INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Projet ARMOR

Architectures et Modèles de Réseaux

Rennes

THÈME 1B

Table des matières

Armor est un projet commun à l'Inria, au CNRS, *à l'université de Rennes 1 et à l'Ecole Nationale Supérieure de Télécommunications de Bretagne* (ENST *Bretagne). Il a été créé en mai 1999.*

1 Composition de l'équipe

Responsable scientifique

Gerardo Rubino [DR Inria]

Assistante de projet

Fabienne Cuyollaa [TR Inria, en congés à partir du 6/9/1999]

Gwënaelle Multon [vacataire Inria, à partir du 6/9/1999]

Personnel Inria

Bruno Sericola [CR]

Bruno Tuffin [CR]

Personnel de l'université de Rennes 1

Bernard Cousin [professeur]

Louis-Marie Le Ny [maître de conférences]

Raymond Marie [professeur]

Personnel de l'ENST Bretagne

Hossam Afifi [maître de conférences[1]]

Sylvain Gombault [ingénieur d'études]

Laurent Toutain [maître de conférences]

Personnel Insa de Rennes

Miklós Molnár [maître de conférences]

Ingénieurs experts

Maryline Laurent [du 1/06 au 31/12]

1. Hossam Afifi est également collaborateur extérieur du projet Rodéo de l'Unité Inria de Sophia-Antipolis

Chercheurs doctorants

Yasser Ahmed [bourse CIES]
Nelly Barbot [bourse Ama]
Atika Bousseta [convention Cifre, société Sofreten]
Moulaye Hamza [bourse du gouvernement ivoirien]
José Incera [bourse du gouvernement mexicain]
Octavio Medina [bourse du gouvernement mexicain]
Ana Minaburo [bourse du gouvernement mexicain, depuis le 1/10/99]
Samir Mohammed [bourse du gouvernement egyptien, depuis le 1/10/1999]
Ahmed Mokhtar [bourse Cnet]
Nathalie Omnès [bourse Cnet]
Ollivier Paul [bourse DGA]
Landy Rabehasaina [bourse Inria, depuis le 1/9/1999]
David Ros [bourse CIES]
Miled Tezeghdanti [bourse Inria et Région Bretagne, depuis le 1/10/1999]

Collaborateurs extérieurs

Haïsçam Abdallah [maître de conférences, université de Rennes 2]

2 Présentation et objectifs généraux

Résumé :

L'objectif central du projet Armor est l'identification, la conception ou la sélection des architectures les plus appropriées pour la mise en place d'un service de communication, et le développement d'outils (informatiques, mathématiques) pour la réalisation de ces tâches. Cet objectif est abordé sous deux angles complémentaires : premièrement, nous nous intéressons aux aspects qualitatifs des systèmes de communication, c'est-à-dire aux mécanismes nécessaires pour fournir le type de service spécifié. Il s'agit typiquement de conception d'architectures, de protocoles, de procédures de contrôle. Deuxièmement, nous considérons les aspects quantitatifs, indispensables pour dimensionner correctement ces architectures et ces services. Il s'agit de l'analyse de systèmes de télécommunication du point de vue des performances, de la sûreté de fonctionnement, de la qualité de service, de la vulnérabilité, de la performabilité. Observons que les aspects purement quantitatifs se trouvent au cœur même des changements technologiques, donc, des aspects qualitatifs ; dans un sens, ils sont la raison d'être de ces derniers : fournir plus de services, de meilleures performances, une plus grande sûreté de fonctionnement, et bien entendu réduire les coûts.

Le projet s'intéresse aux problèmes posés, d'une manière générale, par la conception d'une architecture au sens large, destinée à mettre en place un service de communication. Un tel

service nécessite à la fois de définir un certain nombre de fonctionnalités, de décider de l'endroit où celles-ci doivent se placer dans l'architecture et de dimensionner certains éléments du système. En ce qui concerne les réseaux proprement dits, nous nous intéressons essentiellement aux problèmes liés à Internet et aux protocoles IP et TCP. Ceci dit, nous travaillons également sur des technologies de transport à haut débit et, en particulier, sur le réseau de transport ATM. Nos pôles d'intérêt sont centrés autour des mécanismes de contrôle qui permettent de fournir les services dans les conditions requises, tout en garantissant une utilisation efficace des ressources. Nous considérons différents aspects de la structure des architectures, des problèmes d'organisation topologique des liaisons jusqu'à l'étude des techniques nécessaires pour faire cohabiter des protocoles conçus au départ pour des environnements différents, comme TCP et ATM, ou, dans le cadre du réseau Internet, pour assurer une transition « douce » de IPv4 vers IPv6. Nous étudions également certains aspects des réseaux liés à la nature des supports (par exemple, aux relations entre les performances et l'utilisation de lignes de communication asymétriques). Enfin, nous travaillons sur des applications particulièrement importantes aujourd'hui, comme celle de la téléphonie sur un réseau IP.

Outre les aspects de nature qualitative, ces tâches demandent des capacités d'analyse et d'évaluation quantitative. Le projet organise une partie importante de ses travaux de recherche dans cette direction. Il s'agit des technologies d'évaluation de *modèles*, depuis les techniques classiques comme la simulation à événements discrets jusqu'à celles plus récentes comme l'utilisation de modèles dits *fluides*, c'est-à-dire à variables d'état continues. Nous développons ces travaux sur plusieurs axes. D'une part, nous nous intéressons à la simulation événementielle et aux spécificités imposées dans ce contexte par les systèmes de communication, avec une attention particulière pour le haut débit. D'autre part, nous menons des travaux sur les techniques d'analyse mathématique des modèles, soit exactes, soit approchées. Ces dernières ont pour principal *raison d'être* le coût important en calcul souvent associé aux premières. Ceci dit, elles peuvent également être nécessaires pour cerner un aspect précis d'un système, qui n'est pas facilement identifiable par une analyse exacte. Par exemple, le fait de passer à une approximation du problème peut permettre de traiter formellement des expressions qui ne pourraient être manipulées que numériquement. Dans le cadre des méthodes dites approchées, nous explorons deux directions de recherche : nous étudions les techniques de Monte Carlo permettant d'évaluer une large classe de systèmes, et nous faisons des recherches sur des méthodes de type numérique pour faire face au problème fréquent de l'explosion combinatoire des espaces d'état.

La méthodologie employée pour remplir nos objectifs se veut un équilibre mesuré entre analyse et expérimentation, entre traitement conceptuel à partir de modèles et mise en oeuvre de prototypes pour explorer, valider ou consolider une approche donnée. D'une part nous nous intéressons aux concepts qui sont à la base des développements actuels majeurs ainsi qu'aux aspects méthodologiques. D'autre part, nous travaillons sur les problèmes posés par des systèmes spécifiques en opération, activité qui va depuis la veille technologique jusqu'à l'étude de réseaux existants. Nous tirons profit pour cela de la diversité des origines des membres de ce projet, dont les activités vont de la mise en place de plates-formes expérimentales qui permettent de tester et valider des choix architecturaux, jusqu'à l'étude mathématique de modèles pour analyser un mécanisme ou un algorithme (ou encore, jusqu'au développement de nouvelles méthodes d'analyse).

3 Fondements scientifiques

Résumé :

Les fondements scientifiques de nos travaux sont ceux de la conception de réseaux d'une part, et de leur analyse quantitative d'autre part. Ceci concerne, d'abord, les principes scientifiques sur lesquels reposent les principaux réseaux de communication, et en particulier les réseaux basés sur le protocole IP. *Nous trouvons ensuite des théories mathématiques et des méthodes algorithmiques, numériques et non numériques, sur lesquelles s'appuient les outils d'analyse que nous développons. Ces fondements sont brièvement décrits dans la suite.*

Mots clés : allocation de ressources, ATM, contrôle de congestion, contrôle de flux, contrôle de trafic, CoS (classe de service), différenciation de service, dimensionnement, disponibilité, fiabilité, files d'attente, IP, modèle à événements discrets, modèle fluides, multicast, multimédia, performabilité, performances, processus de Markov, processus stochastiques, protocoles, QoS (qualité de service), réseaux haut débit, réseaux maillés, réseaux, sécurité, simulation, sûreté de fonctionnement, TCP, techniques de Monte Carlo, UDP.

3.1 Historique

La conception de protocoles et de services dans les réseaux connaît depuis quelques années un fort regain d'intérêt. Les protocoles utilisés actuellement (TCP/IP, X25,...) ont tous été conçus dans les années 70 avec trois hypothèses majeures : un taux d'erreur élevé sur les voies physiques, une durée de traitement par les entités protocolaires plutôt courte par rapport à la durée d'émission et un coût de transmission élevé. Depuis les années 80, avec entre autre la généralisation des réseaux locaux, le développement des fibres optiques et la conception de nouvelles techniques de codage, les hypothèses de base ont été complètement modifiées (à l'exception du domaine des réseaux sans fil). Le taux d'erreur sur les voies physiques est devenu extrêmement faible et les débits élevés (de 10 Mbit/s à plusieurs Gbit/s). La durée de traitement par les entités protocolaires qui n'a pas été réduite dans les mêmes proportions est devenue importante par rapport au délai d'émission. Les ressources en bande passante augmentent plus rapidement que prévu. Du point de vue des performances, les implications immédiates de ces changements sont essentiellement les suivantes :

- les éléments de commutation (routeurs, commutateurs,...) sont devenus les goulots d'étranglement du réseau du fait du traitement trop long de chaque entité d'information par rapport aux temps d'émission ;
- le coût de traitement des entités protocolaires sur les stations de travail réduit considérablement le débit que les applications seraient en droit d'espérer grâce aux capacités du support physique.

Les conséquences pour les réseaux sont :

- l'explosion du nombre d'entités connectées (ou d'abonnés) ; en particulier, dans le cas d'Internet, cela entraîne un énorme besoin d'adresses, qui deviendra critique dans peu

d'années, et introduit des besoins spécifiques comme celui d'un adressage universel, indépendant de la localisation ;

- l'accroissement du trafic inter-réseaux locaux correspondant à la généralisation dans les applications du modèle client-serveur (en même temps, ce trafic est en train de changer de nature ; c'est la conséquence de la généralisation des applications audio et vidéo, et plus généralement des applications multimédia) ;
- la demande accrue de performance ou plus généralement de qualité de service, en partie due aux exigences associées avec les nouveaux types de trafic évoqués plus haut ;
- le passage, dans certains types de réseaux (typiquement, dans les réseaux d'interconnexion), de la réservation des ressources à l'utilisation de priorités, voire au gaspillage de bande passante étant donnée l'évolution du coût de la transmission.

3.2 Qualité de service

Il est difficile de concevoir aujourd'hui une solution dédiée à chaque besoin applicatif. On vise donc à fournir un *service* banalisé, qui doit pouvoir mettre à la disposition de chaque application des propriétés appelées collectivement « qualité de service » (QoS). Ce service doit donc être générique, mais en même temps adaptatif, car les propriétés de QoS pourront être très différentes d'une application à une autre. D'une certaine façon, le concept de QoS est un fil conducteur dans l'organisation de nos activités de recherche. Nos travaux visent à trouver des moyens pour l'obtenir et à développer des techniques pour l'évaluer. Dans tous les cas, nos efforts sont dédiés à mieux la comprendre. Le but ultime est toujours de donner aux utilisateurs ou aux applications une certaine QoS, c'est-à-dire un service de communication respectant des contraintes numériquement établies au travers d'indicateurs appropriés, en maximisant certaines fonctions et en optimisant l'utilisation des ressources du réseau.

La QoS n'est pas un concept formellement défini. Elle recouvre un ensemble de concepts concernant par exemple le temps de réponse (durée d'émission, délai d'acheminement, gigue,...), le débit (moyen, crête, minimal,...), le taux d'utilisation, les taux de perte et d'erreur, etc. Elle se combine également avec la sûreté de fonctionnement (la fiabilité, la disponibilité sous ses diverses formes –ponctuelle, asymptotique, sur un intervalle,...–, la sécurité,...), ou encore l'évolutivité et l'extensibilité des systèmes. Ces critères sont inégalement importants selon le domaine applicatif, et sont souvent contradictoires (dans le sens où ils ne peuvent pas être raisonnablement satisfaits tous à la fois, conduisant à la recherche de compromis). L'étude de la QoS peut être vue comme un problème multidimensionnel donnant lieu à des problèmes d'optimisation multicritères, dont on sait la solution difficile et très coûteuse. De plus, certains des paramètres de QoS ont une dimension psychosensorielle (qualité des images, certains aspects des temps de réponse,...) difficile à cerner formellement. C'est le cas typiquement de la qualité de restitution d'un document vidéo pour lequel il n'y a pas de mesure formelle efficace.

La QoS peut bien sûr être vue sous deux angles distincts selon que l'on s'y intéresse du point de vue de l'utilisateur (de l'application finale) ou du point de vue d'une entité composant l'architecture du système supportant l'application (le composant majeur étant pour nous celui qui rend le service considéré). Ceci est tout-à-fait classique en évaluation de performances. Ces deux points de vue conduisent à l'étude de paramètres spécifiques et parfois à la résolution de problèmes assez différents.

La QoS peut concerner deux situations bien différentes, selon qu'il s'agisse d'une architecture en boucle ouverte ou en boucle fermée. Dans le premier cas, il n'y a pas de *retour* d'information issue des autres composants de l'architecture ; c'est en général une approche de type préventif qui est adoptée au niveau de la QoS, par exemple lorsqu'on cherche à éviter a priori les congestions et les pertes ; le contexte principal où on la rencontre est celui des applications ayant de fortes contraintes d'interactivité (comme dans le temps-réel) et de certaines situations ne tolérant aucune dégradation. En boucle fermée, l'environnement (éventuellement de bout en bout) restitue un signal qui permet d'adapter le comportement du composant aux besoins de l'application ou, réciproquement, d'asservir l'application aux contraintes posées par les composants utilisés. Cette approche est du type réactif, où l'on agit sur la source, de manière adaptative, pour la contraindre par exemple à diminuer son débit en cas de problème ; le contexte usuel où l'on rencontre ce comportement est celui des applications de transmissions de données, qui n'ont pas, en général, à respecter des contraintes temporelles fortes. Signalons que le délai introduit par les mécanismes de rétrocontrôle (*feedback*) n'est pas favorable au haut débit.

