Contrôles d'admission basés sur des mesures : Evaluation et comparaison de solutions existantes

Doreid Ammar, Thomas Begin, Isabelle Guérin-Lassous, Ludovic Noirie

▶ **To cite this version:**

Doreid Ammar, Thomas Begin, Isabelle Guérin-Lassous, Ludovic Noirie. Contrôles d'admission basés sur des mesures : Evaluation et comparaison de solutions existantes. CFIP 2011 - Colloque Francophone sur l Ingénierie des Protocoles, UTC, May 2011, Sainte Maxime, France. inria-00586873

HAL Id: inria-00586873

https://inria.hal.science/inria-00586873

Submitted on 18 Apr 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Contrôles d'admission basés sur des mesures

Evaluation et comparaison de solutions existantes

Doreid Ammar* — **Thomas Begin*** — **Isabelle Guerin-Lassous*** — **Ludovic Noirie****

(*)Université Lyon 1 / LIP (UMR ENS Lyon - INRIA - CNRS - UCBL)
(**)Alcatel-Lucent Bell Labs, Nozay, France[1]

RÉSUMÉ. *Le contrôle d'admission est un mécanisme destiné à prévenir la congestion des réseaux informatiques et à assurer ainsi à tous les flux du réseau un niveau de performances suffisant. Ce travail vise à présenter une évaluation pratique de solutions existantes pour le contrôle d'admission basé sur les mesures dans le cadre des réseaux sémantiques. Ainsi, le réseau, en plus d'acquérir une connaissance sur les caractéristiques du trafic circulant sur chaque lien qui a été préalablement admis, acquiert également une connaissance sur le flux entrant à accepter grâce à l'analyse des premiers paquets de ce flux. Dans ce contexte, nous avons comparé trois solutions appartenant à ce type d'approche en les paramétrant de telle sorte qu'elles aient un objectif identique en termes de taux de perte toléré. Nous avons évalué les performances de chacune de ces solutions par voie analytique et par simulation en les rapportant au contrôle d'admission « idéal ». Les résultats obtenus indiquent que la prise en compte d'un estimateur de l'écart-type sur le débit semble nécessaire à une bonne caractérisation du trafic déjà admis sur ce lien quelles que soient sa nature et son intensité. Néanmoins, ces solutions, utilisant l'écart-type sur le débit, restreignent trop, dans certains cas, le nombre de flux acceptés.*

ABSTRACT. *Admission control aims at preventing computer networks from becoming congested so that accepted flows receive a sufficient level of performance. In this paper, we provide a practical evaluation between existing measurement-based admission controls considering semantic networks. Thus, the network learns a knowledge on on-going traffic of the link as a knowledge on the entering flow thanks to the analysis of the first packets of this flow. In this framework, we compared three solutions belonging to this kind of approach and parameterizing them in a way they achieve identical target in terms of maximum loss rate. We evaluated the solutions' performance using an analytical way or by simulation and compared them to ideal admission control. Our conclusions tend to show that an estimation on standard-deviation of the arrival rates seems necessary to well characterize the traffic already accepted on this link whatever its nature and its intensity. However, these solutions, based on this standard-deviation, are, in some cases, too restrictive in terms of the number of accepted flows.*

MOTS-CLÉS : *contrôle d'admission, mesures, performances, réseaux sémantiques*

KEY WORDS: *admission control, measurement, performance, semantic networks*

1. Ce travail a été soutenu par le projet *Semantic Networking* dans le cadre du laboratoire commun INRIA - Alcatel Lucent-Bell Labs

