes circonstances, y compris les plus difficiles. De ce fait, le réseau devient très sensible aux attaques, et notamment aux attaques de déni de service (DoS) quelles soient simples ou distribuées. En effet, les ruptures (i.e. des anomalies) dans le trafic – induites par ces attaques que le réseau propage – peuvent entraîner des changements dans la QoS perçue par tous les utilisateurs du dit réseau, et ainsi briser le contrat de service (ou SLA : Service Level Agreement) au tort du fournisseur de service. Ce serait aussi et surtout très pénalisant pour les utilisateurs : par exemple dans les applications d'environnements de travail collaboratifs, télé-ingénierie, visioconférence, commerce électronique (B2B et B2C), etc. pour lesquels il faut assurer tout au long des communications les qualité adéquates sur chacun des médias, une baisse de la qualité – même ponctuelle – sur la voix conduisant à des baisses sensibles de l'efficacité des réunions de travail virtuelles. D'ailleurs, le problème de la garantie de la QoS dans les réseaux consiste à fournir le service demandé dans tous les cas, y compris les cas pires, le cas pire correspondant vraisemblablement aux moments où une attaque de déni de service est en cours [Sha 03]. Les attaques de DoS peuvent donc entraîner pour les opérateurs et les utilisateurs de leurs services de communication des manques à gagner financiers importants. Il en est de même pour tous les types d'anomalies dans le trafic comme les pannes – par arrêt du service ou byzantines – ou même des anomalies légitimes, par exemple liées à la diffusion d'un événement médiatique sur le réseau (concerts, événements sportifs, etc.). Toutes ces anomalies, au premier rang desquelles les attaques, sont donc de nature à nuire au bon fonctionnement du réseau qui ne pourra plus garantir les services qu'il s'est engagé à rendre.

Face à ce risque de plus en plus présent et aux conséquences de plus en plus coûteuses, les spécialistes en sécurité informatique ont œuvré pour proposer des améliorations, notamment au niveau des pare-feux ou des systèmes de détection d'intrusion. Cet axe de recherche – et c'est une de ses principales originalités – propose d'étendre les travaux actuels en sécurité en utilisant la métrologie des réseaux de l'Internet, qui représente également une des grandes avancées de ces quelques dernières années dans le domaine de l'ingénierie, la gestion et la recherche en réseau. Ce projet a donc pour ambition de combiner vers un même objectif des approches issues des communautés de recherche en réseau et en sécurité traditionnelle. Cette approche est particulièrement originale, et à ce jour très peu de travaux de ce type ont été menés. A notre connaissance, aujourd'hui, seuls les travaux – décrits dans [Che 02], [Li 03] et [Hus 03] et ayant la même approche que celle décrite ici – ont émergé, même si la tendance semble être à la hausse (notamment si on se base sur les articles qui ont été soumis tout récemment dans les conférences des domaines des réseaux et de la sécurité).

Il est à noter enfin que ce thème de recherche a conduit au lancement du projet *MétroSec* labellisé par le ministère de la recherche dans le cadre de l'ACI (Action consultée Incitative) Sécurité et Informatique, et qui a débuté en septembre 2004. A noter également que ce projet s'inscrit dans le cadre d'une collaboration multidisciplinaire entre des équipes spécialistes des réseaux informatiques, du traitement de signal, de la théorie des graphes et des systèmes répartis, déjà impliquées indépendamment dans l'étude des réseaux de l'Internet. L'enjeu de *MétroSec* consiste donc en la création d'une synergie multidisciplinaire entre des sciences qui ont des approches et des outils *a priori* différents. Cette synergie est le fruit des réflexions menées par les experts de l'Action spécifique 88 du département STIC du CNRS sur la « métrologie des réseaux de l'Internet » et dont les recommandations mettent l'accent sur la nécessaire collaboration de compétences multiples, issues de disciplines différentes, pour mesurer, superviser et analyser les réseaux [Owe 03c].

L'objectif de cet axe de recherche – inclus dans le projet MétroSec – est donc d'augmenter la robustesse et l'insensibilité du réseau vis-à-vis des anomalies dans le trafic et la topologie, afin qu'il puisse continuer de fournir un service acceptable et de garantir la QoS demandée (réduisant ainsi à néant l'effet de possibles attaques).

Ce projet se propose donc d'abord de développer et mettre en œuvre des outils de métrologie – actif et passif – et de supervision et de surveillance des caractéristiques du réseau et de son trafic. L'analyse des traces et mesures doit permettre de mettre en évidence la nature et l'importance de l'impact de ces anomalies sur la QoS du réseau, ainsi que sur la propagation en temps et en espace (à travers la topologie du réseau) d'éventuelles altérations de celle-ci.

Le travail proposé dans ce projet est en fait fondé sur les premiers résultats de caractérisation et de modélisation du trafic issus des travaux de métrologie engagés depuis quelques années [Che 02] [Li 03] [Hus 03] [Jin 04] [Owe 05]. Ces travaux mettent le plus souvent en évidence des phénomènes d'invariance d'échelle qui constituent l'une des caractéristiques majeures qui décorent les statistiques du trafic Internet moderne (cf. partie 2.2). Ces derniers se développent à la fois sur des échelles de temps allant de la minute à la journée, caractérisant le type de trafic produit par les utilisateurs ou leurs comportements et activités sur le réseau et à la fois sur des échelles de temps allant de la milliseconde à la seconde, caractérisant le fonctionnement des protocoles ou des équipements du réseau. Il a d'autre part, été montré que les attaques perpétrées sur un réseau induisent des variations fortes, voire des ruptures, dans les signatures topologiques et dans les invariances d'échelle. L'étude de ces variations et de leurs dynamiques temporelles et/ou spatiales est au cœur du projet. Elle pourra permettre le repérage des attaques (des pannes), l'analyse des modes de propagation des virus, des vers ou de toute autre forme d'attaques dans l'Internet. Ces approches ayant donné d'encourageants premiers résultats, l'objectif de cet axe de recherche est donc de construire des outils de traitement du signal permettant de détecter, mettre en évidence et caractériser des ruptures, des variations « anormales » des caractéristiques du trafic. Ces variations seront, dans un premier temps, recherchées par analyses en ondelettes, décomposition modale empirique ainsi que par des méthodes de type filtre de Kalman multi-échelles.

De façon complémentaire, le projet propose d'utiliser des outils de théorie des graphes pour détecter les anomalies dans le comportement du réseau. Il s'agit ici de surveiller les variations dans la topologie observée du réseau ou des échanges. Les outils statistiques d'analyse des graphes et de leur dynamique permettent d'espérer une description fine de ces

topologies et de l'impact des anomalies de comportements du réseau sur leurs propriétés. Il s'agit donc de mesurer cet impact, de l'analyser et de développer des méthodes de détection et de réaction appropriées.

A partir des analyses précédentes, il sera proposé des améliorations architecturales, protocolaires et topologiques pour le maintien du réseau à un niveau élevé de QoS, malgré l'occurrence d'anomalies. La robustesse vis-à-vis des anomalies donnera aux outils de métrologie et d'analyse (traitement du signal et graphe) le temps de classer l'anomalie en temps réel et de mettre en place des réactions appropriées. En cas d'attaque, par exemple, des outils d'identification et d'élimination des paquets incriminés seront développés et mis en œuvre, ainsi que des mécanismes d'identification des attaquants. On peut ainsi imaginer que des recommandations de modification de la topologie des réseaux pourraient être énoncées, afin de limiter la vitesse de propagation des attaques dans les réseaux et ainsi réduire les dégradations en termes de QoS. Dans le même but, de nouvelles techniques d'ingénierie du trafic pourraient être énoncées. On peut imaginer également que les protocoles de communication, dont l'impact n'est pas forcément positif sur le trafic (par exemple à cause de mécanismes de contrôle de congestion inadaptés qui créent de fortes variations dans le débit du trafic sur les réseaux [Owe 04b]), pourraient être modifiés pour les insensibiliser à des variations brusques du trafic. D'autre part, dans le cadre d'attaques de DoS ou de DoS distribuées, des mécanismes d'identification des paquets fautifs (ceux qui ont contribué à des anomalies au niveau des lois d'échelles caractéristiques de la dynamique du trafic) pourront être proposés et on pourra ainsi utiliser de nouveaux mécanismes de « backtracking » pour identifier la ou les sources des attaques, et les couper au niveau du premier routeur que ces flux rencontrent. Il est important de voir ici, et c'est un des points forts du projet, que la sécurisation des services du réseau se fera à deux niveaux pour rendre le réseau plus robuste aux anomalies du trafic : tout d'abord, seront proposées des améliorations pour rendre le réseau insensible (ou du moins peu sensible) à des pannes ou des variations fortes et parfois légitimes du trafic. Par contre, dès lors qu'une attaque sera identifiée à l'aide de l'outil de métrologie et de supervision du réseau, des techniques de défense distribuées, basées sur le « backtracking », seront mises en place, en sachant que grâce aux améliorations du réseau pour l'insensibiliser aux variations du trafic, le temps qui sera nécessaire pour identifier qu'une attaque est perpétrée sur le réseau, l'attaque sera sans effet sur le réseau qui sera conçu pour être capable de la supporter. A terme, le projet doit fournir un ensemble cohérent d'outils de métrologie et d'analyse de trafics et de topologies, qui permettront le développement de méthodes efficaces de surveillance, de supervision et de réaction aux anomalies. Ces méthodes combinées aux nouvelles solutions architecturales et protocolaires de communication augmenteront significativement la qualité des services réseaux, même face à une attaque.

3.2.2. Caractérisation et modélisation du trafic avec et sans anomalies – Contribution à la détection d'intrusions

A la moitié du projet MétroSec, de nombreuses études des caractéristiques du trafic normal, du trafic avec anomalies (foules subites, attaques de DoS) ont été réalisées et ont mené à de très encourageants résultats. La suite présente l'état actuel des travaux relatifs à la caractérisation et la modélisation du trafic avec anomalies, ainsi que sur la classification des anomalies en anomalies légitimes et illégitimes, ce qui ouvre la voie à la conception de nouveaux outils de détection d'intrusion orientés profil. Ces travaux ont été réalisés avec nos collègues de l'ENS Lyon Patrice Abry, Pierre Borgnat, Antoine Scherrer, ainsi qu'avec Nicolas Larrieu (LAAS). L'article [Sch 06] décrit plus en détail ces travaux.

3.2.2.1. Motivation

Combattre les attaques DoS est une tâche difficile et les systèmes de détection d'intrusions (IDS), notamment ceux basés sur la détection d'anomalies, ne sont pas très efficaces. En premier lieu, leurs limitations sont liées à la multitude de formes que peuvent prendre les attaques DoS et qui rendent difficile une définition globale des attaques. Dans un second temps, le fait que le trafic Internet normal présente des variations importantes de son trafic à toutes les échelles, souvent décrites en terme de longue mémoire, auto-similarité, multifractalité rendent plus délicate et incertaine la détection d'anomalies. Troisièmement, le trafic Internet peut présenter des variations fortes, soudaines mais légitimes (comme des foules subites - ou *flash crowds* en anglais - par exemple) qu'il peut être difficile de distinguer des variations illégitimes.
Pour ces raisons, les IDS basés sur la détection d'anomalies souffrent souvent de taux de faux positifs, et sont donc peu populaires. L'évolution actuelle du trafic Internet, avec une variété immense de types de trafics rendent encore plus délicate la conception d'un IDS efficace.
Ce travail, réalise dans le cadre du projet METROSEC, a pour objectifs principaux d'analyser l'impact des anomalies sur les caractéristiques statistiques et de mettre en évidence des signatures caractéristiques du trafic contenant des anomalies légitimes (par exemple les foules subites) et illégitimes (par exemple les attaques DDoS). A la fin, ces résultats doivent servir à améliorer les mécanismes réseau et les rendre capable de combattre les anomalies, notamment les malicieuses.
Pour cela, nous proposons d'utiliser un modèle de processus stochastique non Gaussien et à mémoire longue représentant le trafic Internet. Nous montrons expérimentalement que ce modèle est suffisamment versatile pour décrire une grande variété de trafics réguliers ainsi que des trafics comportant des anomalies, légitimes ou non. Nous montrons aussi que les évolutions des estimations des paramètres pour le modèle proposé permettent de différencier le trafic avec et sans anomalies et de classifier ces anomalies.

3.2.2.2. Modélisation de trafic : une introduction

3.2.2.2.1. Trafic sans anomalie

Le trafic des réseaux d'ordinateurs peut se caractériser par un processus d'arrivée de paquets. Il a été montré il y a plus de 10 ans que ces processus d'arrivée des paquets sont très éloignés du modèle de Poisson (voir par exemple [Pax 95]), en particulier parce que les inter-arrivées de paquets ne sont pas indépendantes. On peut les modéliser en utilisant soit des processus non stationnaires [Kar 04] soit des processus markovien modulés stationnaires [And 98]. Par conséquent, une description générale du processus est $\{(t_l, A_l), l = 0,1,2,...\}$ ou t_l représente l'estampille d'arrivée du l-ème paquet et A_l certains attributs du paquet (comme sa charge utile, ses ports source et destination, ...). Cependant, étant donné le grand nombre de paquets impliqués, cela engendre des ensembles de données énormes.
C'est pourquoi il est souvent préférable de considérer les processus décomptant le nombre d'octets ou de paquets du trafic agrégé, notés $W_\Delta(k)$ et $X_\Delta(k)$. Ils correspondent au nombre d'octets (resp. paquets) qui transitent au cours de la k-ème fenêtre de taille $\Delta > 0$, i.e., dont les estampilles se situent entre $k\Delta \leq t_l < (k+1)\Delta$. D'autres analyses pourraient reposer sur le processus d'arrivée des flux comme dans [Bar 02] par exemple. Dans cet article, nous restons au niveau paquet et nous nous concentrons sur la modélisation conjointe des distributions marginales et de la fonction de covariance de $X_\Delta(k)$. L'adéquation et l'intérêt des processus multifractals – dont les propriétés d'échelle ne sont pas complètement décrites au second ordre

statistique, et implique donc des ordres statistiques supérieurs – ont été étudiés en détail dans de nombreux articles (voir [Fel 98], [Taq 97], [Zha 03]). Cet aspect, qui reste un problème ouvert, ne sera pas étudié dans cet article.