On peut se demander à quel niveau doivent se situer les différentes fonctions d'un système de communication, pour satisfaire les demandes en QoS tout en optimisant l'utilisation des ressources disponibles. Dans la mesure où certains services doivent être fournis en respectant des contraintes, on peut classer très schématiquement les multiples approches en deux classes : d'une part nous avons celles qui traitent le réseau comme une boîte noire et qui portent tout l'effort au niveau des applications ; d'autre part, nous avons celles qui cherchent à modifier le réseau lui-même, pour améliorer l'utilisation faite de ses ressources, voire pour rendre possible un service autrement difficile à satisfaire. Le cadre de nos études se situe dans ce dernier cas, pour une raison essentiellement économique : comme nous l'avons dit plus haut, un réseau est un système complexe difficile à contrôler de façon globale. Par exemple, nous pensons qu'il est difficile de maîtriser complètement le comportement des sources. Il s'agit dans un certain sens d'un problème quantitatif : s'il est concevable de contrôler individuellement une source particulière, il est beaucoup plus difficile de le faire pour tout un ensemble, ou bien cela impose trop de restrictions. Nous concentrons donc nos efforts sur le contrôle réalisé à l'intérieur du réseau, où en particulier on dispose d'informations plus précises pour agir.

3.3 Contrôle dans les réseaux

Pour satisfaire les besoins croissants des applications tout en assurant une utilisation efficace des ressources disponibles, les réseaux doivent être *contrôlés* de façon appropriée. Le contrôle peut prendre diverses formes et agir à différents niveaux. Les diverses formes de contrôle n'utilisent pas toutes le même type d'information pour agir et elles ne travaillent pas toutes à une même échelle de temps. Enfin, les différents types de contrôle ne se trouvent pas systématiquement dans tous les réseaux : leur usage est souvent spécifique au mode de transport de l'information.

Tout d'abord, nous avons le *contrôle d'admission*, dont le rôle est d'accepter ou de refuser les connexions, dans le cas de services fonctionnant en mode connecté (un réseau fonctionnant en mode non connecté accepte en principe tout le trafic offert et essaye de partager ses ressources équitablement). Cette décision dépend des caractéristiques des connexions en cours et

de l'état du réseau. Plus spécifiquement, les dispositifs de contrôle basent leur décision sur des informations de nature statistique censées caractériser le réseau et la source pendant la durée de la nouvelle communication (on ne réalise pas cette tâche en fonction d'un état instantané du système). L'une des difficultés principales pour mettre en place ce type de contrôle provient du fait que l'effet de la décision est irréversible, et que l'on doit tenir compte, par exemple, d'éventuelles augmentations postérieures du trafic rentrant en concurrence avec celui de la communication que l'on vient d'accepter.

Le réseau gère ou contrôle ensuite son fonctionnement au niveau du *routage*, en sélectionnant le chemin que les informations vont suivre. Cette gestion est faite en fonction de critères divers et en tenant compte de l'état global du système ; comme nous allons le voir, le mode de connexion affecte aussi l'algorithme de routage. Le routage peut être statique ou dynamique. Les routes statiques sont figées dans le système et changées manuellement ou très lentement. Dans le cas d'utilisation d'algorithmes qui évaluent les routes entre deux sites de manière permanente, le routage est dit dynamique. Pour les réseaux fonctionnant en mode non connecté tel que les réseaux IP, le routage dynamique peut affecter la route de chaque paquet transmis. Deux paquets consécutifs peuvent ne pas suivre le même chemin à cause d'un changement dans les tables (et arriver à la destination dans l'ordre inverse à celui de leur émission). Dans le cas des réseaux qui fonctionnent en mode connecté, il est rare (sauf certains cas de téléphonie où un re-routage est effectué) que les circuits soient modifiés durant leur vie. Ceci n'empêche pas d'avoir un algorithme de routage dynamique dans ces réseaux. Lorsque cette décision de modifier le routage est prise pour éviter des parties saturées du réseau (typiquement dans le cas de la commutation de paquets), on parle de *contrôle de congestion*. On parle aussi de contrôle de congestion à propos de mécanismes utilisés pour restreindre l'accès à une ressource surchargée, à l'intérieur du réseau. Ce type de contrôle peut être vu comme l'un des aspects de l'administration des réseaux, concept bien entendu beaucoup plus général.

Les réseaux fonctionnant en mode datagramme ou par circuits virtuels, peuvent décider de limiter le nombre d'unités d'information envoyées à chaque instant pour éviter la formation de points de congestion. On parle alors de *contrôle du flux*. Signalons que ces décisions sont prises en général en temps-réel, en tenant compte d'indicateurs d'état instantané. Le premier exemple de ce type de mécanisme est le contrôle par *fenêtre coulissante*, soit au niveau d'un lien, soit de bout en bout. Une technique proche et particulièrement importante dans le cadre des réseaux ATM, est le *traffic shaping*, où l'on cherche à modifier certaines caractéristiques du trafic sortant d'une source pour qu'il rentre dans le réseau en vérifiant des propriétés données. Il ne faut pas confondre contrôle de flux et contrôle de congestion. Le premier est plus général, et on peut dire qu'entre autre, il est mis en place par exemple pour assurer le second. Le second a pour objectif de s'assurer que le réseau peut transporter, selon les spécifications, le traffic qui lui est offert. Le contrôle du flux est toujours lié à une source et un récepteur. On peut classifier les techniques de contrôle de flux en techniques en boucle ouverte et en boucle fermée. Le *traffic shaping* est un exemple de technique utilisée en boucle ouverte et les fenêtres coulissantes sont le mécanisme de contrôle principal en boucle fermée. Il faut souligner que lorsqu'on parle de contrôle de flux en boucle ouverte, on doit aussi intégrer les techniques de contrôle d'admission dont on a déjà parlé.

Enfin, nous avons le problème du partage de la capacité d'un nœud. Celui-ci doit décider de la fraction de la bande passante et des ressources de stockage qui doivent être allouées. On parle

alors d'*allocation de ressources*. Cette allocation peut être statique et rester fixe pendant toute la communication, ou variable, et s'adapter ainsi à l'évolution de l'état du système. Dans ce dernier cas il s'agit aussi de décisions temps-réel, comme pour le contrôle de flux. Le problème est en général associé à la transmission en mode connecté mais pas exclusivement (cf. RSVP dans le cadre des évolutions prévues du réseau Internet).

Observons que des problèmes spécifiques peuvent apparaître lorsque l'on connecte des réseaux de natures différentes, par exemple, fonctionnant dans des modes distincts. Un exemple est celui posé par le routage de paquets IP sur un réseau de transport ATM, c'est-à-dire, un réseau travaillant en mode datagramme utilisant les services d'un système de transport fonctionnant en mode connecté (par circuits virtuels). En particulier, il faut qu'au niveau des utilisateurs, des mesures de Qualité de Service (QoS, voir plus loin) respectent certaines contraintes, ce qui conduit à des mécanismes de contrôle qui doivent être relativement sophistiqués pour tenir compte de cette hétérogénéité.

3.4 L'Internet

L'une des caractéristiques de l'Internet est l'absence d'état global dans le réseau ; sa principale implication est le fonctionnement en mode datagramme. Pour chaque information élémentaire (paquet), la décision de routage est prise localement et indépendamment des autres informations. Grâce à la gestion du réseau ce comportement simple n'est pas synonyme d'anarchie. Ainsi, par exemple, le déséquencement de paquets qui est un problème inhérent au fonctionnement en mode datagramme, est en pratique relativement rare pour un flux donné. Une autre incidence de cette absence d'état global est le paradigme de bout-en-bout selon lequel le contrôle est reporté aux extrémités du réseau. Un exemple en est le contrôle de flux et d'erreur du protocole TCP. Le contrôle de flux de TCP est un mécanisme essentiel à la bonne marche du réseau, en particulier celui de TCP qui représente une bonne part du trafic sur l'Internet. Il permet d'adapter le rythme d'émission des données au rythme de consommation de celles-ci par le destinataire et d'éviter une saturation des équipements intermédiaires. L'émetteur n'a pas la connaissance ni du chemin pris par les paquets, ni de la capacité des liens, ni de leur taux d'occupation instantané. Pour estimer le débit et optimiser la connexion sans nuire au réseau, l'émetteur se base sur le taux de perte observé sur ces paquets, c'est-à-dire sur les informations contenues dans les acquittements.

Les mécanismes de contrôle de flux mis en place dans l'Internet se sont avérés résistants au facteur d'échelle, et ils ont permis de construire le grand réseau que l'on connaît actuellement. Cependant, l'influence de ces mécanismes sur le comportement global du réseau sont mal compris. En particulier, il est difficile de déterminer la frontière précise à partir de laquelle une amélioration des performances d'un (type de) flux nuit au fonctionnement global du réseau. Pourtant, la connaissance du comportement global de TCP est nécessaire pour pouvoir améliorer la qualité de service. L'approche analytique fournie des modèles relativement grossiers et ne permet pas d'appréhender finement le comportement d'un flux. La simulation permet une étude plus fine mais n'autorise qu'un nombre limité de connexions simultanées inférieur de plusieurs facteurs à ce que l'on rencontre dans les réseaux d'opérateurs. Le paradigme de bout-en-bout est en train d'évoluer vers un contrôle possible aux frontières entre deux domaines (entre un site et son fournisseur d'accès ou entre fournisseurs d'accès, la notion de domaine ou

de système autonome étant définie initialement pour le routage). Cette tendance a été mise en oeuvre dans un premier temps pour augmenter la sécurité des sites avec le contrôle d'accès à l'aide de routeurs filtrants et les architectures firewall. Avec des protocoles comme Cops, il est même possible d'associer un flux à un utilisateur, dans le but de contrôler ou de facturer l'utilisation des ressources. Le contrôle aux frontières de domaine est en train de se développer avec l'introduction de la différenciation de service dans le réseau. La différenciation de service permet au routeur de traiter différemment les paquets. Les paquets dont le traitement doit être différencié du Best-Effort sont marqués comme appartenant à une certaine classe de service. Le fournisseur vérifie la conformité de ce marquage avec un contrat passé au préalable. Si ce contrat n'est pas respecté, les paquets peuvent être détruits, retardés pour être mis en conformité avec le contrat ou voir leur priorité baissée pour être rejetés plus facilement en cas de congestion. Ces différents traitements sont sélectionnés en fonction de la classe de service spécifique.

Cette absence d'état global n'empêche pas la mise en place d'états locaux pour optimiser le fonctionnement d'un équipement. Par exemple, des caches mis en place dans les routeurs permettent d'optimiser le relayage des trames une fois qu'un flux a été identifié. Mais cet état peut être étendu à l'ensemble d'un domaine. Ainsi le protocole MPLS permet de mieux gérer les flux à l'intérieur d'un réseau d'opérateur. Une étiquette est ajoutée au paquet à l'entrée dans le réseau. Cette étiquette peut être associée à un identificateur de voie logique pour les réseaux ATM ou Frame Relay. L'opérateur peut gérer un agrégat de flux correspondant par exemple au trafic d'un Réseau Privé Virtuel. Ce type de mécanisme est l'objet d'intenses recherches à l'heure actuelle, recherches auxquelles notre groupe participe.

3.5 Les techniques d'évaluation par analyse de modèles

Rappelons d'abord les différents types d'approches que l'on peut suivre pour l'évaluation d'un modèle. La situation idéale est celle où le modèle est suffisamment simple ou suffisamment « régulier » pour permettre un traitement analytique. À l'opposé, lorsqu'il représente un système avec beaucoup de détails, conséquence de la complexité de ce système, il peut être trop difficile de mettre en évidence des relations explicites, et ainsi conduire à une étude par simulation. À mi-chemin entre les deux, on peut envisager une résolution numérique, qui n'apporte pas autant de connaissances sur le système que le traitement analytique, mais qui a sur la simulation l'avantage d'apporter des solutions (numériquement) exactes, et parfois représenter un coût de calcul moins important. Enfin, il est souvent possible d'approcher les résultats cherchés (soit dans une analyse mathématique, soit dans une étude numérique), avec des compromis acceptables entre la qualité du résultat et le coût nécessaire pour l'obtenir.

Dans les vingt dernières années, on a vu se développer considérablement l'ensemble des techniques mathématiques et algorithmiques de résolution de problèmes de base. Le fait que les techniques d'évaluation aient connu des progrès significatifs joint à l'augmentation considérable de la capacité de calcul des machines, font que l'on peut traiter aujourd'hui des problèmes de plus en plus complexes, avec des tailles des données de plus en plus importantes. L'une des conséquences de ceci est que la construction même des modèles, de façon fiable et efficace, n'est plus un problème secondaire mais est devenu un problème central. En outre, d'autres problèmes apparaissent, aussi bien dans le monde des techniques numériques que dans les méthodes de

simulation. Du point de vue des premières, la résolution numérique de systèmes d'équations de grande taille (millions ou milliards d'équations et d'inconnues, voire une infinité) n'est pas une tâche aisée. En ce qui concerne la simulation, la prise en charge de la rareté de certains événements (la défaillance d'un système ou la perte d'une cellule dans un commutateur ATM) est un problème non trivial.

Parallèlement, les transformations technologiques dans le monde des communications ont apporté de nombreux problèmes nouveaux, à plusieurs niveaux. D'abord, les mesures usuelles de performance et de sûreté de fonctionnement, traditionnellement utilisées en informatique, ne sont plus suffisantes pour cerner un certain nombre d'aspects de ces systèmes. On parle maintenant de *performabilité* et, comme on l'a vu plus haut, de QoS. Ensuite, des approches nouvelles voient le jour : on commence à s'intéresser de plus en plus à des techniques déterministes et à l'analyse des cas les pires (*worst case analysis*), on travaille à des échelles de temps qui étaient auparavant inhabituelles, ce qui conduit à travailler dans des formalismes de modélisation nouveaux comme les modèles *fluides* (voir ci-après), on introduit des concepts nouveaux comme celui de *bande passante équivalente* qui à leur tour amènent des classes de problèmes spécifiques. Enfin, des domaines jusqu'à présent sans grand intérêt pour la communauté scientifique comme celui des procédures de facturation des services réseaux font maintenant l'objet de recherches intenses de nature mathématique, conséquence du fait qu'un meilleur contrôle des réseaux de communication peut être obtenu via des mécanismes de tarification sophistiqués.