1. Introduction

Le contrôle d'admission est un mécanisme destiné à prévenir la congestion des réseaux informatiques et à assurer ainsi à tous les flux du réseau un niveau de performances suffisant. Si beaucoup d'études sur le contrôle d'admission ont été réalisées, très peu de solutions, voire aucune, ont été déployées et utilisées sur des réseaux opérationnels. Les opérateurs considèrent, jusqu'ici, que les réseaux sont sur-dimensionnés par rapport aux besoins actuels en communication et ne nécessitent donc pas de contrôle d'admission. Or depuis quelques années, il y a un réel changement dans les usages des réseaux en termes d'applications véhiculées ainsi qu'en nombre. On voit de plus en plus d'applications contraintes en termes de délai, comme par exemple la Téléphonie sur IP, ainsi que d'applications gourmandes en ressources comme par exemple le Streaming Vidéo. La croissance en volume de ces applications commence à poser des problèmes de congestion dans les réseaux sans fil comme, par exemple, celui rencontré par AT&T en été 2010 dans ses réseaux d'accès sans fil dû à une utilisation intensive des iPhones et iPads [lex10]. Avec une utilisation plus massive de la Télévision sur Internet, de la Vidéo à la Demande et avec l'arrivée de la vidéo 3D et/ou très haute définition, les problèmes de congestion pourraient aussi se poser dans les réseaux filaires. La problématique du contrôle d'admission est donc toujours d'actualité.

Il existe différentes approches pour réaliser le contrôle d'admission. Les solutions de contrôle d'admission aux extrémités utilisent généralement des paquets de tests envoyés sur le chemin à emprunter par le flux qui demande à entrer dans le réseau afin d'évaluer la charge et les capacités offertes sur ce chemin [BRE 00b]. Ces approches sont qualifiées de solutions actives car elles injectent du trafic de contrôle dans le réseau pour réaliser le contrôle d'admission. Ce trafic peut, d'une part, avoir un impact sur les performances des flux existants et, d'autre part, ne donne une indication sur l'état du chemin que sur un intervalle de temps réduit, correspondant au temps d'envoi des paquets de test. On distingue également les solutions de contrôle d'admission basé sur la description (*a priori*) du trafic. Ce type de solutions suppose la connaissance de descripteurs de trafic pour tous les flux désirant entrer dans le réseau, mais également pour ceux déjà entrés afin d'estimer la charge courante dans le réseau et d'en déduire la possibilité ou non d'accepter de nouveaux flux [JAM 97b]. Déterminer les descripteurs de trafic qui caractérisent avec précision les profils des flux peut s'avérer être une tâche coûteuse et difficile pour l'utilisateur et l'opérateur. On pourrait également envisager à caractériser par un descripteur de trafic unique l'agrégation de flux résultant du multiplexage réalisé dans le réseau afin de réduire le nombre de descripteurs à maintenir, mais, en pratique, cette opération se révèle difficile à réaliser avec précision. Enfin, il existe les solutions de contrôle d'admission basé sur les mesures. Comme leur nom l'indique, ces solutions utilisent des mesures sur des liens pour estimer les capacités résiduelles offertes par le réseau. Il s'agit donc d'une approche basée sur des mesures passives, contrairement au premier type de solutions, et qui ne nécessite pas la connaissance de descripteurs de trafic pour les flux déjà admis, contrairement au deuxième type de solutions. Ces avantages en font une approche intéressante pour le contrôle d'admission et c'est cette approche que nous considérerons dans toute la suite de cet article.

Plusieurs solutions de contrôle d'admission basé sur des mesures ont été proposées dans la littérature. Ces solutions sont généralement pensées pour fonctionner à l'échelle d'un lien et le contrôle d'admission doit donc être répété à chacun des liens traversés par le flux. Leur mécanisme peut se décomposer en deux parties. Premièrement, des opérations de mesure sur le trafic déjà admis permettent de le caractériser et d'en déduire un certain nombre de métriques (e.g., la capacité résiduelle du lien). Deuxièmement, un algorithme, composé d'une (ou plusieurs) opération(s) de test, permet d'évaluer si, étant donné le débit du flux cherchant à entrer, supposé connu, le réseau peut correcte-