3.2.2.2.2. Détection d'anomalies

Les IDS basés sur la détection d'anomalies n'utilisent pas, en général, des modèles statistiques riches. Ils supervisent seulement des paramètres simples du trafic comme son débit d'octets ou de paquets, et la plupart de ces IDS recherchent juste des séquences de paquets spécifiques, connues comme des signatures d'attaques [Pax99]. Les alarmes sont essentiellement générées lorsqu'un seuil est dépassé [Bru 00, Vac89], ce qui conduit à un nombre important de faux positifs [Moo01]. Par conséquent, ces IDS sont souvent assez peu satisfaisants car ils ne peuvent pas différencier les variations légitimes du trafic des attaques.
Les progrès récents en modélisation obtenus dans les projets de métrologie du trafic ont cependant renouvelé les stratégies de conception des nouveaux IDS. Même si ces derniers restent à des étapes de développement peu avancées, des résultats très intéressants utilisant des caractérisations statistiques ont été publiés. Par exemple, Ye a proposé dans [Ye 00] un modèle Markovien pour le comportement temporel du trafic, et génère des alarmes lorsque le trafic s'éloigne significativement du modèle. D'autres auteurs [Jin 04, Yua 04] ont montré que les attaques DoS augmentent la corrélation dans le trafic, ce qui pourrait représenter une technique de détection robuste.
A partir de l'évaluation de l'inter-corrélation de trafics sur différents liens, Lakhina *et al*. ont proposé une méthode pour détecter les anomalies dans les matrices de trafic à l'échelle du réseau global [Lak 04]. Hussain et ses co-auteurs utilisent la densité spectrale pour identifier des signatures pour différentes attaques [Hus 03]. De la même façon, l'estimation spectrale a été utilisée pour comparer des trafics avec et sans attaques [Che 02]. Alors que la densité spectrale met en évidence des pics autour du RTT pour du trafic normal, ces pics disparaissent en cas d'attaque. Cette caractéristique peut ainsi être utilisée pour concevoir de nouveaux IDS. Enfin, Li and Lee ont utilisé les techniques à base d'ondelettes développées dans [Vei 99] pour calculer une distribution d'énergie. Ils ont observé que cette distribution d'énergies présente des pics lorsque le trafic contient des attaques qui n'existent pas pour le trafic régulier [Li 03]. Le travail présenté en [Bar 02a] exploite les qualités d'analyse multi-résolutions des décompositions en ondelettes pour détecter les anomalies du trafic pour un intervalle d'échelles moyennes. De nombreux travaux prometteurs ont déjà été publiés dans le domaine des attaques DoS [Bar 02, Jun 02]. La détection d'anomalies pourrait reposer sur des analyses dépendantes des applications [Far 05], ou sur les mécanismes des attaques [Kan 05]. Dans ce travail, nous nous focalisons sur le niveau paquet. Cependant, et parce que nous observons le trafic avec différentes échelles de temps, la méthode d'analyse proposée est principalement basée sur la détection de changements dans les caractéristiques statistiques du trafic. En comparant les distributions marginales et les fonctions de covariance obtenues - d'abord sur du trafic régulier, puis sur des trafics présentant une large variété d'anomalies incluant notamment des anomalies légitimes – nous pouvons différencier les changements du trafic dus à des actions légitimes d'actions illégitimes.

Données	Date (début)	T (s)	Réseau (lien)	# Pkts	IAT (ms)	Répertoire
PAUG	1989-08-29(11:25)	2620	LAN(100BaseT)	1	2.6	ita.ee.lbl.gov/index.html
LBL-TCP-3	1994-01-20(14:10)	7200	WAN(100BaseT)	1.7	4	ita.ee.lbl.gov/index.html
AUCK-IV	2001-04-02(13:00)	10800	WAN(OC3)	9	1.2	wand.cs.xaikato.ac.nz/wand/wits
CAIDA	2002-08-14(10:00)	600	Backbone(OC48)	65	0.01	www.caida.org/analysis/workload/oc48/
UNC	2003-04-06(16:00)	3600	WAN(100BaseT)	4.6	0.8	www-dirt.cs.unc.edu/ts
METROSEC-ref1	2004-12-09(18:30)	5000	LAN(100BaseT)	3.9	1.5	www.laas.fr/METROSEC
METROSEC-ref2	2004-12-10(02:00)	9000	LAN(100BaseT)	2.1	4.3	www.laas.fr/METROSEC
METROSEC-DDoS	2004-12-09(20:00)	9000	LAN(100BaseT)	6.9	1.3	www.laas.fr/METROSEC
METROSEC-FC	2005-04-14(14:30)	1800	LAN(100BaseT)	3.7	0.48	www.laas.fr/METROSEC

Tableau 6 : ***Description des Données***. Paramètres généraux des traces étudiées. T est la durée de la trace, en secondes. # Pkts (10^6) est le nombre de paquets dans la trace, en millions. IAT est le temps d'inter-arrivées moyen, en ms.

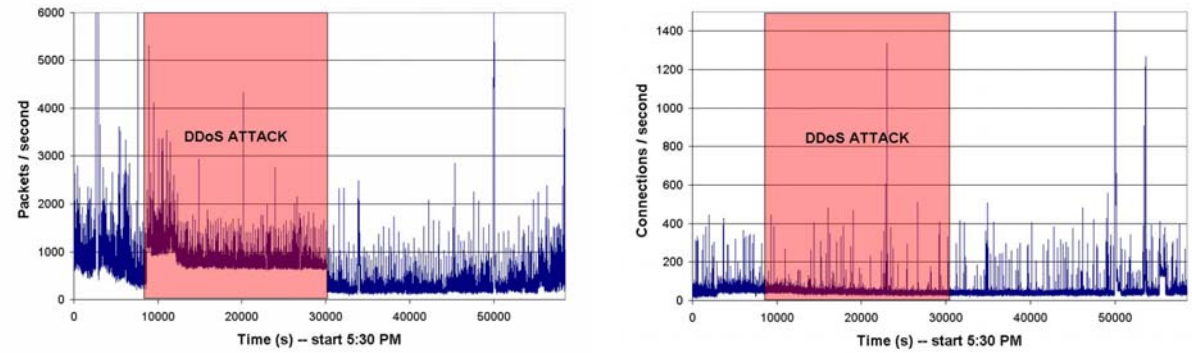

Figure 25 : ***Attaque DDoS***. Débit paquets (à gauche) et Nombre de connexions par seconde (à droite).

3.2.2.3. Données et Expériences

3.2.2.3.1. Trafic sans anomalie

Le modèle et les analyses proposés plus loin ont d'abord été illustrés sur des traces de trafic ne présentant pas d'anomalies, et décrites en détails dans le tableau 6. Nous utilisons à la fois des données standards publiques (Bellcore, LBL, UNC, Auckland Univ, Univ North Carolina, CAIDA), et des séries temporelles de trafics capturées par nos soins dans le cadre du projet de recherche METROSEC. Par conséquent, nous couvrons un ensemble significatif de traces de trafics – provenant de différents types de réseaux (LAN, WAN, ... et des réseaux de bordure, de cœur, ...) et de liens – capturées ces 16 dernières années (de 1989 à 2005). Dans chaque base de données, un grand nombre de traces sont disponibles. Nous nous concentrons dans cet article sur quelques traces qui sont représentatives de ces collections de traces.

3.2.2.3.2. Trafic (ou traces) avec des anomalies

En raison de la difficulté de se procurer des données pour lesquelles des anomalies se produisent, nous avons décidé de réaliser nous mêmes un ensemble d'expérimentations sur le réseau RENATER, dans le cadre du projet METROSEC. Ces expérimentations incluent la génération d'anomalies légitimes (foules subites) et illégitimes (attaques DDoS). Ceci nous permet de réaliser des expérimentations d'une façon reproductible, précise et contrôlée.

• **Attaque DDoS**. L'attaque DDoS étudiée ici est une attaque en UDP flooding distribuée. Elle a été générée depuis 5 sites différents : l'IUT de Mont de Marsan, le LIAFA Paris, l'ENS Lyon, l'ESSI Nice, en France et l'université de Coimbra au Portugal, à l'encontre du LAAS à Toulouse qui était le site ciblé. Le LAAS est connecté à RENATER par l'intermédiaire d'un lien Ethernet 100 Mbps qui n'a pas été saturé pendant l'attaque. Une trace du trafic a été capturée sur le lien d'accès du LAAS. L'attaque a démarré à 20h le 9 décembre 2004 et a duré plus de 5h30. Les caractéristiques de base du trafic sont décrites sur la figure 25 qui montre le nombre de flux et de paquets sur le réseau d'accès du LAAS. Alors que le premier reste très stable, le second présente une augmentation significative du débit des paquets (il est multiplié par presque 3 pendant l'attaque).

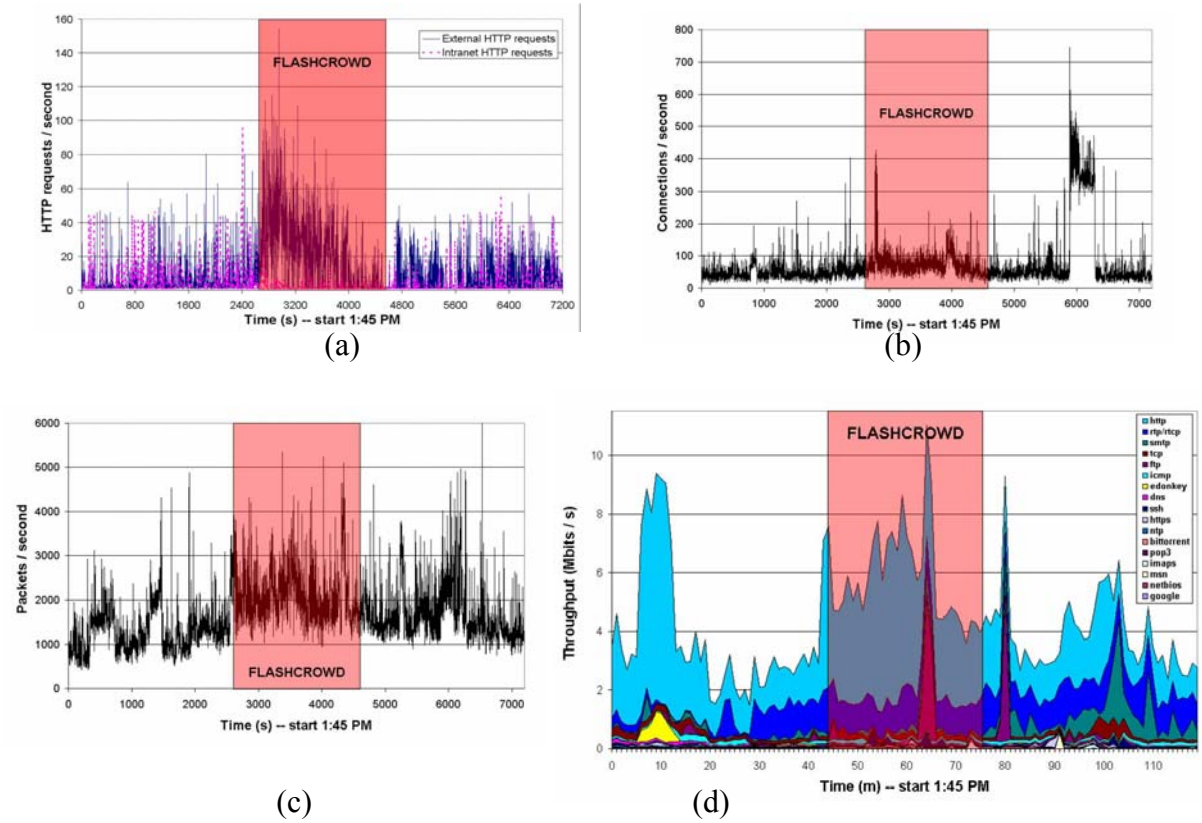

Figure 26 : ***Flash Crowd***. (a) Nombre de requêtes http, (b) de connexions, (c) de paquets par seconde et (d) la distribution des débits par application. La figure (d) suit une approche descendante : l'application apparaissant au plus haut de la légende est celle qui génère le plus de trafic.

• **Flash Crowd (FC) ou foule subite**. Pour comparer l'impact sur les caractéristiques du trafic d'attaques DDoS et de variations légitimes du trafic, nous avons créé des foules subites sur un

serveur web. Pour les rendre réalistes, i.e. humainement aléatoires, nous avons choisi de ne pas utiliser un programme automatique, mais au contraire, de demander à de nombreux collègues académiques de consulter le site web du LAAS (http://www.laas.fr). Les résultats présentés sont ceux obtenus pour la foule subite du 14 avril 2005 qui a duré 30 minutes et a rassemblé plus de 100 participants. La figure 26(a) montre le nombre de requêtes reçues par le serveur web du LAAS (HTTP GET requests), en faisant la distinction entre les requêtes venant de l'intérieur et de l'extérieur du LAAS. Il apparaît clairement que de nombreux utilisateurs ont commencé à naviguer sur le site web du LAAS à 14h30 (augmentation importante du nombre de requêtes), mais également que la plupart ne sont pas restés les 30 minutes. Les figures 26(b) et 26(c) montrent respectivement le nombre de flux et le débit des paquets sur le réseau d'accès du LAAS. Comme c'était attendu, les deux courbes présentent une augmentation du nombre moyen de flux et du débit moyen de paquets, respectivement, durant la foule subite. Cependant, il apparaît aussi une augmentation importante du nombre de flux et du débit paquets après la fin de l'expérience de foule subite. La figure 26(c) montre aussi une augmentation du débit paquets moyen avant l'expérience de foule subite. Pour comprendre ces augmentations, nous avons analysé différentes composantes du trafic en utilisant l'outil Trafic Designer de la société QoSMOS (cf. figure 26(d)). L'analyse a montré que l'augmentation autour de 14h (avant notre expérience) est due à des membres du LAAS qui naviguent sur le web juste après le déjeuner. Un tel comportement a été observé systématiquement sur toutes les traces collectées au LAAS depuis. Le second pic, après l'expérience, est dû à du trafic SMTP. Il peut s'expliquer de deux façons. En premier lieu, il faut savoir que de nombreux chercheurs au LAAS utilisent webmail. Comme le serveur a été très ralenti pendant l'expérience de foule subite, ils ont donc arrêté d'envoyer des e-mails jusqu'à ce que le serveur recommence à fonctionner avec des performances satisfaisantes. Dans un second temps, il faut savoir que le mécanisme de « grey listing » (utilisé pour réduire le nombre de spams) retarde certains e-mails, et les émet tous ensemble lors des ouvertures planifiées des portes. La première ouverture après l'expérience s'est produite à 15h15.