Signalons que même au niveau de la simulation de type événementielle, il y a d'important problèmes de recherche à résoudre. Un exemple de référence est celui de la simulation d'un réseau ATM au niveau cellule. Une représentation à ce niveau implique un très grand nombre d'événements pour simuler de très courtes périodes de temps. Par exemple, la simulation d'une activité durant 3 secondes sur un lien à 155 Mbit/s nécessite le traitement d'environ 10^6 événements. Si l'utilisateur veut valider des taux de perte inférieurs à 10^{-9}, ce type de simulateur doit faire face au problème de l'obtention d'estimations précises pour des probabilités d'événements très rares.

Regardons maintenant de plus près certains problèmes nouveaux posés par l'évaluation des performances et plus généralement de la QoS, dans le cadre des réseaux haut débit. Les premières difficultés liées à ces problèmes d'évaluation concernent la modélisation du trafic et du processus des arrivées aux différents nœuds d'un réseau de communication. On distingue généralement trois échelles de temps différentes pour la modélisation du trafic, qui sont l'échelle des cellules (nous empruntons la terminologie à celle de la technologie ATM), l'échelle des rafales et l'échelle des appels.

- À l'échelle de temps des cellules, le trafic consiste en des entités discrètes, les cellules, produites par chaque source à un taux qui est souvent plus faible de quelques ordres de grandeur que le taux maximal des liens de sortie des nœuds.
- À l'échelle de temps des rafales, la granularité fine de l'échelle cellules est ignorée et le processus d'entrée est caractérisé par son taux instantané. Les modèles fluides apparaissent alors comme un outil de modélisation naturel.
- L'échelle des appels, caractérisée par les temps de séjour des appels arrivant ou par leurs demandes de service, représente la plus grande des trois échelles de temps décrites.

Celle-ci est l'échelle de temps classique dans les études de performance (par exemple, dans les études liées aux architectures en informatique). Aujourd'hui, les caractéristiques des réseaux de communication posent des problèmes nouveaux, même à cette échelle. À titre d'exemple, on peut associer à chaque appel un réel appelé *bande passante effective*, compris entre le débit moyen et le débit crête requis et qui décrit la quantité de bande passante qui doit être allouée à cet appel de manière à conserver la probabilité de perte de cellules en dessous d'un certain seuil.

Les échelles de trafic auxquelles nous nous intéressons plus particulièrement, pour le moment, sont l'échelle des cellules et l'échelle des rafales. En effet, il s'agit des domaines où les problèmes nouveaux à résoudre sont les plus novateurs et difficiles. Lorsqu'elle est pertinente, l'échelle des appels dispose d'un très grand nombre d'outils d'analyse éprouvés.

L'échelle des cellules. À cette échelle, le trafic consiste en des entités discrètes, les cellules, produites par chaque source. Les processus d'arrivée généralement utilisés dans ce contexte pour modéliser le trafic sont des processus d'arrivée par groupes markoviens, aussi notés BMAP (*Batch Markovian Arrival Process*).

Un BMAP est un processus de Markov bidimensionnel $\{A(t),J(t)\}$ où la variable $A(t)$ compte le nombre d'arrivées sur l'intervalle $(0,t)$ et où la variable $J(t)$ représente la *phase* du processus. Le nombre de phases du processus est en général fini. Le générateur infinitésimal du processus est donné par la matrice

$$\begin{bmatrix} D_0 & D_1 & D_2 & D_3 & . & . & . \\ & D_0 & D_1 & D_2 & . & . & . \\ & & D_0 & D_1 & . & . & . \\ & & & D_0 & . & . & . \\ & & & & . & . & . \end{bmatrix}$$

où les D_k, $k \geq 0$, sont des matrices carrées de dimension égale au nombre de phases du processus. Pour $k \geq 1$, les matrices D_k contiennent les taux de transition concernant les arrivées de taille k, avec le changement de phase approprié. La matrice D_0 contient, en dehors de sa diagonale, les taux de transition correspondant à un changement de phase sans arrivée de cellules. La matrice $D = \sum_{k=0}^{\infty} D_k$ est le générateur infinitésimal du processus de Markov $\{J(t)\}$. Le taux moyen d'arrivée en équilibre λ du processus $\{A(t),J(t)\}$ est

$$\lambda = \pi \sum_{k=1}^{\infty} k D_k \mathbb{1},$$

où π est le vecteur ligne des probabilités stationnaires du processus $\{J(t)\}$ et $\mathbb{1}$ est le vecteur colonne dont toutes les composantes valent 1.

Les BMAP forment une classe très large. De nombreux processus d'arrivée familiers peuvent être vus comme des BMAP particuliers. Notamment, en prenant $D_0 = -\lambda$, $D_1 = \lambda$ et $D_k = 0$ pour $k \geq 2$, on obtient un processus de Poisson de taux λ. Un processus de renouvellement de type phase, de représentation (α,T) est un BMAP avec $D_0 = T$, $D_1 = -T\mathbb{1}\alpha$ et $D_k = 0$ pour $k \geq 2$. Si D_1 est diagonale, et $D_k = 0$ pour $k \geq 2$, on obtient un processus de Poisson dont le taux est modulé par un processus de Markov de générateur infinitésimal $D = D_0 + D_1$.

Ce dernier cas particulier de BMAP est aussi appelé un MMPP (Markov Modulated Poisson Process). De plus, tout processus ponctuel peut être approché par un BMAP. Enfin, il est à noter que la superposition de n processus BMAP indépendants est encore un processus BMAP. Cette propriété est particulièrement intéressante pour la modélisation du multiplexage statistique de sources dans les réseaux haut débit.

À l'aide de ces processus BMAP, on peut par exemple modéliser le comportement d'un nœud d'un réseau de communication par une file d'attente BMAP/G/1 à capacité finie ou infinie dans le but d'évaluer des mesures de qualité de service comme la loi du nombre de clients en attente, la loi du temps d'attente ou la probabilité de perte de cellules dans le cas d'une capacité finie. Un tutoriel portant sur l'étude de cette file d'attente se trouve dans [Luc93]. Dans le cas d'une modélisation avec une échelle de temps discrète, on obtient de manière similaire au cas du temps continu, des processus d'arrivée, notés D-BMAP qui conduisent à l'étude de files d'attente discrètes du type D-BMAP/D/1. La fine granularité de l'échelle de temps des cellules pose le problème du grand nombre de paramètres à évaluer pour définir le processus des arrivées, et l'une des principales difficultés rencontrée lors de l'étude des files d'attente associées concerne le temps de calcul des mesures recherchées. En effet, les processus BMAP ou D-BMAP sont définis par un certain nombre de matrices dont la taille pose bien évidemment les problèmes classiques au niveau de la complexité des calculs.

L'échelle des rafales. A l'échelle de temps des rafales, le trafic est considéré comme continu, c'est pourquoi on parle de modèles fluides, et ce trafic est en général caractérisé par son taux instantané. Les plus connus de ces modèles sont les processus dits *on/off* et leurs superpositions. On dit que le trafic provenant d'une source est *on/off* s'il alterne entre des périodes d'activité (les périodes *on*) et des périodes de silence (les périodes *off*). Les taux de transmission sont supposés constants durant chaque période *on*. L'hypothèse de base est que ces processus sont des processus de renouvellements alternés. L'état de la source est alors décrit par un processus semi-markovien. Lorsque ces périodes suivent des lois de type phase, le processus devient markovien et le taux d'entrée devient modulé par un processus de Markov.

En régime transitoire, on considère un buffer de taille finie ou infinie dont les taux d'entrée et de sortie sont fonctions de l'état d'un processus de Markov $\{X_s, s \geq 0\}$ sur un espace d'états S, avec générateur infinitésimal A. Si Q_t désigne la quantité de fluide dans le buffer à l'instant t et si ϱ_i (resp. c_i) désigne le taux d'entrée (resp. de sortie) dans le (resp. du) buffer lorsque le processus $\{X_s\}$ est dans l'état i, alors le couple (X_t, Q_t) forme un processus de Markov. La loi du couple (X_t, Q_t) est donnée par l'équation aux dérivées partielles

$$\frac{\partial F_i(t,x)}{\partial t} = -\eta_i \frac{\partial F_i(t,x)}{\partial x} + \sum_{r \in S} F_r(t,x) A(r,i), \tag{1}$$

où $\eta_i = \varrho_i - c_i$ et où l'on a posé $F_i(t,x) = \Pr\{X_t = i, Q_t \leq x\}$. La mesure qui nous intéresse dans ce contexte est la loi du processus d'occupation Q_t du buffer.

[Luc93] D. M. LUCANTONI, « The BMAP/G/1 queue: A tutorial », *in: Performance Evaluation of Computer and Communications Systems*, L. Donatiello, R. Nelson (éditeurs), Lectures Notes in Computer Science 729, Springer Verlag, p. 330–358, 1993.

Si maintenant X représente l'état stationnaire du processus $\{X_s\}$ et si Q représente la quantité de fluide dans le buffer en régime stationnaire, alors sous les hypothèses classiques de stabilité, on a l'équation différentielle suivante :

$$\eta_j \frac{dF_j(x)}{dx} = \sum_{i \in S} F_i(x) A(i,j),$$

où $F_j(x) = \Pr\{X = j, Q \leq x\}$. Ces travaux concernent non seulement le calcul de la loi de Q [AMS82], mais aussi l'obtention de bornes [LNT97] de cette loi ou d'équivalents de la queue de sa distribution dans le but de contrôler l'admission de nouvelles sources par le respect de critères de qualité de service [EM93].

4 Domaines d'applications

Mots clés : Extranet, ingénierie des réseaux, Internet, Intranet, multimédia, opérateurs, QoS, télécommunications, téléphonie.

Résumé : *Nos domaines d'application principaux sont ceux de la conception de réseaux, aussi bien au niveau de l'infrastructure de transport de l'information qu'à celui des protocoles utilisés dans les différentes couches du réseau. Notre expertise se focalise aujourd'hui sur la technologie* IP *dans divers contextes (*IP *et* QoS*,* IP *et sécurité,* IP *et mobilité,* IP *et téléphonie,...), et sur les outils d'analyse et dimensionnement : configuration d'architectures de télécommunication, recherche des goulots d'étranglement, comparaison des politiques d'allocation des ressources du réseau, etc. Nos travaux sur les protocoles et sur les mécanismes de contrôle trouvent également des applications avec des technologies autres que* IP*, par exemple, dans le cas des supports de transport* ATM*. Les problèmes de cohabitation de technologies distinctes sont aussi sources de nombreuses applications :* IP *et* ATM*,* IP *et* WDM*,* IP*v4 et* IP*v6, etc. Dans le domaine de l'ingénierie du trafic et le dimensionnement des systèmes, l'évolution technologique pose de très nombreux nouveaux problèmes d'analyse de performances, avec des extensions dans d'autres domaines. Citons par exemple tout ce qui concerne l'analyse des méthodes de contrôle, sujet central dans la recherche sur les réseaux, ou les problèmes posés par la tarification, qui intéressent pour des raisons évidentes les opérateurs.*

Le premier domaine dans lequel l'expertise du projet est sollicitée est celui du monde des réseaux IP. Le contexte usuel est celui des industriels désirant développer de nouvelles techniques de contrôle, à différents niveaux, ou celui d'un utilisateur qui doit mettre en place

[AMS82] D. Anick, D. Mitra, M. M. Sondhi, « Stochastic theory of a data-handling system with multiple sources », *Bell System Tech. J. 61*, 8, 1982, p. 1871–1894.

[LNT97] Z. Liu, P. Nain, D. Towsley, « Exponential bounds with applications to call admission », *Journal of the ACM 44*, 3, 1997.

[EM93] A. Elwalid, D. Mitra, « Effective bandwidth of general markovian traffic sources and admission control of high speed networks », *IEEE/ACM Transactions on Networking 1*, 3, 1993.

un système de communication ou de faire évoluer un système existant. Ceci peut concerner un aspect spécifique du système considéré (par exemple, un problème de facturation), ou un type particulier de réseau (par exemple, un problème de configuration dans le cas de l'utilisation de lignes asymétriques comme dans la technologie ADSL).

D'autres applications majeures de nos travaux et de notre expertise sont les problèmes de cohabitation de technologies. On y trouve les différents aspects liés au développement explosif du monde IP : IP sur couche de transport ATM, ou sur WDM, les problèmes spécifiques liés non pas à la technologie IP courante mais à la future version IPv6, y compris ceux de la transition entre les deux versions du protocole. À ceci peuvent s'ajouter encore d'autres problèmes supplémentaires. À titre d'exemple, citons des travaux réalisés pour étudier l'utilisation d'ATM au-dessous du futur protocole IPv6, avec comme objectif d'offrir une certaine QoS aux utilisateurs. Les extensions IP mobile, IP cellulaire, les aspects liés à la sécurité dans le monde IP ou à la diffusion en multicast de l'information, sont également des domaines d'application importants.

Toujours au niveau de l'identification des domaines principaux d'application des activités de recherche d'Armor, nous pouvons les indexer par type de service concerné, et, dans ce cas, l'expertise passée et présente des membres de l'équipe met en avant deux services majeurs : le transport de flux multimédia par les réseaux et la téléphonie sur technologie IP. Dans le premier cas se trouvent les problèmes de conception de mécanismes adaptés à des classes de flux particuliers et des objectifs de QoS spécifiques, aussi bien au niveau de l'accès au réseau que dans les nœuds intermédiaires. Dans le second cas, il s'agit des nombreux problèmes liés au développement déjà aujourd'hui important des applications de téléphonie sur une structure IP qui n'a pas été conçue pour supporter de telles utilisations. Citons, par exemple, l'utilisation de *passerelles*, la mise en œuvre de fonctions de contrôle, la mise en œuvre d'une technologie IP *native* (c'est-à-dire, sans utilisation de mode connecté), la facturation, etc. Nous cherchons maintenant à faire converger ces travaux dans le cadre de la norme UMTS.