ment « absorber » ce nouveau flux tout en maintenant un niveau de performances suffisant à tous les flux. Dans le cas le plus simple, l'algorithme peut se réduire à s'assurer que le débit du flux cherchant à entrer est inférieur à la capacité résiduelle du lien [JAM 97b]. Les solutions existantes pour le contrôle d'admission basé sur les mesures diffèrent par la nature des mesures, par les hypothèses faites sur le trafic entrant et par l'algorithme d'admission.
Dans ce papier, nous positionnons notre étude sur les contrôles d'admission dans le contexte des *réseaux sémantiques* [NOI 09]. De tels réseaux acquièrent progressivement et par eux-mêmes une connaissance du trafic qui est transporté et raisonnent au niveau des flux en fonction de cette connaissance dans le but de pouvoir s'autogérer. Ces réseaux sont capables d'apprendre les caractéristiques du trafic non pas grâce à une connaissance explicite sur les flux entrants, mais en analysant leurs caractéristiques intrinsèques. Dans le contexte d'un contrôle d'admission, le réseau en plus d'acquérir une connaissance sur les caractéristiques du trafic circulant sur chaque lien qui a été préalablement admis comme c'est le cas pour n'importe quel contrôle d'admission basé sur les mesures, acquiert également une connaissance sur le flux entrant à accepter. Cette connaissance n'est pas donnée par une signalisation explicite dans le réseau, mais acquise grâce à l'analyse des premiers paquets de ce flux, notamment une estimation du débit de ce flux entrant[1]. Dans ce contexte, les premiers paquets d'un flux jouent le rôle de signalisation implicite pour l'admission définitive de ce flux dans le réseau. Dans cet article, nous évaluons et comparons trois solutions existantes pour le contrôle d'admission basé sur les mesures dans le cadre des réseaux sémantiques. L'originalité de ce travail est double. Premièrement, nous avons relâché l'hypothèse sur la connaissance du flux entrant. A la différence des travaux de comparaison précédents [JAM 97b, BRE 00a, NEV 08], nous ne supposons aucune connaissance explicite *a priori* sur le flux entrant, ni sur le trafic de fond, qu'elle soit directe ou indirecte (par l'existence d'un seau à jetons placé en amont du réseau). Deuxièmement, nous avons comparé les trois solutions en les paramétrant de telle sorte qu'elles aient un objectif identique exprimé en termes de performances. Nous avons choisi le taux de pertes. A notre connaissance, aucun autre travail dans la littérature n'a comparé ces méthodes dans un tel contexte. Cet article est organisé de la façon suivante : un état de l'art sur le contrôle d'admission basé sur les mesures est donné dans le chapitre 2 ; les solutions de contrôle d'admission retenues pour l'étude sont décrites avec plus de précision dans le chapitre 3 ; enfin le chapitre 4 décrit le cas d'étude à partir duquel nous avons mené notre évaluation ainsi que les résultats obtenus.

2. État de l'art

Dans cet état de l'art, nous ne nous intéressons qu'au contrôle d'admission basé sur les mesures puisque seule cette approche est considérée dans ce travail. Les auteurs de [GUE 91] ont été les premiers à proposer la notion de *capacité équivalente* utilisée dans plusieurs solutions de contrôle d'admission. La capacité équivalente (du trafic) d'un lien, notée $C(\epsilon)$, est telle que, en régime stationnaire, le taux d'arrivée sur ce lien excède $C(\epsilon)$ avec une probabilité au plus de ϵ. Dans les contrôles d'admission utilisant la notion de capacité équivalente d'un lien, l'algorithme d'admission s'assure que la capacité équivalente actuelle du lien à laquelle s'ajouterait le flux cherchant à entrer n'excède pas la capacité nominale du lien. La formule de la capacité équivalente donnée dans [GUE 91] repose sur l'hypothèse que le taux d'arrivée des flux suit une distribution Normale ainsi que sur un modèle sans buffer. Floyd, dans [FLO 96], a proposé une autre formule pour la capacité équivalente en se basant sur les bornes de "Hoeffding". Dans [GEO 08], les auteurs se basent aussi sur la for-