3.2.2.4. Processus non Gaussien à mémoire longue

3.2.2.4.1. Le modèle Gamma farima

Dans cet article, nous nous proposons de modéliser la série temporelle $\{X_\Delta(k), k \in Z\}$ pour tous les niveaux d'agrégation Δ. Modéliser la série temporelle $\{W_\Delta(k), k \in Z\}$ donne des résultats équivalents, mais pour des raisons de clarté, nous nous limitons à la modélisation de la première série. Le modèle proposé est un processus stationnaire, non Gaussien et à longue mémoire : le processus Gamma (marginale) Farima (covariance). Nous supposons que le processus est stationnaire car cela facilite les choses d'un point de vue théorique, et vérifions empiriquement la validité de cette propriété durant les analyses.

• Statistiques du premier ordre (Marginale): Distribution Gamma.

$X_\Delta(k)$ est par définition une variable aléatoire positive ; plusieurs travaux ont proposé de décrire sa loi marginale avec des lois positives bien connues comme les lois exponentielle, log-normale, Weibull ou des distributions Gamma [Mel 93]. En raison de la nature du trafic, ($X_\Delta(k)$ est conçu à partir d'un processus d'arrivées de paquets [Eva 00]), des distributions Poisson ou exponentielle sont attendues pour les niveaux de faible agrégation Δ. Pour des données fortement agrégées (pour des Δ plus grands), les lois gaussiennes constituent de bonnes approximations. Cependant, aucune d'elles ne peut modéliser de façon satisfaisante les lois marginales du trafic pour un spectre large de (petits et grands) Δ. Nos études empiriques montrent qu'une distribution Gamma $\Gamma(\alpha,\beta)$ représente mieux les marginales de X_Δ.

Une distribution Γ(α,β) est définie pour des variables aléatoires positives X par

$$\Gamma_{\alpha,\beta}(x) = \frac{1}{\beta\Gamma(\alpha)}\left(\frac{x}{\beta}\right)^{\alpha-1} \exp\left(-\frac{x}{\beta}\right) \qquad (1)$$

où :
Γ(*u)*est la fonction Gamma standard (voir [Eva 00]). Elle dépend de deux paramètres : la forme α et l'échelle β. Sa moyenne est μ = α β et sa variance $\sigma^2 = \alpha \beta^2$. A noter que l'inverse du paramètre de forme, 1 / α agit comme un indicateur de la distance avec une loi gaussienne.

Statistiques du second ordre (covariance): Dépendance à long terme.
Après les travaux présentés dans [Lel 94], il est, aujourd'hui, communément accepté que le trafic sur un réseau d'ordinateurs se caractérise par des propriétés de mémoire longue ou de dépendance à long terme (cf. [Ber 94]). La dépendance à long terme (LRD) est généralement définie par une densité spectrale en puissance $fX_\Delta(\nu)$ du processus qui se comporte à l'origine comme :

$$fX_\Delta(\nu) \propto C|\nu|^{-2d}, |\nu| \to 0, avec\_0\langle d\langle 0.5 \qquad (2)$$

La dépendance à long terme dans le trafic Internet est une propriété d'importance car elle entraîne des baisses de performance et de QoS (voir par exemple [Gro 96]). Considérer précisément la LRD est une condition importante pour concevoir des réseaux adaptés aux besoins (taille des buffers, dimensionnement, ...) et en prédire les performances. Il est donc crucial d'incorporer la LRD dans les modèles de description du trafic. Cela élimine de fait les processus poissonnien ou markovien ainsi que leurs déclinaisons.
Par conséquent, les processus à longue mémoire comme les mouvements Browniens fractionnaires, les bruits Gaussiens fractionnaires [Nor 95] ou les modèles *Fractionally Integrated Auto-Regressive Moving Average* (FARIMA) ont été largement utilisés pour décrire et / ou analyser les séries temporelles extraites du trafic Internet (voir [Par 00] et les références associées).
Cependant, à cause de la multitude de mécanismes réseaux et de sources de trafics différents, le trafic présente aussi des caractéristiques de dépendance à court terme (SRD) qui se superposent à celles de mémoire longue (cela a été étudié pour le trafic vidéo VBR [Hua 95]). Par conséquent, utiliser le processus FARIMA [Ber 94] est naturel car il permet de décrire à la fois les dépendances courtes et longues.
Un modèle farima(P,d,Q) est défini par deux polynômes d'ordres P et Q et d'une intégration fractionnaire $\mathbf{D}^{-d}$, d'ordre -1/2 < d < 1/2:

$$X_\Delta(k) = \sum_{p=1}^{P} \phi_p X_\Delta(k-p) + D^{-d}\left(\varepsilon(k) - \sum_{q=1}^{Q} \theta_q \varepsilon(k-q)\right),$$

où les ε(l) sont des variables aléatoires indépendantes, aux distributions identiques avec une moyenne nulle et une variance σ^2_ε. Pour la partie fractionnaire d, l'intégrateur fractionnaire s'exprime par : $D^{-d} = \sum_{i=0}^{\infty} b_i(-d)B^i$, où B est l'opérateur retard Bε(i)=ε(i-1), et $b_i(-d)$ = Γ(i+d)/ Γ (d) Γ (i+1). La densité spectrale de puissance de ce processus est :

$$fX(\nu) = \sigma_\varepsilon^2 \left|1 - e^{-i2\pi\nu}\right|^{-2d} \frac{\left|1 - \sum_{q=1}^{Q} \theta_q e^{-iq2\pi\nu}\right|^2}{\left|1 - \sum_{p=1}^{P} \phi_p e^{-ip2\pi\nu}\right|^2}, \qquad (3)$$

pour -1/2<ν < 1/2. Cela montre que pour d ∈ (0,1/2), ce processus est à mémoire longue.
Dans ce cas, les paramètres ARMA(P,Q) et l'intégration fractionnaire d'ordre d décrivent respectivement la corrélation à court et long terme de façon indépendante. Les polynômes de forme P et Q peuvent être utilisés pour reproduire le spectre des hautes fréquences (i.e. les petites échelles), alors que d représente l'intensité de la mémoire longue (i.e. les grandes échelles).

• **Commentaires.** Pour les analyses et exemples présentés dans cet article, nous allons nous limiter à des processus Farima dont les polynômes P et Q ont un degrés au plus égal à 1, que nous notons dans la suite farima (ϕ, d, θ). Ainsi, les processus Γ(α,β) – farima (ϕ, d, θ) ne comportent que 5 paramètres qu'il faut extraire des données. Ils forment une famille de modèles simples, une propriété importante si on veut pouvoir l'utiliser pour une analyse à la volée (ou en temps-réel) du trafic qui soit robuste et efficace. Il faut toutefois noter que les premier et second ordres statistiques ne caractérisent pas complètement le processus car il est non Gaussien. Cela laisse donc la place pour améliorer ce modèle et l'affiner afin qu'il décrive mieux d'autres propriétés. Toutefois, cette tâche difficile n'est pas nécessaire pour les propriétés du trafic que nous souhaitons pouvoir capturer.

3.2.2.4.2. Analyse

• **Stationnarité des données.** Pour chaque niveau d'agrégation Δ on réalise une analyse de X_Δ. Etant donné l'hypothèse de stationnarité de $X_\Delta$dont nous avions besoin pour la modélisation théorique, nous commençons par une vérification empirique des analyses et estimations obtenues sur des sous-blocs adjacents et disjoints. Ensuite, nous analysons seulement les ensembles de données pour lesquels la stationnarité est une hypothèse raisonnable. C'est une approche dont l'esprit est très proche de celles développées dans [Vei 01]. Il ne reste plus alors qu'à estimer les paramètres du modèle pour chacun des Δ choisis.

• **Estimation des paramètres de la loi Gamma**. Plutôt que d'utiliser la technique classique des moments, $\hat{\beta} = \hat{\sigma}^2 / \hat{\mu}$, $\hat{\alpha} = \hat{\mu} / \hat{\beta}$ $ où $\hat{\mu}$ et $\hat{\sigma}^2$ sont les estimateurs standard pour la moyenne et la variance, nous utilisons une technique basée sur le maximum de vraisemblance pour estimer α et β [Hah 94]. La distribution conjointe de n variables Γ(α,β) indépendantes et identiquement distribuées peut être obtenue comme le produit des n termes, comme dans l'équation 1. La dérivation de ce produit conduit aux estimations de α et β. Il faut noter que le terme ML qui est attribué en standard à cette méthode est utilisé abusivement ici car, dans notre cas, les $X_\Delta(k)$ sont fortement dépendants. Il a d'ailleurs été vérifié – de façon empirique à partir de simulations numériques – que cette procédure d'estimation donne des résultats très précis, même lorsqu'elle est appliquée à des processus à longue mémoire [Sch 05].

• **Estimation des paramètres Farima.** Il est établi aujourd'hui que l'estimation du paramètre de mémoire longue est une tâche difficile en statistiques qui a pourtant été largement étudiée (voir [Dou 03] par exemple, pour une présentation actualisée). Par conséquent l'estimation conjointe des paramètres de mémoire courte et longue du processus farima (ϕ, d, θ) est une tâche très ardue. Une méthode d'estimation basée sur le maximum de vraisemblance des

formes analytiques du spectre dont l'expression est rappelée par l'équation 3 est possible mais est lourde en puissance de traitement.
Nous avons donc développé une procédure d'estimation en deux étapes : tout d'abord, nous estimons le paramètre de LRD d en utilisant une méthode basée sur une décomposition en ondelettes. Cette méthode est celle décrite dans la partie 2.2.2.
Ensuite, à partir de cette estimation à base d'ondelettes $\hat{d}_W$, nous opérons une dérivation fractionnaire d'ordre $\hat{d}_W$ de X_Δ. On élimine ainsi la LRD du processus de sorte qu'il ne reste plus que les composants ARMA. Une procédure itérative classique (basée sur l'algorithme de Gauss-Newton) [Lju 99] est alors appliquée pour estimer les paramètres ARMA. Evidemment, la principale faiblesse de cette procédure d'estimation en deux phases se situe au niveau de la qualité de l'estimation de d. Si d est mal estimé, les paramètres ARMA le seront aussi. Toutefois, la qualité des estimations obtenues avec cette procédure a été étudiée numériquement dans [Sch 05] à partir d'un processus de synthèse de trafic $\Gamma(\alpha,\beta)$ – farima (ϕ, d, θ). Les résultats obtenus sont très bons et valident ainsi cette méthode d'estimation.

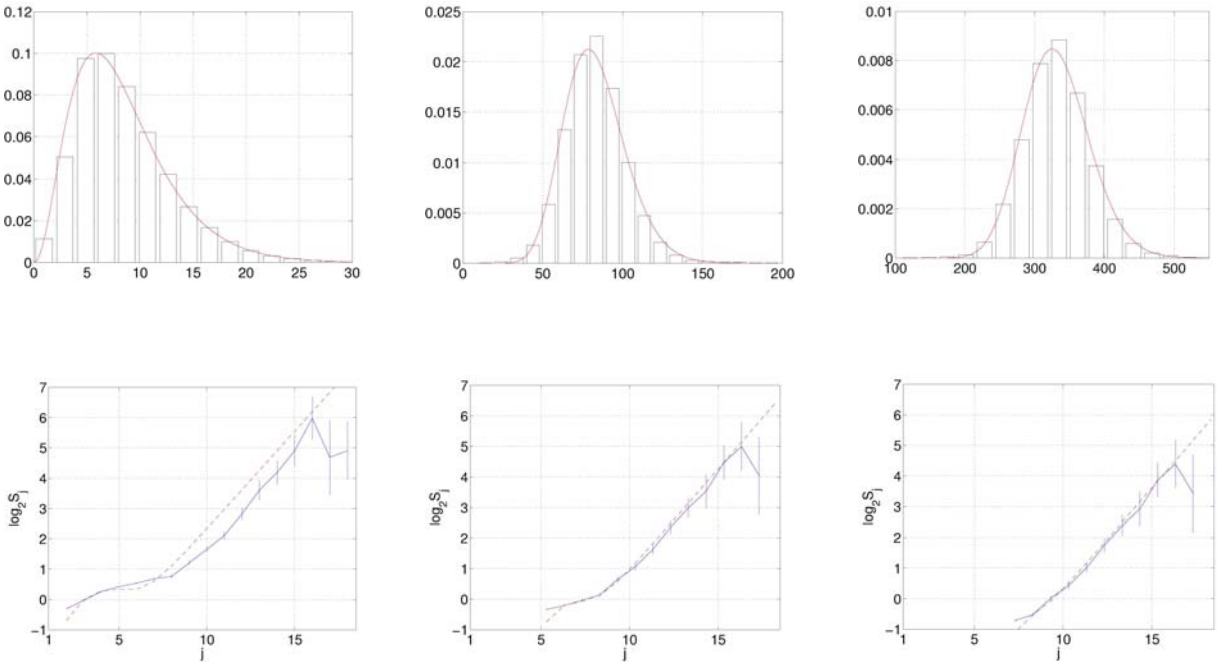

Figure 27 : ***AUCK-IV***. Adéquation des marginales (en haut) et des covariances (en bas) du processus $\Gamma(\alpha,\beta)$ – farima (ϕ, d, θ) pour Δ =10, 100, 400 ms (de gauche à droite); j=1 correspond à 10 ms.