Dans les aspects liés à l'analyse et au dimensionnement, nous apportons nos compétences dans l'utilisation des différentes méthodologies associées (mesures, simulation, techniques dites *analytiques*) mais aussi dans le développement de nouveaux outils, mathématiques et informatiques. Nous développons des modèles destinés à capter des aspects spécifiques des systèmes, liés par exemple à la QoS. Nous développons également des méthodologies de simulation, pour pouvoir analyser des aspects d'accès difficile avec les technologies disponibles. Enfin, il faut observer que les réseaux offrent maintenant des services avec un certain niveau de redondance, ce qui conduit à des problèmes de sûreté de fonctionnement. Notre groupe a maintenant une longue expérience dans l'étude spécifique de cet aspect des systèmes, et sur des problèmes liés comme ceux de l'analyse de la performabilité, ou de la vulnérabilité d'une topologie maillée, par exemple.

5 Logiciels

Nous avons mis en œuvre et nous maintenons une plate-forme IPv6 intégrant différents mécanismes proposés récemment dans le cadre de la QoS dans les réseaux IP (RSVP, différenciation de services, techniques d'ordonnancement). Il s'agit d'un support de recherche qui, de plus,

permet à notre groupe et à des acteurs extérieurs, de tester ces nouvelles technologies. Cette plate-forme fait partie du réseau expérimental IPv6 français (le *G6-bone*), lui-même inclus dans le réseau mondial expérimental IPv6, le *6-bone*. Elle est maintenant le Point d'Interconnexion Régional pour la Bretagne et les pays de Loire.

Lors de travaux de recherche précédents, nous avons développé des logiciels fournissant des services de sécurité et aujourd'hui dans le domaine publique. C'est le cas de NSP (*Network Security Probe*), outil de supervision destiné à l'administration de la sécurité d'un site IP ; voir `http://www.rennes.enst-bretagne.fr/nsp/xnsp`.

Nous développons des outils logiciels pour l'évaluation de modèles de divers types. Par exemple, nous avons produit pour le Celar une bibliothèque de méthodes d'évaluation d'architectures de réseaux maillés du point de vue de la fiabilité. Les programmes de cette bibliothèque sont capables de calculer des mesures de fiabilité et d'analyser également leur sensibilité par rapport aux données. Ces évaluations se font suivant des approches de type combinatoire ou par Monte Carlo. Nous avons également développé des programmes d'analyse de la vulnérabilité, toujours pour le même type de réseaux, et des programmes d'analyse de certaines mesures de performabilité. Nous avons également développé des logiciels permettant de construire des modèles markoviens et des bibliothèques d'analyse de ce type de modèle (en particulier dans des collaborations avec le Cnet).

Notre groupe a développé des outils variés de simulation, et continue à en développer des nouveaux. Nous avons fait plusieurs contributions au simulateur du Nist pour des réseaux ATM. L'équipe a développé également un simulateur à événements discrets appelé Samson, spécialisé dans les problèmes de type temps réel, utilisé par plusieurs centres académiques en France ; (voir `http://www.rennes.enst-bretagne.fr/~toutain/samson`). Nous avons fait des contributions au langage QNAP, qui fait actuellement partie du progiciel Modline développé et distribué par la société Simulog. Nous travaillons actuellement sur un simulateur travaillant dans le paradigme des modèles *fluides* (à états continus), qui est particulièrement efficace dans le cas des réseaux haut débit.

6 Résultats nouveaux

Résumé :

Nous structurons la description des travaux réalisés cette année en deux groupes, fédérés respectivement par les problèmes de contrôle et les problèmes d'analyse et dimensionnement de réseaux (autant du point de vue l'étude d'un système spécifique que de celui du développement méthodologiques).

6.1 Contrôle dans les réseaux

6.1.1 Ingénierie des réseaux IP

Participants : Octavio Medina, Ahmed Mokhtar, Gerardo Rubino, Laurent Toutain.

L'un des problèmes majeurs des réseaux IP, et en particulier du réseau Internet, est la difficulté à gérer convenablement la QoS pour de nouvelles applications comme le multimédia

ou la téléphonie. Le protocole TCP avec ses mécanismes de contrôle de flux n'est pas adapté. Si la modification du comportement de TCP est délicate et ne pourra se faire que lentement, différentes approches pour améliorer le comportement du réseau sont suivies par de nombreux groupes de recherche. Ces tentatives passent nécessairement par la modification de la gestion des files d'attente dans les équipements d'interconnexion. La politique de service Fifo peut être remplacée par des politiques comme Weighted Round Robin ou Weighted Fair Queuing. Mais une garantie de bande passante ne peut être établie que si un contrôle d'admission s'applique pour les trafics concernés. Plusieurs possibilités sont envisageables pour cela. La première approche a été historiquement standardisée par l'IETF ; elle comprend les travaux autour du protocole RSVP permettant de signaler les caractéristiques des flux pouvant nécessiter une amélioration de la qualité par rapport au Best Effort. Les flux ainsi identifiés peuvent être mis par les équipements dans la classe garantie et bénéficient d'un temps de traversée des paquets borné[2]. Une autre classe de service, plus simple à mettre en œuvre, offre un comportement plus simple, en simulant les performances d'un réseau peu chargé. Signalons, malgré tout, que l'utilisation à grande échelle de RSVP se heurte au problème dit du passage à l'échelle. En d'autres termes, pour ce travail le coût associé croît trop vite avec la taille du réseau. En outre, RSVP est confronté à l'absence d'un mécanisme de facturation. Cela ne permet pas son déploiement à travers un réseau d'opérateurs. Tous ces facteurs devraient limiter l'usage de RSVP à un domaine (système autonome) donné.

L'approche privilégiée actuellement, et sur laquelle nous travaillons, est celle de la *différenciation de service*. Il s'agit d'une proposition visant à offrir à certaines classes de trafic une portion importante de la bande passante, allant même jusqu'au surdimensionnement du réseau, en cas de congestion. Leurs paquets auront une probabilité de rejet inférieure aux autres. L'hypothèse concernant le contrôle d'admission adopté pour la différenciation de service ne permet pas d'obtenir des garanties absolues. Elle suppose un dimensionnement correct du réseau par l'opérateur pour un sous-ensemble de flux marqués. Des mécanismes de contrôle situés à l'entrée du réseau permettent de s'assurer que ces flux respectent le contrat passé entre l'utilisateur et le réseau, ainsi qu'entre les réseaux interconnectés. Cette approche est envisageable si la proportion des flux marqués est relativement faible par rapport aux flux restants qui seront traités en Best Effort. Actuellement, deux comportements dans les routeurs sont définis par l'IETF. Ils permettent de construire des classes de service au sein d'un réseau d'opérateur. Nous nous intéressons tout particulièrement aux interactions entre les trafics TCP et UDP. Ces derniers sont principalement utilisés par les flux multimédia. Nous avons défini un marquage à la source qui permet au réseau de prendre en compte la valeur sémantique de l'information transportée pour évaluer la probabilité de rejet en cas de congestion.

Nous travaillons également sur l'architecture des systèmes de caches sur Internet. Notre intérêt porte sur la coopération entre des systèmes locaux, c'est-à-dire, travaillant à l'intérieur d'un site, et des systèmes globaux. Nous avons défini une architecture permettant d'organiser la collaboration entre ces deux niveaux, dont des premiers éléments sont présentés dans [26].

Pour améliorer la qualité de service, une voie différente de celles discutées ici s'appuie sur l'ingénierie de trafic. Cette approche est décrite dans la section suivante.

2. Une approche récente, appelée *Network Calculus*, permet dans certains cas de calculer des bornes intéressantes des délais. Dans d'autres cas, les garanties offertes peuvent être calculées dans des situations très pessimistes, ce qui implique généralement une sous-utilisation des ressources du réseau.

6.1.2 MPLS

Participants : Bernard Cousin, Laurent Toutain, Miled Tezeghdanti.

Actuellement, avec les protocoles de routage interne (intra domaine), la détermination des routes à l'intérieur d'un domaine est automatisée et un seul chemin est utilisé à la fois. Ceci conduit à la sous-utilisation de certains liens et à la saturation de certains autres. Une gestion plus fine des flux à l'intérieur d'un domaine permettrait une meilleure utilisation des ressources et par conséquent une meilleure qualité de service. Pour répondre à ces besoins, la technique MPLS (MultiProtocol Label Switching) a été développée. Ce protocole intègre le matériel de commutation de niveau 2 déjà existant (comme les commutateurs ATM) et le protocole IP, tout en conservant le plan de signalisation IP (c'est-à-dire le routage). MPLS apporte de nouvelles fonctionnalités au routage IP classique. Il rend disponible les fonctions de gestion de la qualité de service d'ATM. Il autorise aussi la conception d'un routage contraint par la qualité de service ou routé par la source.

Si certains mécanismes liés à MPLS sont déjà standardisés au sein de l'IETF ou en passe de l'être, d'autres parmi les plus prometteurs restent encore à explorer. Nous nous proposons d'étudier la gestion de l'agrégation et l'intégration du multicast dans un réseau à commutation de labels. D'une part, cela suppose l'étude de l'interaction des algorithmes de routage multicast (PIM, CBT, MOSP, DVMRP,...) et de la commutation de labels. Nous étudions plus particulièrement la cohérence des politiques et des mécanismes de gestion de la qualité de service avec le trafic multicast. D'autre part, MPLS autorise l'agrégation des multitudes de flux qui circuleront dans le réseau. Cette agrégation permettant d'économiser les ressources du réseau et d'améliorer les performances, il nous paraît intéressant d'étudier les implications d'une telle agrégation sur les politiques de gestion de la qualité de service. Nous avons proposé un algorithme permettant de calculer les étiquettes de commutation en fonction des informations transportées par les protocoles de routage [33]. Cet algorithme permet d'automatiser la gestion d'un réseau MPLS. Cette automatisation ne sera pas générale. En effet, certains flux, comme ceux produits par les réseaux privés virtuels, seront traités avec plus d'attention par les opérateurs. Dans ce cas, les routes seront déterminées et dimensionnées par ce dernier. En particulier des routes de secours seront prévues en cas de problèmes sur le chemin principal. Nos travaux sur la fiabilité dans les graphes (voir module 6.2.3) permettent de concevoir des réseaux ayant une résistance à la panne de certains liens ou équipements de commutation. En cas de défaillance, des ressources pourront être préemptées pour que, par exemple, les réseaux privés virtuels continuent de bénéficier d'une qualité de service.

6.1.3 Diffusion et communication multicast

Participants : Raymond Marie, Miklós Molnár.

Dans les réseaux haut débit, les applications qui nécessitent une communication entre plusieurs utilisateurs sont de plus en plus présentes (diffusion de séquences vidéo, organisation des téléconférences, etc.). La diffusion des messages, ou la communication multipoint, est optimale du point de vue topologique si son support correspond à un arbre couvrant partiel minimal. La construction d'arbres couvrants partiels minimaux (problème de Steiner des réseaux) étant

un problème NP-complet, plusieurs heuristiques ne nécessitant qu'un temps d'exécution polynomial sont utilisées. Pour la diffusion multipoint des messages, la longueur de l'arbre utilisé est très importante puisque le coût de la diffusion dépend de cette longueur. Une partie des heuristiques (comme l'heuristique de Takahashi et de Matsuyama, celle de Kruskal ou l'algorithme de Kou et al.) utilise les plus courts chemins du graphe pour construire l'arbre. Dans certains cas, nous avons constaté que la performance des arbres construits sur la base des plus courts chemins ne peut pas être améliorée ; hélas, il existe des configurations pour lesquelles l'arbre couvrant obtenu par les plus courts chemins est éloigné de l'arbre minimal de Steiner (du groupe concerné de sommets). Nous avons donc développé plusieurs algorithmes de construction pour trouver des approximations moins coûteuses de l'arbre minimal de Steiner. Certains sont basés sur des connexions plus avantageuses que les connexions réalisées à l'aide des plus courts chemins.

Pour établir des arbres de diffusion plus favorables, la connexion optimale de deux arbres isolés afin d'obtenir un arbre commun a été étudiée. Dans les heuristiques classiques, s'il s'agit de l'union des sous-arbres, un chemin qui correspond à la distance entre les arbres est utilisé pour connecter les sous-arbres de la solution finale. Nous avons constaté que la connexion optimale, elle aussi, est un arbre minimal de Steiner. En fonction du nombre de feuilles de l'arbre qui réalise la liaison, plusieurs connexions peuvent être envisagées (l'optimum est une des connexions sous forme d'arbre). Dans les cas de dimension trop élevée, le calcul de la solution optimale peut coûter très cher ; mais les connexions alternatives permettent de trouver une solution quasi-optimale pour unifier les arbres dans un temps de calcul limité. Pour améliorer la performance des arbres de diffusion multipoint sous contrainte de temps de calcul, nous avons développé des heuristiques avec une complexité paramétrisable.

Un de nos algorithmes suit la construction proposée par Kruskal mais il examine les arbres minimaux de Steiner de complexité limitée pour établir les connexions [37]. Les résultats sont en général des arbres aussi performants que les solutions obtenues par les meilleures heuristiques. L'avantage de la solution proposée vient du fait que la complexité des arbres de liaison et la profondeur de la recherche des liaisons possibles au cours de la construction sont des paramètres qui peuvent fournir un compromis entre la qualité du résultat et le temps d'exécution [27].

L'algorithme modifié de Kruskal est également intéressant du point de vue de parallélisation. Nous avons élaboré la version distribuée de cette nouvelle heuristique afin d'utiliser les capacités de calcul potentielles des serveurs gestionnaires du réseau pour calculer indépendamment les différents sous-arbres du support multipoint [28].