1. Cette propriété implique qu'un flux peut être refusé bien que ses premiers paquets aient été transmis.

mule de la capacité équivalente donnée dans [GUE 91] mais intègrent un facteur d'admission (APF - Admission Policy Factor) dans leur algorithme d'admission afin de moduler le niveau de rigueur de l'admission que l'opérateur désire appliquer en termes de taux de perte sur les paquets. Ces trois solutions nécessitent une mesure du taux d'utilisation ou du débit courant du lien pour fonctionner. Dans [JAM 97a], les auteurs intègrent la contrainte de délai pour certains flux dans leur contrôle d'admission. Pour cela, l'algorithme nécessite, en plus d'une mesure du taux d'utilisation courant du lien, une mesure du délai (d'attente) maximal enregistré sur ce lien. Leur algorithme d'admission se décompose en deux parties : un test relatif au taux d'utilisation courant du lien et un test pour le délai. Les auteurs de [QIU 01] ont cherché à améliorer les travaux de [JAM 97a] en proposant une autre mesure du taux d'utilisation du lien afin de mieux caractériser le trafic circulant sur ce lien ainsi qu'un algorithme d'admission plus flexible que celui de [JAM 97a] où les paramètres de QoS peuvent être directement contrôlés sans fixer au préalable des valeurs seuils comme dans [JAM 97a]. Notons que toutes les solutions citées précédemment ont été pensées et évaluées en supposant une connaissance du débit crête des flux entrant, soit parce qu'il est donné, soit parce qu'il peut être déduit des paramètres connus du seau à jetons appliqué en entrée du lien.
Quelques travaux ont cherché à comparer ces différentes solutions entre elles. Dans [JAM 97b], une comparaison de trois solutions de contrôle d'admission basé sur des mesures a été réalisée sous simulation. Les résultats obtenus montrent, entre autres, qu'une version simplifiée de la solution de [JAM 97a] (n'intégrant pas la contrainte de délai) obtient une meilleure utilisation du lien au prix d'un petit taux de perte comparé à la solution de [FLO 96] qui, elle, n'induit aucune perte de paquet. Ces mêmes auteurs étendent leurs travaux dans [BRE 00a] avec une comparaison de six solutions de contrôle d'admission basé sur des mesures réalisée sous NS2. En faisant varier les paramètres utilisés dans les tests d'admission des solutions étudiées, ils montrent que toutes ces solutions atteignent le même ensemble de valeurs sur le compromis taux d'utilisation du réseau et taux de pertes sur les flux. Les auteurs concluent sur le fait que la difficulté réside dans les valeurs à donner aux paramètres des contrôles d'admission afin d'obtenir un compromis taux d'utilisation - taux de pertes donné car ces valeurs ne correspondent pas au final aux performances réellement obtenues sur le réseau et les flux et qu'elles sont donc, par conséquent, difficiles à déterminer *a priori*. Dans [NEV 08], les auteurs comparent trois solutions pour divers types de flux entrant. Malgré le nombre et la diversité des scénarios traités dans ces articles, ces travaux, à l'instar des évaluations présentées dans les articles décrivant les solutions de contrôle d'admission, supposent que le trafic est lissé en entrée par un seau à jetons dont les paramètres sont connus. Dans notre étude, nous supposons aucune connaissance *a priori* sur les flux entrant qu'elle soit directe ou indirecte (par l'existence d'un seau à jetons placé en amont du réseau).

3. Solutions Considérées

Dans notre étude, nous considérons trois solutions de contrôle d'admission basé sur des mesures : (1) la solution appelée *Somme Mesurée* [JAM 97a, JAM 97b] car son test d'admission basé sur le taux d'utilisation est simple ; (2) une solution basée sur la notion de *Capacité Equivalente* telle que donnée dans [GUE 91] afin de tester les performances offertes par cette notion ; (3) la solution *Enveloppes du Trafic Agrégé* [QIU 01] car elle intègre une caractérisation plus fine de la variation du trafic en considérant plusieurs échelles de temps. Notons que dans leur forme originale, toutes ces solutions supposent que des flux de débit crête r connu cherchent à entrer dans un lien de communication avec une capacité de transmission C.