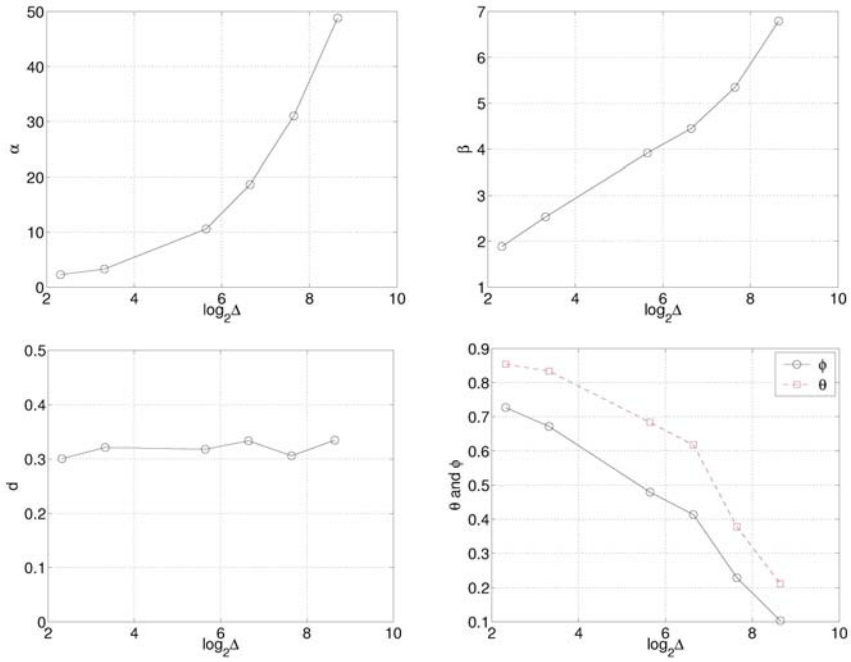

Figure 28 : ***AUCK-IV***. Paramètres estimés du processus Γ(α,β) – farima (ϕ, d, θ) en fonction de $\log_2 \Delta$ (avec Δ en ms).

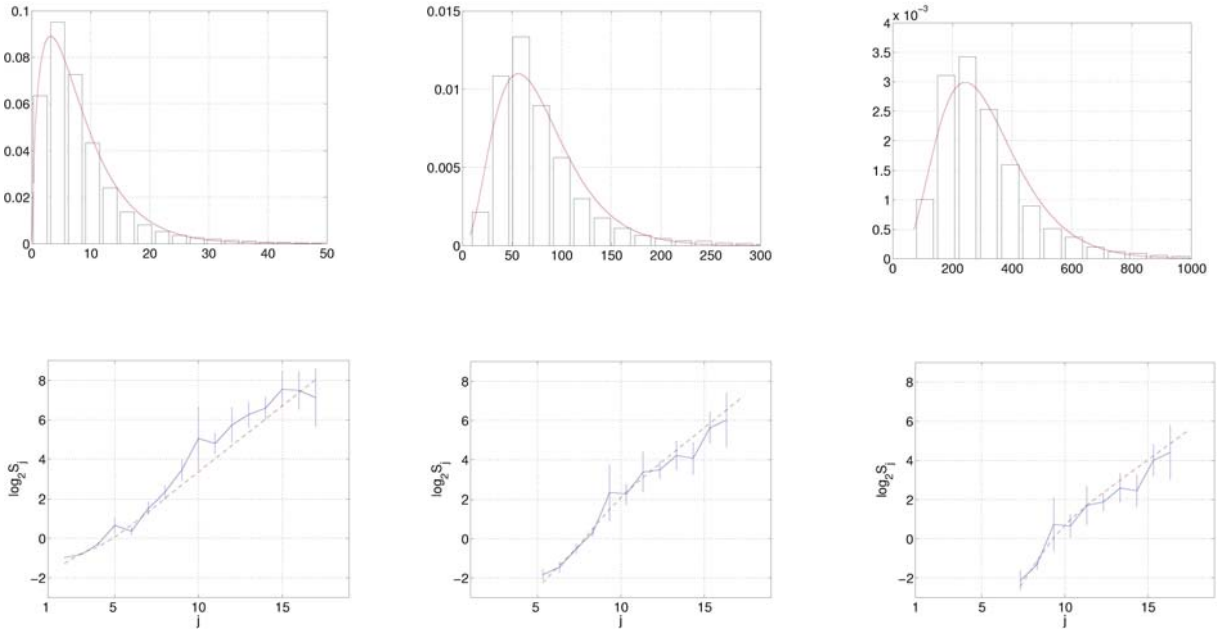

Figure 29 : ***METROSEC-ref1***. Adéquation des marginales (en haut) et des covariances (en bas) du processus Γ(α,β) – farima (ϕ, d, θ) pour Δ =10, 100, 400 ms (de gauche à droite en bas). j=1 correspond à 10 ms.

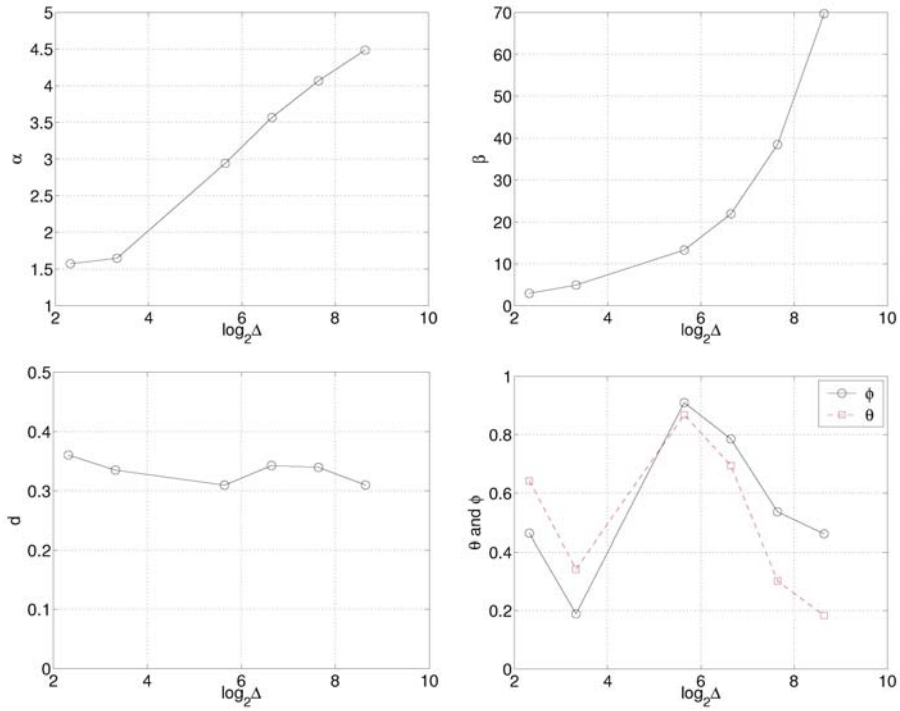

Figure 30 : ***METROSEC-ref1***. Paramètres estimés du processus Γ(α,β) – farima (ϕ, d, θ), en fonction de $\log_2 \Delta$ (avec Δ en ms)

3.2.2.5. Résultats et discussions

3.2.2.5.1. Trafic sans anomalie

Les procédures d'analyse Γ(α,β) – farima (ϕ, d, θ) décrite plus haut ont été appliquées aux séries temporelles du trafic indépendamment pour différents niveaux d'agrégation. Nous présentons ici les résultats détaillés pour les séries issues des traces **AUCK-IV** et **Metrosec-ref1**. Des résultats similaires ont été obtenus pour les autres traces citées dans le tableau 6, mais nous ne les présentons pas dans ce mémoire pour ne pas surcharger.

• **Marginales.** Pour ces deux séries temporelles, la ligne du haut des figures 27 et 29 (le modèle et les histogrammes empiriques correspondent), illustrent respectivement l'adéquation des distributions marginales des processus Γ(α,β) avec $X_\Delta$pour un large spectre de niveaux d'agrégation : 1ms ≤ Δ ≤ 10 s. Cette adéquation a été caractérisée au moyen de tests de χ^2 et de Kolmogorov-Smirnov (non décrits ici). Les distributions Gamma démontrent en général une meilleure adéquation par rapport à celles obtenues avec des lois exponentielles, log-normales ou de χ^2. Pour certaines des séries analysées et certains niveaux d'agrégation, l'une ou l'autre de ces lois peut approximer plus précisément les données que la loi Gamma. Toutefois, les distributions Gamma ne sont jamais très éloignées des données réelles, et même si une distribution particulière approxime mieux les données que la loi Gamma pour un Δ donné, cela n'est pas le cas sur un tout un ensemble de valeurs Δ. A l'opposé, l'adéquation des lois Gamma reste très satisfaisante pour un large spectre de valeurs de Δ, et cela montre une caractérisation des marginales du trafic dépendante de l'échelle d'observation. Les lois Γ(α,β), en faisant varier leurs paramètres de formes et d'échelles, offrent une évolution continue et stable d'une loi exponentielle pure vers une loi Gaussienne.

Ensemble, ces observations militent en faveur de l'utilisation de lois Gamma pour modéliser les marginales du trafic notamment parce que les lois Gamma forment une famille

qui reste stable par l'opération d'addition : pour des variables aléatoires indépendantes X_i (avec i=1, 2), de lois $\Gamma(\alpha,\beta)$, leur somme $X=X_1+X_2$ suit une loi $\Gamma(\alpha_1+\alpha_2,\beta)$. Pour l'agrégation $X_{2\Delta}(k) = X_\Delta(2k) + X_\Delta(2k+1)$. En utilisant la propriété de stabilité par addition, et en supposant l'indépendance des lois, α augmente de façon linéaire avec Δ alors que β reste constant. La première ligne (haute) des figures 28 et 30, montre l'évolution de $\hat{\alpha}$ et $\hat{\beta}$ en fonction de $\log_2\Delta$. Pour toutes les séries temporelles, des écarts significatifs, par rapport à ces comportements idéaux, sont observés. Une analyse attentive montre que $\hat{\alpha}(\Delta)$ n'augmente pas pour les petites valeurs de Δ, puis augmente quasiment comme $\log_2\Delta$ pour des valeurs de Δ plus grandes, alors que le comportement de $\hat{\beta}(\Delta)$ est proche d'une augmentation en loi de puissance. Ces faits constituent des preuves de l'existence de dépendance dans les données. De plus, il faut noter que $\Delta \approx 1$ s, correspond au seuil de longue mémoire (comme cela sera discuté plus loin). Cela signifie que les évolutions de α et β en fonction de Δ montrées ici s'accommodent de la SRD. Les variations conjointes de α et β en fonction du niveau d'agrégation Δ représentent une propriété significative du trafic normal. Nous allons dans la suite utiliser cette propriété pour caractériser et classifier le trafic avec anomalies.

• **Covariances.** Pour les deux séries de référence, la ligne du bas des figures 27 et 29, comparent respectivement les diagrammes (à échelles logarithmiques) obtenus à partir des données avec ceux obtenus avec le modèle. Ces courbes illustrent l'adéquation des covariances du processus farima (ϕ, d, θ) et de X_Δ.
Lorsque Δ augmente, on peut remarquer que les diagrammes sont quasiment obtenus à partir des diagrammes obtenus pour des Δ plus petits que l'on aurait décalés vers les échelles plus grandes. Ceci s'explique facilement car l'agrégation de données consiste à lisser les détails qui apparaissent à des petites échelles, mais qui n'affectent en rien les grandes échelles. Comme on s'y attendait, l'agrégation n'élimine ni n'altère la caractéristique de longue mémoire. On peut le vérifier sur les figures 28 et 30 (en bas à gauche), pour lesquelles $\hat{d}_W$ reste indépendant de Δ. Ceci, une nouvelle fois, souligne que la LRD capture un attribut de longue durée sur le trafic qui n'apparaît pas pour des échelles intermédiaires.
D'un autre côté, les corrélations à courts termes sont éliminées lorsque le niveau d'agrégation augmente. On peut voir sur les figures 28 et 30, en bas à droite, que $\hat{\phi}$ et $\hat{\theta}$ baissent de façon significative lorsque Δ augmente. Ils devraient devenir nuls si le niveau d'agrégation Δ devient plus grand que les échelles des caractéristiques de SRD. La covariance converge théoriquement vers celle d'un bruit Gaussien fractionnaire qui s'avère, pratiquement, être extrêmement proche de celle d'un processus farima(0,d,0). Pour toutes les séries temporelles de référence étudiées ici, l'échelle temporelle pour laquelle la mémoire longue est dominante (mesurée comme le niveau d'agrégation approximatif Δ pour lequel la partie SRD du modèle disparait) correspond à 600 ms $\leq \Delta \leq$ 2 s.

• **Conclusions**. En conclusion (partielle), nous avons mis l'accent sur le fait que pour un large ensemble de traces de trafic différentes collectées sur des réseaux différents, le modèle $\Gamma(\alpha,\beta)$ – farima (ϕ, d, θ) proposé reproduit précisément les marginales ainsi que les corrélations à court et long terme des séries temporelles. Le fait que le modèle proposé est suffisamment versatile pour travailler efficacement sur tous les niveaux d'agrégation est un élément clé pour deux raisons : 1) un problème récurrent de la modélisation du trafic concerne le choix d'un niveau d'agrégation Δ adapté. C'est une question délicate dont la réponse doit tenir compte des caractéristiques des données, l'objectif de la modélisation, ainsi que de problèmes techniques comme les contraintes de temps réel, de taille des tampons ou les contraintes de coûts de

traitement. Par conséquent, choisir Δ a priori peut être très difficile ; l'utilisation d'un processus qui offre une modélisation évolutive en fonction de Δ est donc d'un grand intérêt. 2) les valeurs des paramètres du modèle varient, souvent de façon importante d'un trafic à l'autre. Mais ce ne sont pas les valeurs elles-mêmes qui sont importantes dans ces travaux et pour d'éventuels mécanismes de détection, mais les courbes d'évolution de ces paramètres en fonction de Δ qui offrent des éléments statistiques importants pour l'analyse du trafic.