L'amélioration des connexions au cours de la construction de l'arbre de diffusion est possible en partant de l'heuristique largement utilisée de Takahashi et Matsuyama. La nouvelle heuristique ainsi qu'une analyse du problème des connexions sous forme d'arbre se trouve dans [36].

Actuellement, la nouvelle conception des connexions possibles des arbres nous permet de réviser et de généraliser les heuristiques basées sur la fermeture métrique du problème, à l'aide de la nouvelle conception des connexions potentielles des arbres.

6.1.4 Transition IPv4/IPv6

Participants : Hossam Afifi, Laurent Toutain.

Le protocole IPv6 devrait remplacer à terme le protocole actuel de l'Internet, IPv4. Il ne présente pas vraiment de particularités additionnelles majeures, sauf au niveau de l'adressage. IPv6 apporte une richesse considérable dans l'espace d'adressage qui peut être exploitée pour changer de nombreux principes dans les réseaux. Néanmoins, IPv6 n'est pas compatible IPv4 ; il est donc nécessaire de proposer des mécanismes de transition adaptés. Nous avons développé une technique appelée DTI (*Dynamic Tunneling Interface*) pour la transition entre les deux versions du protocole. Nous avons montré qu'il s'agit d'un mécanisme robuste, qui a été proposé à l'IETF pour devenir un standard [45], après fusion avec un autre mécanisme similaire mais concurrent portant le nom de AIIH (*Assignment of* IPv4 *Global Addresses to* IPv6 *Hosts* ; voir aussi [21]). L'idée principale est basée sur des encapsulations du protocole IPv4 dans des paquets du protocole IPv6 afin de traverser les sous-réseaux IPv6. Des mécanismes de résolution de noms dans le réseau sont alors nécessaires, afin d'apporter la traduction d'adresses entre les deux mondes. Plusieurs mises en œuvre ont été réalisées et des mesures de performances ont été effectuées. Nous avons montré que la performance de DTI est meilleure que celle de IPv4 pour des applications client-serveur. Ceci provient principalement de l'optimisation de la pile IPv6 et de la rapidité avec laquelle lma résolution de noms s'effectue pour l'établissement du tunnel nécessaire. En effet, de nombreuses étapes sont court-circuitées dans IPv6 par rapport à l'ancienne version. Nos tests ont permis de mettre en évidence ces phénomènes.

6.1.5 Ordonnanceur hiérarchique

Participants : Hossam Afifi, Gerardo Rubino.

Des travaux passés nous ont permis de développer des techniques de régulation des flux sortant d'une station de travail pouvant émettre à la fois des flux garantis et non garantis, avec comme objectif le partage équitable de la bande passante. Nous travaillons maintenant sur l'extension de ces mécanismes sur un site complet (un réseau local).

Dans cette situation, nous nous positionnons, par exemple, à la sortie du réseau local d'un site donné, et nous nous posons le problème d'offrir aux applications garanties la proportion de trafic qui leur est destinée et aux flux non-garantis le reste de la bande passante disponible, en évitant surtout de perdre des données. L'idée principale est que l'on ne doit pas perdre de paquets dans son propre réseau. Dans un réseau local, les applications génèrent une variété de trafics appartenant à différentes classes de services : une première classe regroupe les applications sensibles au délai et au débit tels que les flux interactifs et les applications temps-réel. Ces applications ont besoin de garanties sur les paramètres de qualité de service (QoS). On les appelle « applications garanties ». La deuxième classe englobe les applications pouvant s'adapter aux ressources disponibles sur le réseau. Elles sont appelées « applications non garanties ». Une troisième classe englobe la nouvelle génération d'applications à garanties par rafales. Elle est traitée par le mécanisme ABT. L'intégration de ces applications dans un même réseau local a fait émerger le besoin d'un modèle de gestion de la bande passante disponible. Nous avons donc proposé un nouveau modèle capable d'apporter une solution au problème. Il s'agit d'un modèle hiérarchique appelé *Hierarchical bandwidth manager*, qui est capable de gérer simultanément les applications garanties et non garanties de façon à ce que l'excès de bande passante non utilisé par les applications garanties soit partagé entre les applications non garanties. Une

représentation hiérarchique sous forme d'arbre est utilisée pour modéliser le débit sur les liens du réseau local. La régulation du débit disponible sur les liens est assurée d'une façon distribuée. Le schéma adopté est celui qui est utilisé dans les mécanismes connus sous le nom de Weighted Round Robin. La différence est simplement que notre modèle est distribué alors que les modèles tels que le Weighted Round Robin, sont centralisés dans un routeur et ne peuvent donc pas réguler les flux comme nous le faisons. Dans le cas de CBQ, une file qui se remplit peut déborder et perdre des paquets alors que le Hierarchical Bandwidth Manager n'en perdra pas. Ce travail a donné lieu à la conception de deux architectures. Dans la première, un protocole d'échange entre nœuds a été conçu afin d'informer de la disponibilité ou du manque de bande passante pour réduire les débits à la source et ainsi éviter les pertes. L'application de ce mécanisme pourra évidemment servir dans les réseaux, privés virtuels entre sites. Dans la seconde, en cours de développement, nous explorons l'application des réseaux de neurones pour effectuer le partage des charges entre les nœuds par le biais d'un module de prédiction de trafic.

6.1.6 Codage bas débit

Participants : Hossam Afifi, Yasser Ahmed.

Codage par zones. Nous travaillons sur des techniques permettant le codage d'images par régions, dans le but de pouvoir mieux exploiter des liens bas débit. Cette méthode trouve son intérêt dans deux contextes différents. D'une part, elle est utile lorsqu'il est nécessaire de focaliser la haute résolution sur une zone de l'image et de laisser moins de détails dans les autres zones. Ceci trouve des applications dans l'imagerie médicale, par exemple, et dans des outils militaires. D'autre part, elle est intéressante lorsque le débit du réseau est très limité et il est nécessaire de dégrader l'image. Nous devons à ce moment choisir une zone de moindre intérêt et la coder avec moins de précision, afin d'optimiser l'usage du canal. Le choix du standard permettant de réaliser un tel système s'est porté sur MPEG II. Malgré la présence du concept de codage par objets et par régions dans la norme MPEG IV, nous avons préféré travailler avec MPEG II pour des raisons de disponibilité et de large distribution de cette dernière.

Notre architecture consiste en une partie standard correspondant aux processus de codage et de décodage conventionnels, enrichie de la fonctionnalité de codage par zones. Cette fonctionnalité est pilotée par deux mécanismes distincts. Le premier est un accès, dans le récepteur, à l'image affichée. Typiquement, cela consiste en une application graphique qui permet, grâce à un dispositif de pointage, de sélectionner sur l'écran des zones que l'on souhaite recevoir avec plus de précisions. Le second est un accès dans le codeur permettant de coupler un mécanisme de segmentation pour retrouver les contours des objets dans les séquences vidéo. L'objectif est ici de coder chaque objet selon une certaine finesse de grain. Ceci fait la liaison avec la section suivante décrivant des travaux dans le domaine de la segmentation d'images. Les résultats de cette nouvelle méthode ont été très satisfaisants. Ils ont permis, par exemple, de mettre en évidence plusieurs problèmes dans la norme MPEG II (voir [21]).

Techniques de calibration. Dans la section précédente, nous avons vu que certaines zones de l'image vont avoir plus de détails que d'autres. Comme les zones d'intérêt et celles moins importantes sont dans une même image, nous aurons deux facteurs de quantification pour chaque région. Il est même envisageable d'avoir des zones avec trois ou quatre niveaux différents de détail. Ceci dit, lors de la recherche d'un bloc d'une zone de haute qualité dans les régions voisines afin d'éliminer la redondance spatiale, il est très probable de retrouver des blocs similaires dans les régions extérieures à la région initiale. À ce moment, il y a une « infiltration » dans le codage. La raison est que si nous trouvons le même bloc ailleurs, nous ne codons plus le bloc en question mais son vecteur de mouvement. Mais comme le bloc s'est déplacé dans une zone de moindre qualité, il sera codé en fonction de celle-ci. Nous disons alors qu'il y a une *infiltration de bruit* dans la zone. Le remède que nous avons proposé est de coder les contours des objets par des blocs de type I. Ces blocs représentent une sorte d'enveloppe de l'objet et permettent d'éviter de rechercher le bloc hors de la région. L'inconvénient qui en découle est le fait que le rapport de compression de l'image est moins important, dû aux blocs de type I qui sont généralement gourmands en bande passante. Nous montrons que pour le codage d'une seule zone d'intérêt dans une séquence vidéo avec une maquette développée à Berkeley, la qualité se dégrade considérablement au-delà de zones de 45 blocs. Tous ces paramètres dépendent évidemment du débit disponible pour la totalité du flux. Il serait aussi possible de transmettre chaque flux séparément afin de les différentier. Nos travaux s'orientent actuellement dans cette direction (voir [20]).

6.1.7 Téléphonie sur Internet

Participants : Hossam Afifi, Bernard Cousin, Samir Mohammed, Laurent Toutain.

Nous menons une étude dans le cadre de la téléphonie sur Internet. Il s'agit de vérifier l'adéquation des réseaux numériques actuels vis-à-vis du transport de la voix. On se propose de définir les caractéristiques (délai, gigue, taux de perte, etc.) que doit avoir un réseau Internet pour supporter la transmission de la voix, d'analyser les techniques et les outils proposés actuellement, et d'étudier les nouveaux services qui pourraient émerger de la synergie du téléphone et d'Internet. Dans le cadre de ce travail nous conduisons des tests d'intégration de services avec les Gateways et Gatekeepers du marché utilisant la norme H323. Nous envisageons de modéliser une application de type Web capable d'établir sur un simple « click » une liaison téléphonique vers un centre d'appels distants. Un accord de transfert technologique entre l'Irisa et Transpac a été établi autour de ce champ d'étude.

Nous avons également travaillé sur les problèmes d'adressage IPv6 en combinaison avec celui utilisé dans le cas du réseau téléphonique, en l'occurrence la norme E.164 et ses dérivées. L'objectif de ces travaux est d'arriver, à terme, à avoir une méthode unique d'adressage. Sur ce thème, nous avons fait récemment une contribution à l'IETF [44]. L'un des problèmes sur lesquels nous travaillons actuellement est celui du *handover* permettant aux stations de base de ré-attribuer un numéro téléphonique. Le but est d'aboutir à un IP-mobile différent des propositions actuelles, avec un routage plus efficace et une meilleure utilisation de la bande passante.

6.1.8 Sécurité

Participants : Sylvain Gombault, Maryline Laurent, Ollivier Paul.

Sécurité ATM. Faisant suite aux travaux réalisés dans la thèse de Maryline Laurent[Lau97], certaines extensions concernant le placement de services de sécurité dans le modèle ATM ont été obtenus [10].

Dans le cadre du projet ACTS Scan (voir module 7.2), nous avons proposé une méthode pour négocier des services de sécurité dans le protocole ATM. Cette solution est différente de celles préconisés par l' ATM Forum. Elle consiste à utiliser les cellules de gestion ATM pour transporter des informations de sécurité. Le format et l'utilisation de ces nouvelles cellules ont été présentés à l'ATM Forum dans [24]. Cette nouvelle possibilité de négocier des services de sécurité, ainsi que certaines spécifiées par l'ATM Forum sont en cours de développement. Les résultats de ces travaux sont publiés dans [23], [29].

Contrôle d'accès ATM. Des travaux commencés en septembre 97 et menés en collaboration avec la DGA portent sur le contrôle d'accès ATM, au sens de pare-feu ATM (c'est-à-dire, le trafic ATM est filtré en fonction d'une politique de sécurité donnée). Ce travail bénéficie du soutien de Thomson CSF qui a mis en place quelques éléments de filtrage préconisés dans la thèse de M. Paul. Cette thèse a permis de classer les paramètres ATM en fonction de l'intérêt qu'il y a à les filtrer. Différentes architectures permettant d'envisager le filtrage des paramètres en différents points du réseau ont été développées, le but de ces architectures étant de filtrer le plus finement possible le trafic ATM tout en ayant le moins d'impact possible sur la qualité de service des communications ATM. Ces architectures ont été publiées dans [29] et [30]. Suite aux résultats obtenus, un projet avec le Cnet et le Celar devrait voir le jour en décembre 1999 dans le cadre de Goëtic. Ce projet s'appellera Carat (Contrôle d'Accès et qualité de service dans les Réseaux ATM). Il consiste à réaliser une maquette utilisant une carte à 622Mb/s développée par le Cnet et mettant en place un filtrage de niveau ATM. Le but de cette maquette est principalement de tester les capacités requises pour réaliser des contrôles d'accès plus ou moins fins. Ceci permettra de définir une architecture de contrôle d'accès réaliste.

La sécurité IPsec. Cette activité consiste pour l'instant à faire de la veille technologique. Nous étudions la mise en place de services de sécurité dans le protocole IP. Une activité de conseil a d'ailleurs été menée pour Thomson CSF dans ce cadre. Les résultats de cette étude ont fait l'objet d'un chapitre du livre [11] et de la publication [9].

Détection d'intrusions. Nous poursuivons des travaux passés dans le cadre de la détection d'intrusions dans les réseaux. Nous développons actuellement un outil de détection à sondes distribuées, appelé Diams, dans le but de détecter des classes d'attaques étudiées précédemment. Cet outil est basé autour d'un serveur Web et comporte plusieurs types de modules. En particulier, on y trouve une interface permettant de définir des règles de filtrage, des agents

[Lau97] M. LAURENT, *Protection des communications sur les réseaux ATM*, thèse de doctorat, université de Rennes 1, juillet 1997.

intelligents qui analysent le trafic des segments sur lesquels ils sont placés pour analyser, agir, assembler des informations et les envoyer à un collecteur, et des récepteurs qui permettent de visualiser les résultats, en temps réel ou a posteriori.