3.2.2.5.2. Trafic avec anomalies

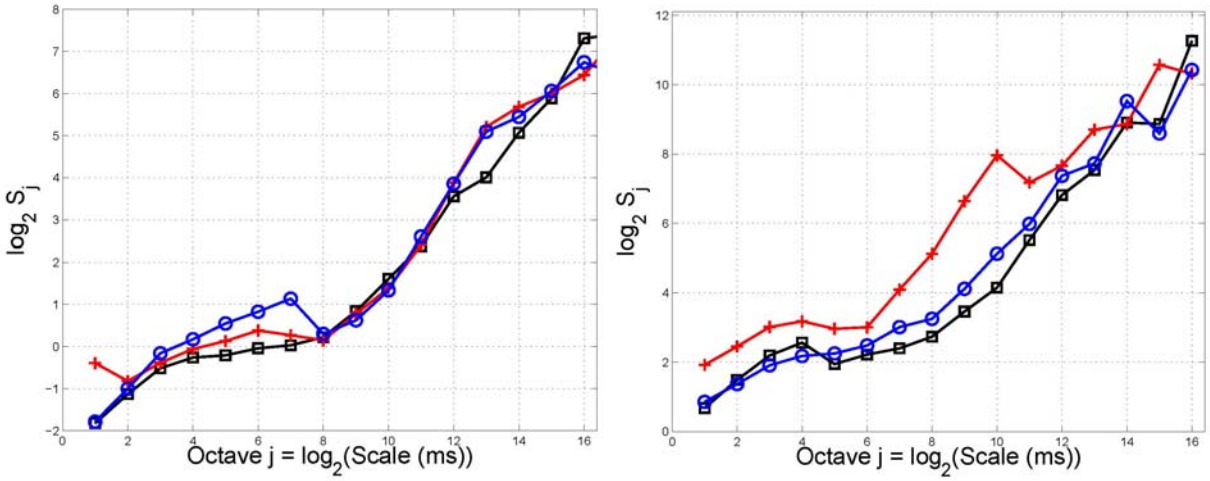

Figure 31 : Diagrammes logarithmiques. Pour la DDoS (gauche) et la Flash Crowd (droite). Pour les deux événements, les courbes sont données pour la période de l'anomalie (croix rouges sur la courbe), avant l'anomalie (carrés noirs) et après (cercles bleus), ces deux derniers cas constituant des références de trafic normal.

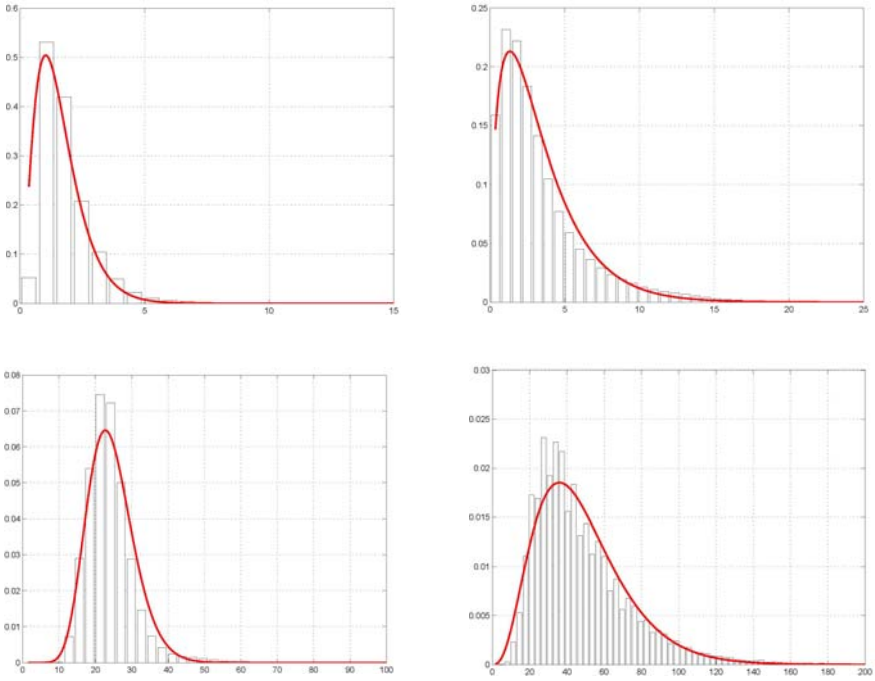

Figure 32 : ***Marginales***. Pour l'attaque DDoS (gauche) et pour la Flash Crowd (droite), adéquation des histogrammes empiriques de X_Δ et les marginales $\Gamma(\alpha,\beta)$ pour Δ = 2ms (haut) and Δ = 32ms (bas)

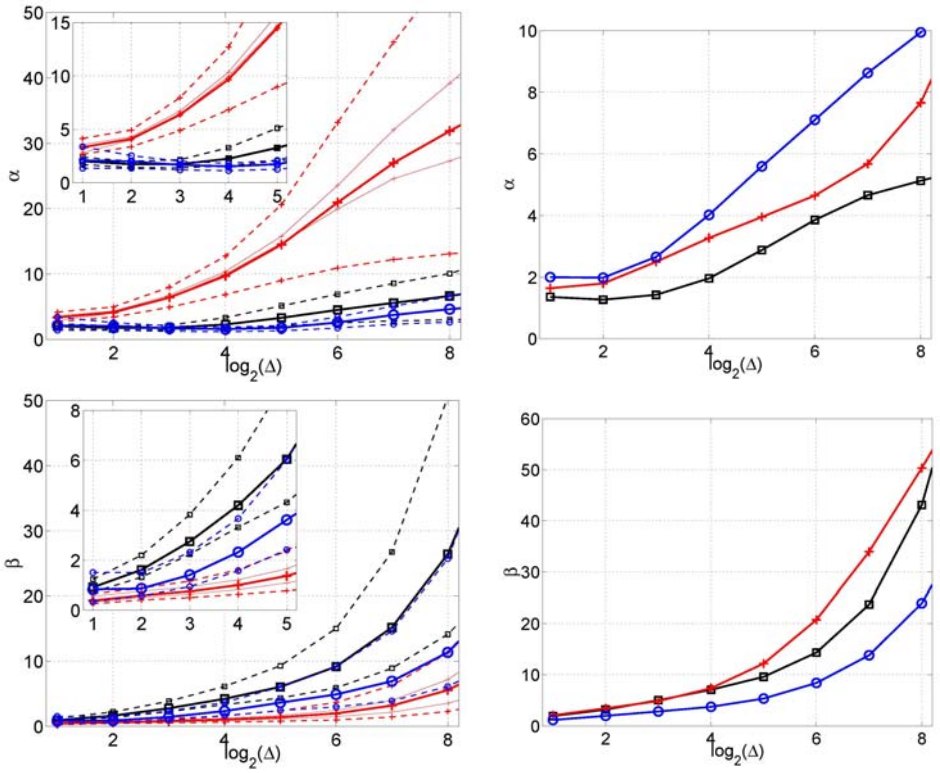

Figure 33: ***Estimation des Γ(α,β).*** Estimation de $\hat{\alpha}$ (haut) et $\hat{\beta}$ (bas) en fonction de $\log_2 \Delta$ pour l'attaque DDoS (gauche) et pour la Flash Crowd (droite). Dans les deux cas, les courbes sont données pour les périodes de l'anomalie (croix rouges), avant (carrés noirs) et après (cercles bleus). Pour l'attaque **DDoS**, l'évolution moyenne des paramètres (ligne épaisse) sur différents blocs de données de 15 min est dessinée et superposée avec les valeurs extrêmes prises pendant chaque période (lignes pointillées). Dans l'exemple, deux évolutions typiques sur un bloc pendant l'attaque sont présentées sur le graphe (lignes fines). Un zoom sur les petites échelles est ajouté. Pour la **FC**, dont la durée est plus courte, une estimation sur une fenêtre de 15 min est rapportée pour chaque période (avant, pendant et après la FC).

• **Attaque DDoS**. Les courbes à gauche de la figure 31, présentent les diagrammes logarithmiques pour des blocs de données d'une heure pendant l'attaque DDoS (Δ = 1ms), par rapport à des blocs d'une heure correspondant à du trafic régulier capturé deux heures avant et après l'attaque. Ces courbes montrent 1) que le modèle farima (ϕ, d, θ) décrit de façon satisfaisante le trafic contenant une attaque DDoS. D'autres courbes, non présentées ici, montrent que c'est également le cas pour de nombreux niveaux d'agrégation.
De plus, pour des échelles supérieures à 500 ms ($ j=9 sur la courbe gauche de la figure 31), aucune différence n'est visible pour les périodes avant/après et pendant l'attaque. En particulier, le paramètre de LRD $\hat{d}_W$ reste étonnamment constant. Cela signifie que la LRD n'est pas créée par l'attaque, mais également qu'elle lui est complètement insensible. La seule différence que l'on remarque sur le diagramme logarithmique est une augmentation relative du composant de SRD (pour les échelles 4 à 7 de j) après l'attaque: C'est dû au fait que les séries du trafic après l'attaque ont été capturées la nuit, et donc avec une charge de trafic plus faible. Le diagramme logarithmique a été décalé vers le haut pour montrer que le paramètre de LRD $\hat{d}_W$ (donné par la pente) ne change pas, même lorsque la charge du réseau est plus faible, et

que, par conséquent, la partie correspondant aux petites échelles augmente. On ne peut donc pas détecter l'anomalie à partir du diagramme logarithmique.
Les deux courbes de la colonne de gauche sur la figure 32 illustrent que les distributions $\Gamma(\alpha,\beta)$.se superposent parfaitement aux marginales du trafic avec attaque. Les deux courbes à gauche de la figure 33 comparent les évolutions des estimations des paramètres $\hat{\alpha}$ et $\hat{\beta}$ en fonction de Δ pour du trafic pendant (croix rouges), avant (carrés noirs) et après (cercles bleus) l'attaque DDoS. Elles représentent les estimations expérimentales moyennes sur des blocs de données disjoints de 15 minutes, superposées avec les valeurs extrêmes prises par ces estimations durant chaque période. Les fenêtres avant et après l'anomalie correspondent à des comportements nominaux pertinents pour le trafic régulier. On peut voir que les fonctions $\hat{\alpha}$ (Δ) et $\hat{\beta}$ (Δ) pendant l'attaque s'écartent significativement des comportements réguliers. Nous insistons sur le fait que les valeurs des paramètres peuvent varier d'un bloc à l'autre, même pendant l'attaque DDoS, mais que les évolutions en fonction de Δ restent comparables et définissent un schéma différent par rapport à celui des trafics normaux.
L'attaque produit une augmentation immédiate et brutale de α dès les petites valeurs de Δ alors que dans des conditions normales α reste constant ou ne présente que des variations limitées, et ce pour $\Delta \approx 20$ ms. L'évolution de β est à l'opposé : il diminue de $\Delta \approx 1$ ms à $ $\Delta \approx$ 30 ms pendant l'attaque DDoS, alors qu'il augmente régulièrement avec Δ dans des conditions normales de trafic. Ces évolutions peuvent être interprétées différemment, en termes d'occurrence d'un *événement 0 paquet* et d'un effet de *Gaussianisation*. Premièrement, comme pendant l'attaque un grand nombre de paquets sont émis avec un débit le plus élevé possible, une conséquence majeure est la possibilité pour un observateur de ne voir aucun paquet (*0 paquet*) dans une fenêtre de taille Δ qui diminue très vite jusqu'à 0 dès que Δ atteint 1 ms. Plus précisément, on observe que les marginales du trafic avec attaque DDoS ne sont pas nulles seulement au delà d'un seuil qui dépend de Δ. C'est une différence majeure avec les marginales du trafic régulier qui décroissent lentement vers 0 lorsque $X_\Delta \to 0$ (comparer les figures 27 ou 29 avec la figure 32). Cet effet a précisément un impact sur les valeurs prises par le paramètre de forme α en fonction de Δ, impliquant que α croît lentement avec Δ pour le trafic régulier et beaucoup plus rapidement pour celui qui contient une attaque.
Deuxièmement, comme cela est mentionné dans la partie 3.2.2.4.1 plus haut, $1/\alpha$ contrôle l'écart entre les distributions $\Gamma(\alpha,\beta)$ et Gaussiennes. Avec le niveau d'agrégation, α tend à toujours croître. Toutefois, les attaques DDoS accélèrent cette croissance avec l'effet de *Gaussianisation*. Ceci constitue une particularité statistique majeure qui différencie le trafic avec attaque du trafic régulier. Pour finir, il faut noter que cet effet implique des échelles pour le trafic allant de 1 ms à 0.5 s, et que la partie ARMA du modèle de covariance (les courbes ne sont pas représentées dans le mémoire pour ne pas le surcharger inutilement) ne peut que très difficilement voir cette partie de la covariance.