6.2 Analyse et dimensionnement

Résumé :

Les travaux décrits dans cette section concernent aussi bien des résultats de type analytique que des recherches sur la simulation, sous diverses formes. L'objectif général est le développement de nouvelles méthodes d'évaluation de modèles, autant du point de vue de la sûreté de fonctionnement que des performances.

6.2.1 Modèles markoviens

Participants : Haïsçam Abdallah, Moulaye Hamza, Gerardo Rubino, Bruno Sericola.

Performabilité et détection du régime stationnaire. Une nouvelle méthode de calcul de mesures transitoires, en particulier la disponibilité et la performabilité ponctuelle ainsi que la disponibilité et la performabilité moyenne sur un intervalle, a été développée pour des modèles à espace d'états fini. Cette méthode, détaillée dans [17] utilise la détection du régime stationnaire qui permet d'une part, d'éviter de nombreux calculs lorsque le régime stationnaire est atteint en un certain sens et d'autre part de connaître la valeur de la mesure recherchée en régime stationnaire. L'étude de la distribution de la performabilité [15] pour des modèles markoviens acycliques par blocs a conduit au développement d'un algorithme spécifique qui permet de simplifier considérablement les calculs effectués dans le cas général. Des études plus fines détaillées dans [39], concernant les distributions jointes de temps d'occupation de sous-ensemble d'états ainsi que les distributions de combinaisons linéaires de ces temps d'occupation ont abouti à des expressions simples de ces distributions.

Sensibilité de mesures de performance et de sûreté de fonctionnement. La sensibilité d'une mesure est sa dérivée partielle par rapport à un paramètre de la matrice de transition (taux de panne, taux de recouvrement, etc.). L'évaluation de la sensibilité de mesures transitoires est nécessaire du fait que les taux sont souvent approchés. On s'intéresse aux modèles markoviens raides pour lesquels les taux de panne sont très faibles par rapport au taux de recouvrement (ou de restauration). Lors de l'analyse de la sensibilité, nous sommes confrontés aux problèmes du temps de calcul et de la précision numérique des résultats. Les travaux consacrés à la sensibilité de mesures transitoires instantanées ont permis l'amélioration des méthodes Ode L-stables à l'aide d'un nouveau choix du pas accélérant leur exécution. Ils ont montré la supériorité des méthodes des puissances uniformisées (PU) et IRK3 face aux techniques d'uniformisation standard (US) et TR-BDF2 ([34],[19]).

En ce qui concerne la sensibilité de l'espérance de récompense accumulée sur un intervalle donné, une extension de la méthode PU a été réalisée. Après adaptation de la méthode IRK3 au calcul de cette sensibilité, les trois méthodes PU, US et IRK3 ont été comparées vis-à-vis de la

complexité temporelle. Les techniques IRK3 et PU affrontent mieux la raideur que la technique US.

En vue d'évaluer des mesures relatives aux systèmes parallèles (et en particulier aux réseaux ATM) ainsi que de leur sensibilité, nous utilisons les réseaux d'automates stochastiques comme outil de modélisation. Ceci évite la construction du générateur infinitésimal. Plus clairement, nous avons affaire à un processus markovien associé à chaque automate avec un espace d'état raisonnable. Le générateur global (le descripteur) peut être exprimé comme un produit tensoriel des générateurs correspondant aux automates. Compte tenu de la sélection des méthodes robustes adaptées aux modèles markoviens à espace d'état raisonnable, le cas d'automates indépendants est alors résolu. Les études actuellement menées concernent le cas où les automates sont dépendants par synchronisation.

Analyse stationnaire de grands modèles. Cet axe de recherche concerne l'un des goulots d'étranglement de la modélisation quantitative, celui de l'explosion combinatoire des espaces d'états des modèles markoviens. Une approche développée récemment pour palier en même temps le problème de l'explosion combinatoire et celui de la raideur des modèles (et qui, en fait, exploite à son profit cette raideur) consiste à calculer des bornes des mesures d'intérêt. L'idée sous-jacente est que, même si l'espace d'états est grand, la valeur de la mesure que nous considérons dépend « essentiellement » de ce qui se passe sur un petit nombre d'états. Tout le problème est d'être capable de borner l'erreur introduite lorsqu'on réalise des calculs avec une information partielle, ainsi que, bien entendu, de concevoir ces procédures de calcul. Un problème supplémentaire est celui de l'identification efficace du sous-espace utile pour l'obtention de bonnes bornes sur les mesures d'intérêt. Des travaux récents ont permis d'obtenir des bornes de qualité pour des mesures asymptotiques, dans le cas de la sûreté de fonctionnement. Ces travaux exigent que les modèles vérifient certaines hypothèses qui sont parfois assez restrictives. Par ailleurs, le phénomène de raideur associé en général aux modèles construits dans le but de travailler avec des mesures de sûreté de fonctionnement, a son analogue dans le monde de l'évaluation de performances, dans le cas des systèmes faiblement chargés. Malheureusement, les conditions d'applicabilité des techniques existantes sont rarement satisfaites dans ce contexte. Notre effort s'est concentré dans cette direction et nous avons développé une nouvelle approche ayant moins de restrictions dans son applicabilité [14]. Par exemple, nous avons obtenu des bornes fines de mesures asymptotiques calculées à partir de réseaux de files d'attente ouverts (i.e., des modèles avec une infinité d'états), pour lesquels il n'y a pas de solution analytique connue. Nous avons poursuivi cet effort pour fondamentalement élargir encore le champ d'application de notre méthode. Dans la mesure où elle dépend encore de la résolution de systèmes linéaires qui peuvent toujours être de grande taille, nous avons développé un raffinement permettant, sous certaines hypothèses, de traiter aussi de tels cas. Nous travaillons sur des extensions de l'approche de base, en particulier, pour traiter des problèmes de performance.

6.2.2 Monte Carlo et Quasi-Monte Carlo

Participants : Louis-Marie Le Ny, Gerardo Rubino, Bruno Tuffin.

Monte Carlo. Nous avons travaillé dans le cadre de l'évaluation de mesures de sûreté de fonctionnement de systèmes multi-composants réparables, à partir de modèles markoviens [35]. En considérant le cas des mesures stationnaires ou encore de la MTTF, nous avons étudié les méthodes de Monte Carlo existantes, appartenant toutes au cadre de l'échantillonnage préférentiel. Nous avons proposé des améliorations de certaines de ces méthodes, et nous avons comparé les performances obtenues.

Approximation normale bornée. Une autre contribution apportée à la simulation des systèmes markoviens hautement fiables est l'introduction d'un nouveau concept, l'*approximation normale bornée* [18], qui valide l'utilisation, parfois abusive, de la loi normale pour des fiabilités proches de 1 (i.e. quand $\varepsilon \to 0$), ainsi qu'une condition nécessaire pour obtenir cette propriété. En effet, la littérature s'était focalisée sur la notion d'erreur relative bornée (déterminant si la taille relative de l'intervalle de confiance est bornée quand $\varepsilon \to 0$), indépendamment de savoir si la loi normale, dont dépend l'intervalle de confiance, est bien approximée. La propriété d'approximation normale bornée est basée sur le théorème de Berry-Esseen déterminant la vitesse de convergence de la distribution *empirique* F_I centrée et normée vers la loi normale centrée et réduite $\mathcal{N}$ en fonction des moments absolus d'ordre deux et trois σ^2 et ρ de la variable aléatoire considérée et de la taille I de l'échantillon :

$$|F_I(x) - \mathcal{N}(x)| \leq \frac{c\rho}{\sigma^3\sqrt{I}}.$$

Une condition nécessaire et suffisante pour obtenir la propriété est donc une condition sur chaque cycle régénératif de la chaîne de Markov pour que la quantité ρ/σ^3 reste bornée quand $\varepsilon \to 0$. Il a été possible, grâce à la mise en évidence de cette condition, de déterminer les techniques, parmi toutes celles existantes, vérifiant la propriété et de démontrer que l'approximation normale bornée impliquait l'erreur relative bornée. Ce dernier résultat montre que la propriété importante à vérifier est celle d'approximation normale bornée. Notons aussi que les nouvelles méthodes introduites dans [35] vérifient cette propriété d'approximation normale bornée.

Quasi-Monte Carlo. Nous avons prolongé certains travaux dans le cadre des applications techniques dites de « quasi-Monte Carlo ». Dans quasi-Monte Carlo, l'erreur commise lorsqu'on approche une intégrale

$$\int_{[0,1]}^{s} f(x)dx$$

par

$$\frac{1}{N}\sum_{n=1}^{N} f(\{X + \xi^{(n)}\})$$

(où $(\xi^{(n)})_{n\geq 1}$ est une suite dite à discrépance faible) est bornée par des quantités dépendant de la discrépance de la suite et de la variation, en un certain sens, de la fonction que l'on veut sommer. L'estimation de ces composants des bornes de l'erreur étant en pratique difficile, voire impossible, l'utilisation des suites à discrépance faible comme technique de réduction de la variance dans le cadre de Monte Carlo est une alternative judicieuse. Ainsi nous pouvons

obtenir un intervalle de confiance par le théorème central limite et bénéficier de la bonne répartition des points de la suite à discrépance faible dans l'intervalle d'intégration. L'idée est d'approcher l'intégrale par

$$\widetilde{I} = \frac{1}{MN} \sum_{m=1}^{M} \sum_{n=1}^{N} f(\{X^{(m)} + \xi^{(n)}\})$$

où $(X^{(n)})_{n\geq 1}$ est à nouveau une suite de variables (pseudo-)aléatoires i.i.d. uniformes sur $[0,1]^s$ et $(\xi^{(n)})_{n\geq 1}$ est une suite à discrépance faible. Nous avions précédemment montré que, moyennant des conditions techniques appropriées, la vitesse globale de convergence est en $O(M^{-1/2}N^{-1}(\log N)^s)$ et pouvait même dans certains cas être plus rapide.

Nous avons généralisé l'application de cette méthode à une plus grande classe de réseaux à perte que nous ne l'avions fait précédemment [43], nous permettant maintenant de considérer divers types de réseaux de communications tels que, par exemple, les réseaux ATM. De plus nous avons parallélisé cette méthode et avons illustré sur un modèle de files d'attente multi-classes à forme produit que le gain apporté était linéaire par rapport aux nombres de processeurs utilisés [12].

6.2.3 Architectures de réseaux maillés

Participant : Gerardo Rubino.

Un réseau de communication est vu ici comme un système multi-composants fait de « lignes » et de « nœuds ». Du point de vue de la sûreté de fonctionnement, on représente un tel système par une fonction de structure Φ, en utilisant un langage de haut niveau tel qu'un diagramme de fiabilité, un arbre de défaillance, etc. Concernant la topologie de l'architecture d'un réseau maillé, c'est-à-dire, d'un réseau à grande étendue, il est usuel de le représenter par un graphe dont les éléments sont pondérés par des probabilités (un *graphe stochastique*). Le critère global de bon fonctionnement (la définition de Φ) est en général basé sur des propriétés de connexion dans le réseau : par exemple, il faut que deux nœuds particuliers puissent communiquer, ou que tous les nœuds puissent le faire entre eux, etc. Il s'agit alors de quantifier le comportement du réseau vis-à-vis de ce critère global de bon fonctionnement. Nous avons travaillé dans ce contexte, dans trois directions différentes : fiabilité, performabilité, vulnérabilité. Sur le premier thème, nous avons développé des outils de calcul de diverses mesures de fiabilité, des algorithmes de calcul des sensibilités des dites mesures, et des méthodes d'estimation par Monte Carlo.

Cette année nous avons centré nos efforts au niveau de l'analyse de certaines mesures de performabilité. Pour les définir, nous tenons compte de la capacité des liens et de la quantité de flux qui est envoyé. Ce type de modèle est pertinent en particulier dans le contexte des réseaux de communication (où le flux transporté est l'information). Dans ce contexte, les mesures classiques de fiabilité sont trop pauvres, car elles ne tiennent pas compte des capacités des lignes ni de la quantité de flux qu'il faut transporter. Des mesures de type performabilité sont, bien sûr, capables de cerner l'ensemble des aspects du problème. Encore faut-il être capable de les évaluer, sachant que l'on est dans un cadre plus général que celui considéré dans le module précédent (en effet, le problème du calcul de la fiabilité est un cas particulier de celui-ci). Dans

le cadre d'une collaboration avec le Celar, nous avons étendu des travaux précédents réalisés dans l'équipe, pour traiter des mesures de performabilité multi-sources et multi-terminaux. En particulier, elles permettent d'évaluer la capacité d'un réseau à faire communiquer des sous-réseaux entre-eux [48], [47], [46].

Nous nous sommes intéressés aux techniques de Monte Carlo, et nous avons développé des nouveaux plans d'échantillonnage basés sur une méthode de décomposition de l'espace d'états du modèle. Ces techniques sont du type « réduction de la variance ». Elles permettent d'obtenir des gains très importants (plusieurs ordres de grandeur), en particulier dans le cas de réseaux hautement fiables, ou bien dans le cas où la demande est proche du flot maximal qui peut transiter dans le réseau. Bien entendu, le gain est dans le produit temps-variance, car il faut des méthodes rapides (temps de calcul court) et précises (variance de l'estimateur petite).

6.2.4 Soutien intégré

Participants : Atika Bousseta, Raymond Marie.

La mise en place d'infrastructures de soutien intégré pour des systèmes complexes (*eg*, un système de contrôle aérien au niveau d'un pays) conduit à déterminer la valeur d'un grand nombre de variables. Il faut définir différents sites de maintenance et différents niveaux de compétence ; les sites de niveau le plus faible sont les plus proches des bases d'exploitation : ce sont les feuilles de l'arbre de maintenance (en général unique). Plus on se rapproche de la racine et plus la compétence du site est élevée. En général, cette structure de maintenance existe au moins partiellement avant la mise en place d'un nouveau système. On peut aussi concevoir la structure de ce nouveau système à soutenir comme un arbre dont la racine est le système complet. Cet arbre n'est pas donné *a priori*, il fait partie de l'ensemble des variables de décision. Les feuilles correspondent à des articles (des sous-ensembles) mis au rebut alors que les noeuds intermédiaires correspondent à des articles qui seront réparés par échange d'un sous-ensemble correspondant à un noeud fils. À chaque article associé à un noeud intermédiaire, correspond un site d'échange et un site de réparation.