• **Flash Crowd**. Les deux courbes de droite de la figure 32 illustrent que les distributions $\Gamma(\alpha,\beta)$ correspondent bien aux marginales du trafic en présence d'une Flash Crowd (FC) et ce pour un large ensemble de niveaux d'agrégation (de 1ms à 1s). Les deux courbes de droite de la figure 32 comparent les évolutions des courbes de $\hat{\alpha}(\Delta)$ et $\hat{\beta}(\Delta)$ pour le trafic pendant (courbe rouge) avant (courbe noire) et après (courbe bleue) la FC. Chaque courbe correspond à des blocs de données de 15 min qui ne se chevauchent pas. Les formes des courbes $\hat{\alpha}(\Delta)$ et $\hat{\beta}(\Delta)$ observées pendant l'événement ne s'écartent pas de façon significative de celles du trafic normal. Quelques écarts existent pour les grandes valeurs de Δ (de 0.5 à 1 s), ce qui est consistant avec les observations faites sur les diagrammes logarithmiques. Cette différence sur

$\hat{\alpha}(\Delta)$ observée entre une attaque DDoS et une FC est consistante avec le fait que la FC n'intègre pas de mécanisme tendant à empêcher le phénomène *0 paquet par fenêtre* contrairement à l'attaque DDoS.
La courbe de droite de la figure 31 présente les diagrammes logarithmiques de deux blocs de données de 15 min pendant la FC (Δ = 1 ms) à comparer avec les blocs de données, de 15 min aussi, enregistrés quelques minutes avant et après la FC. Sur cette courbe, on voit nettement un changement sur le diagramme logarithmique pendant la FC. Pour les octaves j =8 à j= 10, i.e., pour les échelles de temps allant de 250 ms à 1 s, un fort pic d'énergie apparaît (un tel pic n'a jamais été observé pour du trafic régulier). Naturellement, le processus farima (ϕ, d, θ) (les courbes ne sont pas présentées par manqué de place) échoue à représenter tout à la fois la SRD, la LRD et ce pic d'énergie. Les tests de concordance entre les données et le modèle associé conduit à un rejet, ce qui nous offre en fait un outil pertinent pour détecter ces anomalies. Notons également que le paramètre de LRD d, lorsqu'il est estimé pour des octaves supérieures à celles correspondant au pic d'énergie ne s'écartent pas significativement des valeurs estimées avant et après la FC. Cela signifie que la LRD n'est pas due à la FC et qu'elle n'est pas affectée par la FC. Au pire, le pic d'énergie agit comme un effet masquant dans un sous intervalle d'échelles temporelles, de 250 ms à 2 s.

• **Commentaires.** Il faut ainsi noter que comme cela a été dit dans l'introduction, l'estimation de la moyenne et la variance de X_Δ en fonction de Δ ne permet pas de distinguer des trafics avec ou sans anomalies, et encore moins entre une attaque DDoS ou une FC. Toutes les courbes $\hat{\mu}(\Delta)$ et $\hat{\sigma}^2(\Delta)$ ont les mêmes formes.
La forme farima de la covariance n'arrive pas à représenter le pic d'énergie dû à la FC pour certaines échelles spécifiques. Les distributions $\Gamma(\alpha,\beta)$ reproduisent les marginales de tous les types de trafic avec et sans anomalies, que ces anomalies soient légitimes ou non. Ainsi – surveiller l'adéquation du modèle $\Gamma(\alpha,\beta)$ – farima (ϕ, d, θ) avec l'évolution des paramètres estimés en fonction de Δ, pour Δ allant de 1 ms à 10 s – permet de distinguer des trafics avec et sans anomalies, et même de classifier les anomalies en anomalies légitimes ou illégitimes.

• **Détection.** Une application majeure de ce travail concerne donc la détection en temps réel d'anomalies dans le trafic. Pour une bonne caractérisation statistique, les analyses de la partie 3.2.2.5.1 ont été réalisées sur des blocs d'une heure pour les séries temporelles de référence, et de 15 min pour les séries liées aux attaques et aux FC. De telles durées permettaient des descriptions statistiques précises, mais correspondent naturellement à des durées d'observation trop longues pour satisfaire aux besoins d'une détection rapide des anomalies. Nous développons donc actuellement des outils de surveillance de α, β, θ et ϕ, ainsi que des formes globales des marginales et des diagrammes logarithmiques pour des périodes d'observation plus courtes.
La figure 34 montre l'estimation de $\hat{\alpha}(\Delta)$ sur des fenêtres d'une minute. L'évolution de la moyenne $\hat{\alpha}$ reproduit les caractéristiques soulignées pour des fenêtres de 15 minutes (voir la figure 32, pendant l'attaque ou pour le trafic de référence (avant et après l'attaque).On voit clairement que la forme de la courbe $\hat{\alpha}(\Delta)$ subit un changement drastique à toutes les échelles pendant l'attaque DDoS. Ce changement pourrait être quantifié au moyen de distances (de type Kullback ou Bhattacharyya par exemple) ou de divergences [Bas 89]. De plus, l'analyse étant faite sur des blocs d'une minute, une détection fiable sur un temps très court pourrait être effectuée. Ceci pourrait servir comme un des éléments de base à la conception d'un IDS.

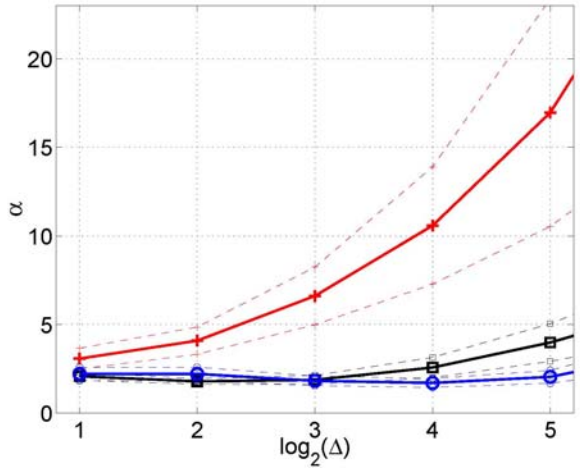

Figure 34: ***Attaque DDoS***: Moyenne de $\hat{\alpha}$ sur des fenêtres d'une minute. $\hat{\alpha}$ (ligne pleine), et écart maximum (lignes pointillées) en fonction de $\log_2\Delta$, pendant (croix rouges), avant (carrés noirs) ou après (cercles bleus) l'anomalie.

3.2.3. Conclusions sur les premiers résultats et travaux futurs

Nous venons d'introduire un processus non gaussien dépendant à long terme, le Γ(α,β) – farima(P,d,Q), pour modéliser les statistiques de premier et second ordre du trafic des réseaux d'ordinateurs. Nous avons également décrit des procédures d'estimation des paramètres correspondants. Nous avons montré sur un grand nombre de trafics standards de référence qu'il constitue un modèle à la fois pertinent et versatile, et ce pour un grand nombre de niveaux d'agrégation Δ. De plus, ses paramètres évoluent régulièrement avec Δ fournissant ainsi une caractérisation statistique utile du trafic régulier. Nous avons également montré que des écarts par rapport à ces comportements de référence (selon Δ) nous permettent de distinguer des trafics avec ou sans anomalies, et aussi de déterminer si les anomalies sont légitimes (flash crowds) ou illégitimes (attaque DDoS).
Ce travail peut être étendu selon plusieurs axes de recherche. En premier, nous allons continuer à explorer le bestiaire des trafics réguliers et avec anomalies en analysant des traces de trafic très récentes, ainsi qu'en provoquant une plus grande variété d'anomalies (attaques DDoS plus avancées et plus diffuses, des flash crowds plus importantes, des pannes de réseau,...). Dans ce but, une plate-forme expérimentale (incluse à laasnetexp.fr) a été mise en place dans le cadre du projet METROSEC. Nous voulons à la fois explorer les possibilités pour notre modèle de caractériser significativement ce grand nombre d'anomalies, et l'enrichir. Deuxièmement, en utilisant les caractérisations statistiques que nous avons faites, nous espérons mettre au point dans un futur proche un mécanisme de détection capable d'identifier automatiquement les changements dans ces caractéristiques statistiques et de les classifier en anomalies légitimes ou illégitimes. Il devrait fonctionner comme un IDS, et se baser sur des fenêtres d'observation temporelles courtes. Comme nous l'avons vu dans la partie 3.2.1, notre but ultime est de développer des mécanismes et des stratégies réseaux (protocoles, architectures, ...) pour améliorer la robustesse des réseaux aux attaques. Cette insensibilité accrue devrait permettre de maintenir le niveau de QoS requis. Ce travail constitue une première étape vers cet objectif global.

L'apport des « pots de miel »
Dans ce thème de recherche à long terme, nous pensons également qu'un IDS serait d'autant plus performant s'il avait une connaissance de l'activité « pirate » ou « illicite » dans

l'Internet. Nous avons donc comme projet de mesurer, ou du moins, d'estimer et d'analyser cette activité et d'identifier et évaluer les menaces qu'elle représente. Pour cela, nous proposons une approche dont l'originalité réside dans l'utilisation conjointe de la métrologie réseaux et de pots de miels, et notamment de pots de miel à haute interaction incluant le niveau réseau.

Il existe plusieurs définitions pour un « pot de miel ». Lance Spitzner, le leader du projet honeynet, définit un « pot de miel » comme une ressource dont le rôle est d'être sondé, attaqué ou compromise [Hon 05]. Une autre définition considère les « pots de miel » comme des environnements dans lesquels des vulnérabilités ont été délibérément introduites pour observer des attaques et des intrusions [Dac 04]. Entre ces deux définitions, nous préférons plutôt définir le « pot de miel » comme une ressource d'un système d'information dont l'intérêt se situe au niveau des utilisations illicites de la ressource en question [Hol 05].

Les pots de miel sont donc des machines dont personne ne se sert et pour lesquelles tout paquet reçu devient suspect. Ces pots de miel permettent donc de tracer une activité sur le réseau qui est, a priori, illicite. Parmi ces pots de miel, le plus grand nombre de ceux qui sont utilisés aujourd'hui sont dits à basse interaction : ils apparaissent comme des machines normales, avec des interfaces applicatives standards, mais ces interfaces sont en fait des coquilles vides : les requêtes des internautes – a priori des pirates – sont enregistrées, mais le service associé n'est pas rendu. Les traces ainsi constituées permettent de connaître l'activité illégale présente sur l'Internet. Par rapport à la problématique de la sécurité des réseaux d'infrastructures, ces pots de miel présentent deux limites : d'abord, ils se positionnent comme une station d'extrémité et ne peuvent pas capter les attaques réseau (comme les attaques des sessions BGP par exemple), puis, comme ils ne se comportent pas comme une vraie machine (les services ne sont pas rendus), les pirates expérimentés s'aperçoivent vite de la supercherie, et s'informent entre eux des nouveaux pots de miel afin de les éviter dans le futur. Les pots de miel classiques, dits aussi à basse interaction, ne sont finalement que des « attrape-nigauds » pas forcément bien adaptés pour capturer l'activité des pirates les plus dangereux.

Les travaux futurs que nous allons mener proposent donc de corriger ces lacunes en proposant d'utiliser des pots de miel à haute interaction (existants ou à concevoir et développer), qui en plus d'enregistrer l'activité des pirates, vont se comporter comme des machines normales, et laisser le pirate dérouler complètement son attaque. De plus, ces pots de miel pourront simuler des composants du réseau comme des routeurs, commutateurs, serveurs réseau, etc. – afin de pouvoir avoir une image de l'activité illicite à l'encontre des infrastructures du réseau – ce qui est une des originalités de cette approche. De plus, pour collecter encore plus d'informations sur les attaques, nous couplerons les pots de miel avec des outils de métrologie, afin d'analyser ces attaques et mesurer leur impact sur le fonctionnement du réseau et sur sa qualité de service.

Ce travail a démarré en mars 2006 ; un premier pot de miel à haute interaction – *Nepenthes* [Hol 05] – a été installé début avril 2006. Son but est de détecter et identifier les machines corrompues (Zombies ou bots) qui appartiennent à des botnets (armées de zombies) utilisées pour perpétrer des attaques de DDoS à large échelle dans l'Internet. Nous pensons qu'identifier ces machines potentiellement dangereuses peut aider ensuite à ajuster les mécanismes de détection d'intrusion, et les renforcer lorsqu'il s'agit d'un trafic venant d'une machine corrompue. Dés sa mise en service, nous avons pu observer une activité significative sur notre pot de miel. Toutefois, il n'est pas en service depuis assez de temps pour pouvoir tirer des conclusions ou des statistiques sûres. De plus, nous sommes légalement obligés de brider les possibilités de notre pot de miel à haute interaction, car s'il est piraté et sert à son tour à pirater d'autres machines, la responsabilité pénale incombe au LAAS. Nous sommes donc obligés de contrôler et souvent bloquer le trafic qui sort de notre pot de miel, ce qui limite ce que l'on peut observer de l'activité des pirates que l'on bride.

Ce travail s'effectue pour partie dans le cadre du projet MetroSec, mais également dans le cadre du projet RNRT OSCAR (démarré en avril 2006) sous la conduite de France Télécom R&D, un grand opérateur national aux prises avec de nouveaux problèmes de sécurité liés au développement actuel de l'Internet grand public et des besoins de ses clients industriels et institutionnels. Ce projet intègre également Mitsubishi Electrics un grand groupe spécialisé dans la fourniture de services et équipements de communication – principalement dans le sans fil, et Miriad technologie, une PME en île de France spécialisée dans la fourniture de composants de sécurité pour les réseaux et les serveurs. L'objectif du projet, en plus de sécuriser le réseau d'infrastructures, est de sécuriser les réseaux d'overlay communautaires que sont les réseaux P2P, de jeux distribués et de voix sur IP, afin que ceux-ci fonctionnent normalement tout le temps, i.e. qu'ils aient une disponibilité de 100%, même en cas d'attaques.

Impact sur les expérimentations

Sortant du cadre de ce thème de recherche sur la sécurité, les premiers résultats qui découlent des 18 premiers mois de travail – par le biais du modèle $\Gamma(\alpha,\beta)$ – farima (ϕ, d, θ) – vont avoir un impact sur la façon dont nous gérons nos expérimentations, que ce soit en simulation ou en émulation. En effet, cette caractérisation $\Gamma(\alpha,\beta)$ – farima (ϕ, d, θ) du trafic Internet ouvre de nouvelles possibilités pour l'émulation de trafic réaliste. En effet, grâce à ce modèle on peut envisager une nouvelle façon de générer du trafic de fond réaliste, avec ou sans anomalies, et ce, à moindre coût en termes de machines à utiliser pour les différentes sources. C'est un résultat essentiel pour permettre de plus facilement réaliser des expérimentations à grande échelle sur Grid Explorer et laasnetexp.fr.

Ainsi, un générateur de trafic selon le modèle $\Gamma(\alpha,\beta)$ – Farima (ϕ, d, θ) sera développé et validé dans un futur proche.