Au cours des dernières années, le développement technologique a rendu les systèmes plus complexes et a accru les besoins en logistique. En conséquence, le coût d'acquisition d'un système complexe est devenu secondaire face au coût total sur la durée de vie (coût global de possession). Et l'expérience a montré que le coût du soutien est l'un des coûts primordiaux d'une opération. L'objectif actuel est d'inclure l'organisation de la maintenance lors de la réalisation du système. Le logiciel Diana développé par la société Sofreten vise à satisfaire cet objectif. Une partie du travail de thèse de A. Bousseta consiste à enrichir ce logiciel. Dans [22], on présente ce logiciel qui au niveau de l'algorithmique est composé de deux modules principaux. Le premier (Optim-stock) exploite une heuristique cherchant une politique quasi-optimale visant à maximiser la disponibilité du système sous une contrainte de coût. Le second (Cost) aide au calcul du coût global de production.

6.2.5 Dimensionnement de réseaux ATM

Participants : Raymond Marie, Nathalie Omnès.

Nous nous intéressons à certains aspects du dimensionnement de réseaux ATM. Nous avons travaillé sur le dimensionnement d'un espaceur pour la classe de trafic CBR. On examine la situation où une connexion traverse les réseaux de plusieurs fournisseurs de service et où un fournisseur particulier met un contrôleur-espaceur à l'entrée de son réseau. On suppose que le trafic de la connexion CBR est caractérisé par une périodicité T_E et une gigue maximale τ_E.Sous des hypothèses assez générales, on met en évidence une condition nécessaire et suffisante de perte par débordement de capacité de l'espaceur. Ce qui permet d'en déduire un dimensionnement garantissant l'absence de perte. Ensuite, on suppose que la contrainte de gigue maximale τ_E est respectée à ϵ près. À condition de supposer les délais à accroissements indépendants, on démontre que la probabilité de perte est aussi inférieure à ϵ.

6.2.6 Modèles fluides

Participants : Nelly Barbot, José Incera, Raymond Marie, Landy Rabehasaina, David Ros, Gerardo Rubino, Bruno Sericola, Bruno Tuffin.

Réseaux de Petri. Les réseaux de Petri constituent un outil très puissant pour la description et l'analyse de systèmes présentant des « concurrences », de la synchronisation et/ou des conflits. Depuis leur introduction dans les années 70, de nombreuses extensions ont été développées, par l'introduction du temps puis du hasard (utilisant tout d'abord des lois exponentielles pour la date de déclenchement des transitions, puis des lois plus générales). Plus récemment, les réseaux de Petri stochastiques fluides, constitués de places discrètes, mais aussi de places contenant du fluide ont étés introduits. Du fluide peut alors couler vers les places fluides, ou s'en échapper. Ces nouveaux modèles permettent d'approcher une grande quantité de jetons dans une place discrète par un niveau de fluide dans une place fluide, simplifiant ainsi le nombre d'opérations à effectuer sur le modèle pour le résoudre. De plus, nous pouvons ainsi modéliser des systèmes physiques contenant des quantités continues contrôlées par une logique discrète.

Nous avons étudié ces nouveaux modèles, et les avons comparés avec les modèles généralement utilisés pour représenter les systèmes hybrides souvent utilisés en théorie du contrôle notamment [41].

Nous avons aussi participé au développement du logiciel SPNP (pour *Stochastic Petri Net Package*) créé à l'université de Duke et destiné à résoudre des problèmes de performance, fiabilité ou performabilité modélisés par des réseaux de Petri stochastiques (fluide ou non). De nombreux tests du logiciel ont donc été effectués, permettant d'en améliorer l'efficacité ainsi que le manuel [40]. Notamment, le simulateur inclus dans SPNP a été amélioré, incorporant maintenant un choix de nombreuses distributions pour les transitions. De plus, nous avons ajouté des méthodes de réductions de la variance dites d'*importance splitting* pour la simulation des événements rares [42] et illustré le gain obtenu.

Files d'attente. Dans le cadre des travaux menés sur les modèles fluides en régime transitoire avec buffer de taille infinie, nous avions obtenu la distribution de la quantité d'information en attente de traitement lorsque le taux d'entrée dans le buffer est modulé par un processus de Markov à espace d'états fini. Ces études se poursuivent dans le cadre de réseaux de files fluides

alimentés par des sources dont le débit est modulé par un processus de Markov. Plusieurs politiques de service sont envisagées comme la politique Fifo ou la politique GPS ou encore des politiques de service dépendant de la quantité d'information en attente de traitement.

En régime stationnaire, on considère des modèles fluides alimentés par des files markoviennes. Le débit d'entrée dans la file fluide est fonction de l'occupation des serveurs de la file markovienne dont le trafic de sortie peut représenter par exemple le trafic traversant une partie d'un réseau. Ce trafic de sortie sert alors de trafic d'entrée à la file d'attente fluide que l'on souhaite étudier.

Les résultats obtenus dans [16] sont assez généraux, puisque le taux d'entrée dans la file fluide est supposé être modulé par un processus de Markov à espace d'états fini ou dénombrable avec générateur infinitésimal tridiagonal par blocs et uniforme. On suppose de plus que seul un état a un taux d'entrée effectif négatif et que la borne inférieure de l'ensemble des taux d'entrée effectifs positifs est positive. Ces processus de Markov incluent notamment les files M/M/1, M/M/K, M/PH/1, M/PH/K à capacité finie ou infinie.

Pour ces modèles, on obtient dans [16] une expression de la distribution de la quantité d'information en attente et on en déduit un algorithme de calcul qui s'avère être rapide, stable et précis. Des travaux sont en cours pour étendre ces résultats à des files fluides à capacité limitée.

Enfin, les réseaux de files fluides tels que décrits dans le paragraphe précédent sont aussi à l'étude en régime stationnaire, pour diverses politiques de service.

Simulation de réseaux haut débit. Nous avons développé un prototype d'outil de simulation pour l'évaluation de modèles fluides de réseaux haut débit. L'outil est basé sur la simulation à événements discrets d'un modèle fluide (continu) : en posant certaines contraintes sur les sources de trafic, il est possible de décrire complètement l'évolution d'un tel modèle en observant son état uniquement dans un ensemble dénombrable d'instants [38].

Ce type d'approche nous permet d'évaluer des mesures de performance pour lesquelles on ne dispose pas de résultats analytiques, comme par exemple la fréquence et la durée des pertes lors d'une congestion, ainsi que le volume d'information perdu [32], notamment pour des réseaux hétérogènes. Dans de nombreux cas, la simulation fluide s'avère beaucoup plus efficace qu'une simulation équivalente au niveau paquet. Dans ce cadre, nous avons également proposé une méthode heuristique pour l'estimation du délai de bout en bout subi par une connexion [31].

Nous avons pu valider l'approche de la simulation fluide, non seulement dans le contexte des trafics en boucle ouverte[3] qui font habituellement l'objet d'études analytiques, mais aussi en présence de *protocoles* de contrôle de trafic. Pour cela nous avons développé des modèles fluides pour des mécanismes de type ABR et ABT.

Nous étudions actuellement, à l'aide de l'outil de simulation fluide, des algorithmes pour le partage de bande passante dans un réseau ATM transportant des trafics de type ABT élastique.

L'outil a été écrit en C++ et consiste en une bibliothèque modulaire de composants réseau, ainsi qu'un noyau de simulation et des bibliothèques pour la génération de séquences aléatoires, l'obtention de statistiques, etc. En ce qui concerne les composants du réseau, nous disposons

3. Par exemple, la catégorie de service VBR dans les réseaux ATM.

aujourd'hui de classes d'objets permettant la simulation des éléments dits « de base », notamment :

- sources de trafic à boucle ouverte ;
- sources de trafic à boucle fermée, leur débit étant adapté en fonction des informations reçues du réseau, selon un algorithme donné ;
- nœuds de multiplexage, avec des disciplines de service de type Paps ou GPS et, en option, des mécanismes de contrôle de trafic pour les classes de service ABR ou ABT dans les réseaux ATM ;
- matrices de commutation, pour la modélisation de commutateurs ;
- liens de communication ;
- connexions point-à-point unidirectionnelles.

Actuellement nous travaillons sur l'extension de l'approche de simulation fluide à des réseaux TCP/IP, ainsi que sur le développement d'une interface utilisateur. Cette interface devrait faciliter la description des réseaux que l'on souhaite évaluer, ainsi que l'obtention des résultats de simulation. Elle aura une version textuelle et une version graphique.

7 Contrats industriels (nationaux, européens et internationaux)

7.1 Performabilité des réseaux à large étendue, 1 98 C 531

Participant : Gerardo Rubino.

Résumé : *Il s'agit d'une convention de recherche passée avec le Celar (Centre d'Électronique de l'Armement). Elle s'est déroulée du 2/11/98 au 30/9/99.*

Cette convention de recherche avait comme objectif celui de fournir au Celar un outil capable d'évaluer des mesures de performabilité dans un réseau à large étendue. Plus précisément, il s'agissait de calculer la probabilité que le réseau soit capable de transporter une certaine quantité minimale d'information, c'est-à-dire, de satisfaire une demande donnée, partant de la topologie du réseau, de la probabilité de bon fonctionnement des lignes et de leurs capacités. La prise en compte de celles-ci fait qu'il s'agit d'une mesure de type performabilité et non pas de fiabilité classique. Le travail a consisté à étendre le travail de thèse de S. Bulteau[Bul97], réalisé su sein de notre groupe, pour pouvoir traiter des cas plus complexes (voir [48], [47], [46]).

7.2 Scan (Secure Communications in ATMNetworks), 1 99 C 254

Participants : Maryline Laurent, Gerardo Rubino.

[Bul97] S. Bulteau, *Étude topologique des réseaux de communication : fiabilité et vulnérabilité*, thèse de doctorat, université de Rennes 1, novembre 1997.

Résumé : *Il s'agit d'un projet européen Acts, allant de mars 1998 à décembre 1999. Les partenaires sont l'université technologique de Graz, Autriche, les sociétés espagnoles Robotiker et Intelcom, les Postes et Télécomunications autrichiennes (*PTA*), et l'*ENST *Bretagne.*

Ce projet Scan a pour objectif la réalisation d'un prototype de protection des communications sur les réseaux ATM. Il s'agit de réaliser une carte ATM avec des fonctionnalités de cryptographie et intégrant des services de signalisation.

Notre contribution se situe dans ce dernier aspect, sous la forme de modules de gestion de clés et de la politique de sécurité. Elle a donné lieu aux publications [24], [25], [13] et [23].

7.3 Asia (Accelerated Signalling of Internet over ATM), 1 98 C 531

Participants : Hossam Afifi, Ana Minaburo, Landy Rabehasaina, David Ros, Bruno Sericola.

Résumé : *Il s'agit d'un projet* RNRT *précompétitif, d'une durée de deux ans (01/01/1999 - 31/12/2000). Nos partenaires dans le projet sont le Cnet Lannion (chef de file), Airtria (*PME *de Lannion) et* MET *(Matra Ericsson Telecom).*

Le but de ce projet est la conception et la réalisation d'un réseau Internet haute qualité sur ATM. Pour faire face à l'explosion du trafic engendré par l'Internet ainsi qu'à l'émergence sur ce réseau de nouvelles applications multimédia exigeant une haute qualité de service, il devient primordial pour les opérateurs de télécommunications de concevoir un réseau capable non seulement d'écouler le trafic mais aussi d'améliorer sensiblement la qualité de transfert dans l'Internet actuel. Granularité fine des débits, puissance de commutation, flexibilité d'allocation de ressources multidébits et capacité à garantir des objectifs de qualité de service sont les caractéristiques naturelles du réseau ATM, qui en font un réseau fédérateur apte à relever ce défi. Cependant, on constate que l'Internet n'exploite ces potentialités que de manière très limitée. C'est pour améliorer la synergie entre ATM et Internet que le projet Asia se propose, via des concepts de signalisation allégée, de réaliser un couplage efficace entre l'ATM et les protocoles de l'Internet, sans aucune modification de ces derniers. La preuve de ces concepts sera effectuée sur un matériel industriel enrichi de capacités de signalisation allégée et leurs performances seront analysées mathématiquement.

Il s'agit pour nous d'abord de déterminer un modèle d'un réseau ATM doté de capacité de signalisation allégée. Ce modèle sera ensuite simulé dans un premier temps puis étudié de manière analytique après d'éventuelles simplifications. Les résultats de ces travaux permettront de déterminer les performances du réseau en termes de blocage, occupation des liens, trafic écoulé, etc. Notre but est de mettre au point, pour une matrice de trafic et une méthode de routage connues, des algorithmes d'optimisation du rendement du réseau (en terme de trafic écoulé), principalement via des algorithmes de partage de bande passante assurant une certaine équité entre les différents utilisateurs du réseau.

8 Actions régionales, nationales et internationales

8.1 Actions régionales

Nous participons au groupe régional Goëtic, avec des industriels et le Celar (Centre d'Électronique de l'Armement). L'objectif de Goëtic est de promouvoir les coopérations entre partenaires dans les activités de recherche autour des télécommunications et ses principales applications.

Nous travaillons avec le Cnet Lannion et la PME Airtria de Lannion dans le cadre du projet RNRT Asia.

8.2 Actions nationales

L'équipe a organisé l'école d'été RHDM'99 du thème « Réseaux haut débit et multimédia » du GDR ARP (Architecture, Réseaux et parallélisme) du CNRS.

L. Toutain est membre du G6, réseau national travaillant sur la future version du protocole IP (IPv6).

8.3 Actions européennes

L'équipe collabore avec des chercheurs de l'université de Budapest en Hongrie, de l'université polytechnique de Catalogne à Barcelone en Espagne et de l'université de Vienne en Autriche.