4. Bibliographie

[Abr 98] P. Abry, D. Veitch, "Wavelet analysis of long-range dependent traffic", IEEE Transactions on Information Theory, Vol. 44, n° 1, pp. 2-15, 1998

[Abr 00] P. Abry, P. Flandrin., M. Taqqu, D. Veitch, "Wavelets for the analysis, estimation and synthesis of scaling data", In Self-Similar Network Traffic and Performance Evaluation, K. Park and W. Willinger, Eds., Wiley, 2000

[Ada 00] A. Adams, T. Bu, R. Caceres, N. Duffield, T. Friedman, J. Horowitz, F. Lo Presti, S. B. Moon, V. Paxson, D. Towsley, "The Use of End-to-end Multicast Measurements for Characterizing Internal Network Behavior", IEEE Communications, Vol. 38, n° 5, pp. 152-159, May 2000

[Alm 99a] G. Almes, S. Kalidindi, M. Zekauskas, "A One-way Delay Metric for IPPM", RFC 2679, September 1999

[Alm 99b] G. Almes, S. Kalidindi, M. Zekauskas, "A One-way Packet Loss Metric for IPPM", RFC 2680, September 1999

[Alm 99c] G. Almes, S. Kalidindi, M. Zekauskas, "A Round-trip Delay Metric for IPPM", RFC 2681, September 1999

[Alt 00] E. Altman, K. Avrachenkov, C. Barakat, "A Stochastic Model of TCP/IP with Stationary Random Losses", ACM SIGCOMM, 2000

[And 98] A. Andersen, B. Nielsen, "A Markovian approach for modelling packet traffic with long range dependence", IEEE Journal on Selected Areas in Communications, Vol. 5, n° 16, pp. 719-732, 1998

[Aps 97] J. Apsidorf, "OC3MON: Flexible, affordable, high performance statistics collection", Proceedings of INET, June 1997

[Aqu 05] Site web du projet Européen AQUILA, http://www-st.inf.tu-dresden.de/aquila/

[Asg 02] A. Asgari, P. Trimintzios, M. Irons, G. Pavlou, R. Egan, S. V. den Berghe, "A Scalable Real-Time Monitoring System for Supporting Traffic Engineering", Proc. IEEE Workshop on IP Operation and Management, Dallas, TX, Octobre 2002

[Asg 04] A. Asgari, R. Egan, P. Trimintzios, G. Pavlou,"Scalable monitoring support for resource management and service assurance", IEEE Network, Vol. 18, n° 6, pp. 6-18, November/December 2004

[Ban 04] S. Banerjee, T.G. Griffin, M. Pias, "The interdomain connectivity of PlanetLab nodes", 5th International workshop on Passive and Active Measurements (PAM'2004), Antibes Juan-les-pins, France, April 2004

[Bar 02] C. Barakat, P. Thiran, G. Iannaccone, C. Diot, P. Owezarski, "A flow model for Internet backbone traffic", 2nd SIGCOMM Internet Measurement Workshop (IMW'2002), Marseille, France, November 6-8th, 2002

[Bar 02a] P. Barford, J. Kline, D. Plonka, A. Ron, "A signal analysis of network traffic anomalies", ACM SIGCOMM Internet Measurement Workshop, Marseille, France, November 2002

[Bas 89] M. Basseville, "Distance measures for signal processing and pattern recognition", European Journal on Signal processing, Vol. 18, n° 4, pp. 349-369, December 1989

[Ben 03] N. Ben Azzouna, F. Guillemin, "Analysis of ADSL traffic on an IP backbone link", In Proc. Globecom 2003, San Francisco, December 2003

[Ber 94] J. Beran, "Statistics for Long-Memory Processes", Monographs on Statistics and Applied Probability, Chapman and Hall, New York, NY, 1994

[Ber 95] J. Beran, R. Sherman, M. S. Taqqu, W. Willinger, "Long-range dependence in Variable-Bit-Rate video traffic", IEEE Transactions on Communication, Vol. 43, n° 2/3/4, pp. 1566-1579, 1995

[Bla 92] U. Black, "TCP/IP and related protocols", McGraw-Hill, 1992

[Bla 98] S. Blake, D. Black, M. Carlson, "An Architecture for Differentiated Services", RFC 2475, 1998

[Bol 99] V. A. Bolotin, Y. Levy, D. Liu, "Characterizing data connection and messages by mixtures of distributions on logarithmic scale", Proc. of ITC ’16, pp. 887-894, P. Key and D. Smith (Editors), Elsevier, June 1999

[Bra 97] R. Braden, L. Zhang, "Resource ReSerVation Protocol (RSVP) -- Version 1 message processing rules", RFC 2209, September 1997

[Bru 00] J. Brutlag, "Aberrant behavior detection in time series for network monitoring", USENIX system administration conference, New Orleans, December 2000

[Bur 05] W. Burakowski, M. Yannuzzi, X. Masip-Bruin, R. Serral-Gracià, J. Domingo-Pascual, P. Owezarski, N. Larrieu, G. García de Blas, M. Á. Callejo Rodríguez, J. A. Colás, A. Beben, M. Dąbrowski, J. Śliwiński, D. Duda, P. Krawiec, G. Saccomandi, F. Travaglini, "Developing the monitoring and measurement system", Deliverable of the EuQoS project, funded by the EC under grant IST 004503, July 2005

[Cac 99] R. Caceres, N. Duffield, D. Towsley, J. Horowitz, "Multicast-based Inference of Network-internal loss characteristics", IEEE Transactions on Information Theory, vol. 45, n° 7, pp. 2462-2480, November 1999

[Cai 05] "CAIDA web site", http://www.caida.org

[Cao 01] J. Cao, W.S. Cleveland, D. Lin, D.X. Sun, "Internet traffic tends to Poisson and independent as the load increases", Bell Labs report, available at http://cm.bell-labs.com/cm/ms/departments/sia/InternetTraffic/webpapers.html

[Cha 00] J. Charzinski, "HTTP/TCP connection and flow characteristics", Performance Evaluation, Vol. 42, n° 2-3, pp. 149-162, September 2000

[Che 02] C.M. Cheng, T.T. Kung, K.S. Tan, "Use of spectral analysis in defense against DoS attacks", IEEE Globecom, 2002

[Cla 95] K. Claffy, H-W Braun, G. Polyzos, "A parametrizable methodology for Internet traffic flow profiling", IEEE Journal on Selected Areas in Communication, Vol. 13, n° 8, pp. 1481-1494, October 1995

[Cla 98] K. Claffy, G. Miller, K. Thompson, "The nature of the beast: recent traffic measurements from an Internet backbone", Proc. of INET ’98, Geneva,

Switzerland, July 1998 (http://www.isoc.org/isoc/conferences/inet /98/proceedings/6g/6g_3.htm)

[Cle 00] J. Cleary, S. Donnelly, I. Graham, A. McGregor, M. Pearson, "Design principles for accurate passive measurement", PAM 2000, Hamilton, New Zealand, April 2000

[Cor 01] "CoralReef website", http://www.caida.org/tools/measurement/coralreef

[Cox 84] D. R. Cox, "Long-Range Dependance: A Review", The Iowa State University Press, 1984

[Cro 97] M. Crovella, A. Bestavros, "Self-similarity in World Wide Web traffic : Evidence and possible causes", IEEE/ACM Transactions on Networking, Vol. 5, n° 6, pp. 835-846, December 1997

[Dac 04] M. Dacier, F. Pouget, H. Debar, "Attack processes found on the internet", In Proceedings of NATO Symposium IST-041/RSY-013, 2004

[Dag 01] "Dag 4 SONET network interface", http://dag.cs.waikato.ac.nz/dag/dag4-arch.html

[Dil 01] M. Dilman, D. Raz, "Efficient reactive monitoring", INFOCOM, 2001

[Don 05] B. Donnet, T. Friedman, M. Crovella, "Improved Algorithms for Network Topology Discovery", Passive and Active Measurement (PAM) Workshop, March 2005

[Dou 03] P. Doukhan, G. Oppenheim, M.S. Taqqu, "Long-Range dependence: theory and applications", Birkhäuser, Boston, 2003

[Dow 01] A.B. Downey, "Evidence for long-tailed distributions in the Internet", ACM SIGCOMM Internet Measurement Workshop, November, 2001

[Els 05] C. Elster, D. Raz, R. Wolff, "Autonomous End to End QoS Monitoring", IFIP workshop on End to end monitoring (E2EMON), May 2005

[Eva 00] M. Evans, N. Hastings, B. Peacock, "Statistical distributions", Wiley (Interscience division), June 2000

[Exp 03] E. Exposito, "Spécification et mise en oeuvre d'un protocole de transport orienté Qualité de Service pour les applications multimédias", Thèse de doctorat, Institut National Polytechnique, Toulouse, 17 Décembre 2003

[Fal 99] M. Faloutsos, P. Faloutsos, C. Faloutsos, "On power-law relationship of the Internet topology", ACM SIGCOMM 1999

[Far 05] S. Farraposo, K. Boudaoud, L. Gallon, P. Owezarski, "Some issues raised by DoS attacks and the TCP/IP suite", 4th Conference on Security and Network Architectures (SAR'2005), Batz sur Mer (France), 6 - 10 Juin 2005

[Fel 00] A. Feldmann, "Characteristics of TCP connection arrivals", In 'Self-similar network traffic and performance evaluation', edited by K. Park and W. Willinger, J. Wiley & Sons, 2000

[Fel 00a] A. Feldmann, A. Greenberg, C. Lund, N. Reingold, J. Rexford, F. True, "Deriving traffic demands for operational IP networks: Methodology and Experience", ACM SIGCOMM Conference, Stockholm, 2000

[Fel 98] A. Feldmann, A. C. Gilbert, W. Willinger, "Data networks as cascades: Explaining the multifractal nature of Internet WAN traffic", Proceedings of ACM SIGCOMM '98, August 1998

[Fel 98a] A. Feldmann, A. C. Gilbert, W. Willinger, T. G. Kurtz, "The changing nature of network traffic: Scaling phenomena", Computer Communication Review, Vol. 28, n° 2, pp. 5-29, April 1998

[Flo 94] S. Floyd, "TCP and Explicit Congestion Notification", ACM Computer Communication Review, vol. 24, n°. 5, pp. 10-23, October 1994

[Flo 01] S. Floyd, V. Paxson, "Difficulties in simulating the Internet", IEEE/ACM Transactions on Networking, Vol. 9, n° 4, pp. 392-403, August 2001

[Gar 01] J.M. Garcia, D. Gauchard, O. Brun, P. Bacquet, J. Sexton, E. Lawless, "Modélisation différentielle du trafic et simulation hybride distribuée", Calculateurs parallèles, Vol. 18, n° 3, 2001

[Gro 96] M. Grossglauser, J. Bolot, "On the relevance of long-range dependence in network traffic", ACM SIGCOMM, 1996

[Hah 94] G.J. Hahn, S.S. Shapiro, "Statistical models in engineering", page 88, Wiley (Interscience Division), June 1994

[Han 03] M. Handley, S. Floyd, J. Pahdye, J. Widmer, "TCP Friendly Rate Control (TFRC): Protocol Specification", RFC 3448, Proposed Standard, January 2003

[Hey 98] D. Heyman, "Some issues in performance modeling of data teletraffic", Performance Evaluation, Vol. 34, n° 4, pp. 227-247, December 1998

[Hey 00] D. P. Heyman, T. V. Lakshman, "Long Range Dependence and queueing effects for VBR video", In "Self-similar network traffic and performance evaluation", edited by K. Park and W. Willinger, J. Wiley & Sons, 2000

[Hol 05] T. Holz, "New fields of application for honeynets", PhD thesis, RWTH Aachen, Germany, August, 2005

[Hon 05] The Honeynet Project, "Know your enemy", http://www.honeynet.org, 2005

[Hua 95] C. Huang, M. Devetsikiotis, I. Lambadaris, A. Kaye, "Modeling and simulation of self-similar Variable Bit Rate compressed video: a unified approach", ACM SIGCOMM, Cambridge, UK, August 1995

[Huf 01] B. Huffaker, M. Fomenkov, D. Moore, K. Claffy, "Macroscopic Analyses of the Infrastructure: Measurement and Visualization of Internet Connectivity and Performance", PAM'2001 (Passive and Active Measurements) workshop, Amsterdam, The Netherlands, April 2001

[Hus 03] A. Hussain, J. Heidemann, C. Papadopoulos, "A Framework for classifying denial of service attacks", ACM SIGCOM, Karlsruhe, Germany, August 2003

[Jen 00] A. K. Jena, A. Popescu, P. Pruthi, "Modeling and analysis of HTTP traffic", Proceedings of ITC Specialist Seminar on IP Traffic Modeling, Measurement and Management, September 2000

[Jin 04] S. Jin, D. Yeung, "A covariance analysis model for DDoS attack detection", IEEE International Conference on Communication (ICC'2004), Paris, France, 20-24 June, 2004

[Jun 02] J. Jung, B. Krishnamurthy, M. Rabinovitch, "Flash Crowds and Denial of Service Attacks: characterization and implications for CDNs and web sites", International WWW conference, Honolulu, HI, May 2002

[Kal 99] S. Kalidindi, M.J. Zekauskas, "Surveyor: An infrastructure for Internet performance measurements", Proceedings of INET'99, June 1999

[Kan 05] S. Kandula, D. Katabi, M. Jacob, A. Berger, "Botz-4-sale: surviving organized DDoS attacks that mimic Flash Crowds", In A. Vahdat and D. Wetherall, editors, USENIX' NSDI'05, Boston, MA, May, 2005

[Kar 04] T. Karagiannis, M. Molle, M. Faloutsos, A. Broido, "A non stationary Poisson view of the Internet traffic", Infocom'2004

[Key 01] K. Keys, D. Moore, R. Koga, E. Lagache, M. Tesch, K. Claffy, "The Architecture of the CoralReef: An Internet Traffic Monitoring Software Suite", PAM'2001 (Passive and Active Measurements) workshop, Amsterdam, The Netherlands, April 2001

[Lak 04] A. Lakhina, M. Crovella, C. Diot, "Diagnosing network-wide traffic anomalies", ACM SIGCOMM, August 2004

[Lar 05a] N. Larrieu, P. Owezarski, "Measurement based networking approach applied to congestion control in the multi-domain Internet", 9th IFIP/IEEE International Symposium on Integrated Network Management (IM'2005), Nice, France, 15-19 May 2005