8.4 Actions internationales

Nous avons des projets de recherche avec l'université Fédérale de Rio de Janeiro, au Brésil, et avec l'université de Montevideo en Uruguay. Ils concernent l'analyse de modèles pour l'évaluation quantitative de systèmes de télécommunications. Nous travaillons également avec l'université de Queens, Kingston, Canada, sur les mécanismes de contrôle dans les réseaux, et avec l'université d'Arizona sur les processus de Markov.

R. Marie est membre des groupes de travail Ifip 6.3 (Performance of Communication Systems) et 7.3 (Computer system Modeling and Performance Evaluation).

8.5 Visites, et invitations de chercheurs

Le projet a reçu la visite, de début décembre 1998 à fin janvier 1999, du Professeur H. Mouftah, qui est co-responsable du département d'Ingénierie Électrique et Informatique de l'université Queens, Kingston, Canada, et directeur des Magazines IEEE dans le domaine des réseaux. Les thèmes de travail concernent les mécanismes de réservation de bande passante dans Internet.

9 Diffusion de résultats

9.1 Animation de la Communauté scientifique

B. Cousin et L. Toutain participent au thème « Réseaux haut débit et multimédia » du GDR ARP (Architecture, Réseaux et parallélisme) du CNRS.

9.1.1 Activités d'édition

- H. Afifi appartient au corps d'éditeurs de la revue Computer Communications.
- R. Marie est co-éditeur de la revue *Performance Evaluation.*
- G. Rubino est co-éditeur de la revue *Naval Research Logistics.*
- L. Toutain est co-éditeur de la revue IEEE Communications Magazine, pour les articles sur IP. Il est également éditeur dans la collection « Techniques de l'ingénieur » chez Hermès.

9.1.2 Comités de programme

Bernard cousin est membre du comité de programme du congrès francophone « De nouvelles architectures pour les communications ». R. Marie a été membre du comité de programme du 3^{eme} symposium international Numerical Solution of Markov Chains et du comité de programme du 8^{eme} symposium international PNPM'99 (Petri Nets and Performance Models). G. Rubino a été membre du comité de programme de la conférence internationale PDPTA'99 (Parallel and Distributed Processing Techniques and Applications), Las Vegas, juillet 1999. B. Sericola a été membre du comité de programme de la conférence internationale ESS'99 (11th European Simulation Symposium), Erlangen, 24-27 octobre 1999. R. Marie et G. Rubino ont fait partie du comité de programme de la conférence internationale Icil'99 (International Conference on Industrial Logistics), San Petersburg, juillet 1999.

9.1.3 Participation à des colloques, séminaires, invitations

H. Afifi a fait un séminaire à l'université Queens, Canada, sur la téléphonie sur support IP.

R. Marie a fait un exposé à l'université fédérale de Rio de Janeiro sur la communication multicast. Lors de la réunion annuelle du groupe 6.3 (voir 8.4) en août 1999, il a également fait une présentation sur la recherche d'un arbre couvrant partiel pseudo-optimal pour la diffusion multipoint.

M. Molnár a présenté aux Journées Graphes, Combinatoire et Algorithmes, (8 et 10 septembre 1999, Labri, Bordeaux) des exemples de généralisation d'heuristiques de construction de l'arbre optimal de diffusion basées sur la fermeture métrique du problème.

G. Rubino a fait deux exposés à la City University de Hong Kong, sur des techniques d'analyse de modèles de réseaux de télécommunications.

L. Toutain a fait une présentation sur « Réseaux et Multimédia » à la Cité des Sciences, dans un cycle de conférences organisées par l'Inria et la revue La Recherche, en janvier 1999, une présentation sur « QoS dans les réseaux IPv6 » dans le cadre du séminaire Aristote, et une présentation intitulée « IPv6 : the reasons to move » à Interop'99.

9.2 Enseignement

9.2.1 Enseignement universitaire

Les membres de l'équipe ont des responsabilités d'enseignement diverses dans l'environnement local (Ifsic, Cnam Rennes, IUT de Rennes, Insa, ENST de Bretagne, Institut mathématique de Rennes).

Au niveau Bac+5, B. Cousin, R. Marie, G. Rubino, B. Sericola, L. Toutain, donnent différents cours en DEA de probabilités, en DEA d'informatique et en DESS Isa , à l'université de Rennes 1, ainsi qu'à l'ENST Bretagne et à l'Ensai. Les thèmes principaux sont les réseaux, les protocoles, les problèmes de dimensionnement, etc.

G. Rubino a fait un cours sur l'évaluation de performances des réseaux de communication dans l'institut Iti du Caire, en avril, et dans le DEA Modélisation et Ingénierie du Logiciel Scientifique à l'université libanaise de Beyrouth, au mois de juin.

10 Bibliographie

Ouvrages et articles de référence de l'équipe

[1] H. Afifi, O. Elloumi, « Issues in Improving TCP Performance over ATM », *Computer Communications 21*, 1998.

[2] H. Cancela, M. El Khadiri, « A recursive variance-reduction algorithm for estimating communication-network reliability », *IEEE Transactions on Reliability 44*, 4, décembre 1995, p. 595–602.

[3] P. Leguesdron, J. Pellaumail, G. Rubino, B. Sericola, « Transient analysis of the M/M/1 queue », *Advances in Applied Probability 25*, 3, septembre 1993, p. 702–713.

[4] H. Nabli, B. Sericola, « Performability analysis: a new algorithm », IEEE *Transactions on Computers 45*, 4, 1996, p. 491–494.

[5] G. Rubino, B. Sericola, « Sojourn times in Markov processes », *Journal of Applied Probability 26*, 1989, p. 744–756.

[6] G. Rubino, B. Sericola, « A finite characterization of weak lumpable Markov processes. Part II: The continuous time case », *Stochastic Processes and their Applications 45*, 1993, p. 115–126.

[7] G. Rubino, B. Sericola, « Interval availability analysis using denumerable Markov processes. Application to multiprocessor systems subject to breakdowns and repairs », IEEE *Transactions on Computers 44*, 2, Février 1995, p. 286–291, Special Issues on Fault-Tolerant Computing.

[8] L. Toutain, *Réseaux locaux et Internet*, Hermès, 1999.

Articles et chapitres de livre

[9] H. Hébrard, M. Laurent, « Sécurité des technologies internet et intranet: les IPSEC », *Confidentiel Sécurité 52*, janvier 1999.

[10] M. Laurent, O. Paul, P. Rolin, « Solution SAFE du projet Démostène: un système de protection des communications sur les réseaux ATM », *TSI (Technique et Science Informatique) 18*, 16, juin 1999.

[11] M. Laurent, *IPv6 : Théorie et pratique*, Editions O'Reilly, Gisèle Cizault, 1999, ch. 7: Sécurité.

[12] L. Le Ny, B. Tuffin, « Parallélisation d'une combinaison des méthodes de Monte Carlo et quasi-Monte Carlo et application aux réseaux de files d'attente », *RAIRO: recherche Opérationnelle*, 1999.

[13] H. Leitold, R. Posch, E. Areizaga, A. Bouabdallah, M. Laurent, J. M. Mateos, O. Molino, « Security services in ATM networks », *ICON (Interoperable Communication) journal 2/1*, mars 1999, Special issue: Broadband Telecommunication Management.

[14] S. Mahévas, G. Rubino, « Bound computation of dependability and performability measures », *IEEE Transactions on Computers*, À paraître.

[15] H. Nabli, B. Sericola, « Performability analysis for degradable computer systems », *Computers and Mathematics with Applications*, 1999, À paraître.

[16] B. Sericola, B. Tuffin, « A fluid queue driven by a markovian queue », *Queueing Systems - Theory and Application 31*, 3, 1999.

[17] B. Sericola, « Availability analysis of repairable computer systems and stationarity detection », *IEEE Trans. Computers 48*, 11, novembre 1999.

[18] B. Tuffin, « Bounded Normal Approximation in Simulations of Highly Reliable Markovian Systems », *Journal of Applied Probability*, 1999.

Communications à des congrès, colloques, etc.

[19] H. Abdallah, M. Hamza, « Sensitivity analysis of instantaneous transient measures of highly reliable systems », *in: 11th European Simulation Symposium (ESS'99)*, Erlangen-Nuremberg, 1999.

[20] H. Afifi, Y. Ahmed, « A three dimensional lens », *in: Photonic West*, SPIE, San Jose, USA, 1999.

[21] H. Afifi, L. Toutain, « Methods for IPv4-IPv6 transition », *in: SCC'99*, IEEE, Sharm El Sheik, 1999.

[22] A. Bousseta, R. Marie, « DIANA: a help in decision making for an Integrated logistic support », *in: ICIL'99 (International Conference on industrial Logistics)*, St Petersbourg, Russie, juin 1999.

[23] M. Laurent, A. Bouabdallah, C. A. Bouabdallah, H. Leitold, R. Posch, E. Areizaga, J. M. Mateos, « Secure communications in ATM networks », *in: 15th ACSA/ACM Annual Computer Security Applications Conference ACSAC99*, Phoenix, Arizona, décembre 1999.

[24] M. Laurent, C. Delahaye, M. Achemlal, « Security services negotiation through OAM », *in: ATM Forum/99-0335*, New Orleans, Louisiana, juillet 1999.

[25] M. Laurent, V. Rossi, M. Achemlal, « Inconsistencies and missing information in the security specification 1.0 », *in: ATM Forum/99-0336*, New Orleans, Louisiana, juillet 1999.

[26] A. Mokhtar, G. Rubino, « Mutual synergies between Web caches », *in: Internet Applications (5th International Computer Science Conference, ICSC'99)*, L. C.-K. Hui, D. L. Lee (éditeurs), IEEE, Springer Verlag, Hong Kong, décembre 1999.

[27] M. Molnár, « Construction of More Advantageous Multicast Diffusion Trees », *in: Int. Conf. on Dynamic Control and Systems (DYCONS'99)*, Ottawa, Canada, August 1999.

[28] M. Molnár, « Une heuristique distribuée, paramétrable pour le problème de Steiner », *in: 11ème Rencontres Francophones du Parallèllisme (RENPAR'11)*, Rennes, France, juin 1999.

[29] O. Paul, M. Laurent, S. Gombault, « An asynchronous distributed access control architecture for IP over ATM networks », *in: 15th ACSA/ACM Annual Computer Security Applications Conference ACSAC99*, Phoenix, Arizona, décembre 1999.

[30] O. Paul, M. Laurent, « An alternative access control architecture for IP over ATM networks », *in : 14th IFIP Conference on Communication and Multimedia CMS99*, Leuven, Belgique, septembre 1999.

[31] D. Ros, R. Marie, « Estimation of end-to-end delay in high-speed networks by means of fluid model simulations », *in : 13th European Simulation Multiconference*, Varsovie, 1999.

[32] D. Ros, R. Marie, « Loss Characterization in High-Speed Networks Through Simulation of Fluid Models », *in : SPECTS'99 (1999 Symposium on Performance Evaluation of Computer and Telecommunication Systems)*, Chicago, 1999.

[33] M. Tezeghdanti, J. M. Bonnin, B. Cousin, L. Toutain, « Agrégation dans les réseaux MPLS », *in : De nouvelles architectures pour les communications (DNAC'99)*, Paris, France, décembre 1999.

Rapports de recherche et publications internes

[34] H. Abdallah, M. Hamza, « Sensibilité de mesures transitoires instantanées des systèmes informatiques hautement fiables », *Rapport de recherche n° 1232*, IRISA, Rennes, février 1999.

[35] H. Cancela, G. Rubino, B. Tuffin, « MTTF estimation by Monte Carlo methods using Markov models », *rapport de recherche n° 1245*, IRISA, 1999.

[36] R. Marie, M. Molnár, « Arbre couvrant partiel pseudo-optimal pour diffusion multipoint », *rapport de recherche n° 3636*, INRIA, mars 1999, `ftp://ftp.inria.fr/INRIA/publication/RR/RR-3636.ps.gz`.

[37] M. Molnár, « Construction d'arbres de diffusion multicast basée sur une modification de l'heuristique de Kruskal », *rapport de recherche n° 3587*, INRIA, décembre 1998, `ftp://ftp.inria.fr/INRIA/publication/RR/RR-3587.ps.gz`.

[38] D. Ros, R. Marie, « Simulation de modèles fluides pour réseaux haut débit », *Rapport de recherche n° RR-3596*, INRIA, Rennes, décembre 1998, http://www.inria.fr/RRRT/RR-3596.html.

[39] B. Sericola, « Occupation times in Markov processes », *Rapport de recherche n° 3806*, Inria, Rennes, novembre 1999.

[40] B. Tuffin, D. Chen, *SPNP: Stochastic Petri Net Package, Version 6.0, User Manual*, 1999, Remise à jour et correction du manuel de la version 5.0.

[41] B. Tuffin, C. D.S., K. Trivedi, « Comparison of hybrid systems and fluid stochastic Petri nets », *rapport de recherche*, Duke University, Durham, NC, 1999.

[42] B. Tuffin, K. Trivedi, « Implementation of Importance Splitting techniques in Stochastic Petri Net Package », *rapport de recherche*, Duke University, Durham, NC, 1999.

[43] B. Tuffin, « A randomized Quasi-Monte Carlo method for th the simulation of product-form loss networks », *rapport de recherche n° 1246*, IRISA, 1999.

Divers

[44] H. Afifi, J. Bond, L. Toutain, « Using E.164 numbers in IPv6 addresses », avril 1999, Draft IETF Working Group `ngtrans`.

[45] H. Afifi, L. Toutain, « The architecture of the DTI model », mars 1999, Draft IETF Working Group `OPng`.

[46] G. Rubino, « Convention de recherche 1 98 C 531. Mesures de performabilité dans les réseaux à large étendue. Note sur les modèles à composants dépendants. », octobre 1999.

[47] G. Rubino, « Mode d'emploi des programmes liés à la convention de recherche 1 98 C 531. Mesures de performabilité dans les réseaux à large étendue », septembre 1999.

[48] G. Rubino, « Rapport final de la convention de recherche 1 98 C 531. Mesures de performabilité dans les réseaux à large étendue », septembre 1999.