[Lar 05b] N. Larrieu, "Contrôle de congestion et gestion du trafic à partir de mesures pour l'optimisation de la QoS dans l'Internet", Thèse de doctorat de 3ème cycle de l'INSA de Toulouse, 4 juillet 2005

[Lar 05c] N. Larrieu, P. Owezarski, H. Martin-Deidier, P. Spiesser, "Présentation du logiciel ZOO", Rapport LAAS N°05579, Octobre 2005

[Lel 93] W. Leland, M. Taqqu, W. Willinger, D. Wilson, "On the self-similar nature of Ethernet traffic", ACM SIGCOM, September 1993

[Lel 94] W. Leland, M. Taqqu, W. Willinger, D. Wilson, "On the self-similar nature of Ethernet traffic", IEEE/ ACM Transactions on Networking, Vol. 2, n° 1, pp. 1-15, 1994

[Li 03] L. Li, G. Lee, "DDoS attack detection and wavelets", International Conference on Computer Communications and Networks (ICCCN'03), Dallas, TX, 2003

[Lju 99] L. Ljung, "System identification: theory for the user", chapter 10.2 PTR Prentice Hall, 1999

[Mah 97] B. Mah, "An empirical model of HTTP network traffic", Proc. of INFOCOM '97, pp. 592-600, April 1997

[Mal 99] S. Mallat, "A Wavelet tour of signal processing", Academic Press, 1999

[Mar 01] B. Martinet, J-F. Scariot, "La métrologie, base pour la sécurité : NetSEC", Journées réseaux (JRES'2001), Lyon, France, 10-14 décembre 2001

[Mat 96] M. Mathis, J. Mahdavi, S. Floyd, A. Romanow, "TCP Selective Acknowledgment Options", Request for Commentsc 2018, October 1996

[McC 00] S. McCreary, K. C. Claffy, "Trends in Wide Area IP traffic patterns: A view from Ames Internet Exchange", Proceedings of ITC Specialist Seminar on IP

Traffic Modeling, Measurement and Management, Sept. 2000 (see also CAIDA Technical Report http://www.caida.org/outreach/papers/2000/AIX0005/)

[Mcg 00] T. McGregor, H.-W. Braun, J. Brown, "The NLANR network analysis infrastructure", IEEE Communications, vol. 38, no. 5, pp. 122-128, May 2000

[Mel 93] B. Melamed, "An overview of TES processes and modeling methodology", Performance/SIGMETRICS tutorials, 1993

[Mil 04] I. Miloucheva, P.A. Gutierrez, D. Hetzer, A. Nassri, M. Beoni, "Intermon architecture for complex QoS analysis in inter-domain environment based on discovery of topology and traffic impact", Inter-domain Performance and Simulation Workshop, Budapest, March 2004

[Mol 00] S. Molnar, T. D. Dang, "Scaling analysis of IP traffic components", Proc. of ITC Spec. Seminar on IP Traffic Modeling, Measurement and Management, September 2000

[Mom 05] Projet IST MOME : http://www.ist-mome.org

[Moo 01] D. Moore, G.M. Voelker, S. Savage, "Inferring Internet denial-of-service activity", USENIX security symposium, 2001

[Nab 98] M. Nabe, M. Murata, H. Miyahara, "Analysis and modeling of World Wide Web traffic for capacity dimensioning of Internet access lines", Performance Evaluation, Vol. 34, n° 4, pp. 249-271, December 1998

[Net 01] "Netsizer web site", http://www.netsizer.com

[Net 05] "Netflow Services Solutions Guide", http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/-netflsol/

[Nla 01] "AMP web site", http://watt.nlanr.net

[Nor 95] I. Norros, "On the use of fractional Brownian motion motion in the theory of connectionless networks", IEEE Journal on Selected Areas in Communications, Vol. 13, n° 6, pp. 9583-961, August 1995

[Nuz 00] C. J. Nuzman, I. Saniee, W. Sweldens, A. Weiss, "A compound model for TCP connection arrivals", Proc. of ITC Spec. Seminar on IP Traffic Modeling, Measurement and Management, September 2000

[Oli 01] P. Olivier, N. Benameur, "Flow level IP traffic characterization", Proceedings of ITC ’17, December 2001

[Owe95] P. Owezarski, M. Diaz, P. Sénac, "Modélisation et implémentation de mécanismes de synchronisation multimédia dans une application de visioconférence", Actes du colloque francophone sur l'ingénierie des protocoles (CFIP'95), pp 305-319, éditions Hermès, Rennes, France, 10-12 mai 1995

[Owe96a] P. Owezarski, M. Diaz, "Models for enforcing multimedia synchronization in visioconference applications", proceedings of the 3rd MultiMedia Modeling conference – Towards the information superhighway (MMM'96), pp 85-100, World scientific editor, Toulouse, France, November 12-15, 1996

[Owe96b] P. Owezarski, "Conception et formalisation d'une application de visioconférence coopérative. Application et extension pour la téléformation", Thèse de doctorat de l'Université Paul sabatier Toulouse III, Décembre 1996

[Owe98] P. Owezarski, M. Diaz, C. Chassot, "A Time Efficient Architecture for Multimedia Applications", IEEE Journal on Selected Areas in Communications, special issue on Protocols Architectures for 21st Century Applications, vol. 16, n° 3, pp. 383-396, April 1998

[Owe03a] P. Owezarski, N. Larrieu, "Coherent charging of differentiated services in the Internet depending on congestion control aggressiveness", Computer Communications Journal, Vol.26, n° 13, pp.1445-1456, August 2003

[Owe 03b] P. Owezarski, D. Andreu, C. Fricker, K. Salamatian, C. Chekroun, N. Benameur, P. Olivier, J. Roberts, F. Guillemin, "Projet METROPOLIS. Sous-projet 1 : Rapport d'état de l'art", Rapport du projet RNRT METROPOLIS, janvier 2003

[Owe 03c] P. Owezarski, P. Abry, K. Salamatian, D. Kofman, A. Aussem, F. Guillemin, P. Robert, "Métrologie des réseaux de l'Internet", Rapport dinal de l'Action Spécifique du département STIC du CNRS #88, décembre 2003

[Owe 04a] P. Owezarski, N. Larrieu, "A trace based method for realistic simulations", IEEE International Conference on Communications (ICC'2004), Paris, France, June 20th-24th, 2004

[Owe 04b] P. Owezarski, N. Larrieu, "Internet traffic characterization - An analysis of traffic oscillations", 7th IEEE International Conference on High Speed Networks and Multimedia Communications (HSNMC'04), Toulouse (France), June 30 - July 2, 2004

[Owe 05] P. Owezarski, "On the impact of DoS attacks on Internet traffic characteristics and QoS", 14th IEEE International Conference and Computer Communications and Networks (ICCCN'2005), San Diego, CA, USA, 17-19 October 2005

[Owe 06] P. Owezarski, N. Larrieu, L. Bernaille, W. Saddi, F. Guillemin, A. Soule, K. Salamatian, "Distribution of traffic among applications as measured in the French Metropolis project", Annals of telecommunication, 2006

[Par 96] K. Park, G. Kim, M. Crovella, "On the relationship between file sizes, transport protocols, and self-similar network traffic", Proceedings of IEEE ICNP, 1996

[Par 97] K. Park, G. Kim, M. Crovella, "On the Effect of Traffic Self-similarity on Network Performance", SPIE International Conference on Performance and Control of Network Systems, November, 1997

[Par 00] K. Park, W. Willinger, "Self-similar network traffic: an overview", In "Self-similar network traffic and performance evaluation", edited by K. Park and W. Willinger, J. Wiley & Sons, 2000

[Pax 94] V. Paxson, "Growth trends in wide-area TCP connections", IEEE Network, Vol. 8, n° 4, pp. 8-17, July/August 1994

[Pax 94a] V. Paxson, "Empirically derived analytical models of wide-area TCP connections", IEEE/ACM Transactions on Networking, Vol. 2, n° 4, pp. 316-336, August 1994

[Pax 95] V. Paxson, S. Floyd, "Wide area traffic: The failure of Poisson modeling", IEEE/ACM Transactions on Networking, Vol. 3, n0 3, pp. 226-244, June 1995

[Pax 98] V. Paxson, G. Almes, J. Mahdavi, M. Mathis, "Framework for IP Performance Metrics", RFC 2330, May 1998

[Pax 99] V. Paxson, "Bro: a system for detecting network intruders in real-time", Computer Networks Journal, Vol. 31, n° 23-24, pp. 2435-2463, December 1999

[Pax 00] V. Paxson, A. Adams, M. Mathis, "Experiences with NIMI", PAM (Passive and Active Measurements) Workshop, 2000

[Rob 00] J. Roberts, "Engineering for Quality of Service", In "Self-similar network traffic and performance evaluation", edited by K. Park and W. Willinger, J. Wiley & Sons, 2000

[Rob 96] J. Roberts, U. Mocci, J. Virtamo (editors), "Broadband Network Teletraffic (Final report of COST 242) ", LNCS 1155, Springer Verlag, 1996

[Ryu 01] B. Ryu, D. Cheney, H-W Braun, "Internet flow characterization – Adaptive Timeout and statistical modeling", Proceedings of Passive and Active Measurement Workshop, Apr. 2001

[Sal 01] K. Salamatian, S. Fdida, "Measurement based modelling of Quality of Service in the Internet: a methodological approach", IWDC, 2001

[Sch 05] A. Scherrer, P. Abry, "Marginales non gaussiennes et longue mémoire: analyse et synthèse de trafic Internet", Colloque GRETSI-2005, Louvain-la-Neuve, Belgique, Septembre 2005

[Sch 06] A. Scherrer, N. Larrieu, P. Owezarski, P. Borgnat, P. Abry, "Une caractérisation non Gaussienne et à longue mémoire du trafic Internet et de ses anomalies", Workshop sur la Sécurité et les Architectures Réseaux (SAR), Seignosse, France, 6 – 9 mai 2006

[Sha 03] S. Shalunov, "Quality of service and denial of service", ACM SIGCOM workshop on revisiting IP QoS (RIPQoS'2003), Karlsruhe, Germany, August 27th, 2003

[Sim 01] A. Simon, "netMET – Network's METrology : Une solution de métrologie générale pour les réseaux régionaux, métropolitains et de campus", Journées réseaux (JRES'2001), Lyon, France, 10-14 décembre 2001

[Spr 02a] N. Spring, R. Mahajan, D. Wetherall, "Measuring ISP topologies with Rocketfuel", SIGCOMM, 2002

[Spr 02b] N. Spring, R. Mahajan, D. Wetherall, "Rocketfuel maps and data", http://www.cs.washington.edu/research/networking/rocketfuel

[Ste 00] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Scwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, V. Paxson, "Stream Control Transmission Protocol", RFC 2960, octobre 2000

[Ste 03] R. Stewart, M. Ramalho, Q. Xie, M. Tuexen, P. Conrad, "SCTP Partial Reliability Extension", Internet Draft, juin 2003

[Taq 97] M. Taqqu, V. Teverovsky, W. Willinger, "Is network traffic self-similar or multifractal? ", Fractals, Vol. 5, n° 1, pp. 63-73, 1997

[Tho 97] K. Thompson, G. Miller, M. Wilder, "Wide-area internet traffic patterns and characteristics", IEEE Network, Vol. 11, n° 6, pp. 10-23, November/December 1997

[Tra 00] Ph. Tran-Gia, N. Vicari (editors), "Impacts of new services on the architecture and performance of broadband networks (Final report of COST 257) ", Chapter on "Traffic measurement and data analysis", 2000

[Vac 89] H.S. Vaccaro, G.E. Liepins, "Detection of anomalous computer session activity", IEEE symposium on security and privacy, Oakland, California, USA, May, 1989

[Vbn 01] "vBNS web site", http://www.vbns.net

[Vei 99] D. Veitch, P. Abry, "A wavelet based joint estimator of the parameters of long-range dependence", IEEE Transactions on Info. Theory special issue on "Multiscale Statistical Signal Analysis and its Applications", Vol. 45, n° 3, pp. 878-897 April 1999

[Vei 01] D. Veitch, P. Abry, "A statistical test for the time constancy of scaling exponents", IEEE transactions on Signal Processing, Vol. 49, n° 10, pp. 2325-2334, October 2001

[Ver 00] A. Veres, Z. Kenesi, S. Molnar, G. Vattay, "On the propagation of long-range dependence in the Internet", SIGCOMM'2000, Stockholm, Sweden, September 2000

[Ver 00b] A. Veres, M. Boda, "On the Impact of Short Files and Random Losses on Chaotic TCP Systems", in Proceedings of IFIP ATM & IP 2000 Workshop, Ilkley, UK, July 2000

[Wil 96] W. Willinger, M. S. Taqqu, A. Erramilli, "A bibliographical guide to self-similar traffic and performance modeling for modern high-speed networks", In F. P. Kelly, S. Zachary and I. Ziedins, eds., "Stochastic networks: theory and applications", Clarendon Press, Oxford, UK, 1996

[Wil 97] W. Willinger, M. S. Taqqu, R. Sherman, D. V. Wilson, "Self-similarity through high-variability: statistical analysis of Ethernet LAN traffic at the source level", IEEE/ACM Transactions on Networking, Vol. 5, n° 1, pp. 71-86, 1997

[Wil 98] W. Willinger, V. Paxson, M. Taqqu, "Self-Similarity and Heavy Tails: Structural Modeling of Network traffic", In "A Practical Guide To Heavy Tails: Statistical Techniques and Applications", ISBN 0-8176-3951-9, 1998

[Ye 00] N. Ye, "A Markov chain model of temporalbehavior for anomaly detection", Workshop on Information Assurance and Security, West Point, NY, June 2000

[Yua 04] J. Yuan, K. Mills, "DdoS attack detection and wavelets", technical report, National Institute of Standards and Technology, 2004

[Zha 03] Z. Zhang, V. Ribeiro, S. Moon, C. Diot, "Small time scaling behavior of Internet backbone traffic: an empirical study", Infocom'2003