3.1. *Somme Mesurée (S.M.)*

Jamin et al. présentent dans [JAM 97b] un contrôle d'admission qui se base sur une mesure de la charge existante sur un lien, notée R. Lorsqu'un flux cherche à entrer sur un lien en demandant un débit crête r, l'algorithme vérifie la condition suivante :

$$R + r \leq \nu C \tag{1}$$

où ν est un paramètre permettant de fixer l'utilisation maximale du lien attendue. Si la condition est vérifiée alors le flux est accepté. La mesure sur la charge courante du lien est réalisée sur une fenêtre de mesure T et est répétée sur chaque fenêtre de mesure. Cette fenêtre de mesure est elle-même découpée en périodes d'observation de durée identique. Le débit moyen du trafic sortant du lien est calculé sur chaque *période d'observation* et conservé en mémoire. A la fin d'une fenêtre de mesure, la charge courante est considérée comme étant le maximum des débits moyens obtenus sur les périodes d'observation constituant cette fenêtre de mesure. C'est cette valeur qui est utilisée dans le test d'admission, s'il doit être appliqué, lors de la fenêtre de mesure suivante. Il faut aussi noter que la valeur de la charge courante peut aussi être modifiée à l'intérieur d'une fenêtre de mesure. C'est le cas lorsque le débit moyen calculé sur une *période d'observation* est supérieure à la charge courante utilisée dans la fenêtre de mesure associée ou lorsqu'un nouveau flux est accepté. La charge courante du lien est alors modifiée à l'intérieur de la fenêtre de mesure et prend comme valeur soit le débit moyen qui vient d'être calculé sur la *période d'observation*, soit la charge courante auquel s'ajoute le débit du flux entrant. Il faut noter que les débits moyens calculés sur les périodes d'observation sont toujours conservés en mémoire et ce sont ces valeurs qui sont utilisées pour déterminer la charge courante à la fin d'une fenêtre de mesure.

3.2. *Capacité Equivalente (C.E.)*

Dans [FLO 96], *Floyd* présente une solution de contrôle d'admission basée sur l'estimation de la capacité équivalente pour un ensemble de flux. Un nouveau flux est admis sur un lien si la somme de son débit crête, r, et de la capacité équivalente du lien, $C(\epsilon)$, est inférieure ou égale à la capacité nominale du lien, C. Plus formellement, cette condition s'exprime comme :

$$C(\epsilon) + r \leq C \tag{2}$$

Le point critique de cette méthode repose sur l'estimation de la capacité équivalente, $C(\epsilon)$. Dans notre cas d'étude, nous avons choisi la formule de la capacité équivalente donnée dans [GUE 91] car elle est plus simple à évaluer dans notre cadre. La capacité équivalente proposée dans [GUE 91] est une fonction affine du débit moyen du trafic agrégé, noté $\hat{r}$, et de son écart-type, σ :

$$C(\epsilon) = \hat{r} + \alpha.\sigma, \text{avec } \alpha = \sqrt{2\ln\frac{1}{\epsilon} + \ln\frac{1}{2\pi}}, \tag{3}$$

où ϵ est la probabilité de violation de la capacité équivalente attendue.
Afin de "lisser" la mesure du débit moyen du trafic agrégé, $\hat{r}$, l'auteur suggère de la définir comme une moyenne glissante exponentielle mise à jour après chaque fenêtre de mesure T, $\hat{r} = (1-\omega).\hat{r} + \omega.R$ où R correspond au débit moyen du trafic sortant du lien calculé sur la fenêtre de mesure T et ω est un réel compris entre 0 et 1. Comme rien n'était recommandé par les auteurs sur le calcul de σ, nous avons décidé de le déterminer à partir des M dernières mesures de R.

3.3. *Enveloppes du Trafic Agrégé (Env.)*

L'opération de mesure du contrôle d'admission proposée dans [QIU 01] vise à caractériser le débit du trafic agrégé par des enveloppes sur le débit crête. Les mesures se font sur une fenêtre de mesure de longueur T découpée en périodes d'observation de durée identique. Au sein d'une fenêtre de mesure, les mesures des débits crêtes se font sur différentes échelles de temps : R_k^m correspond au débit maximal obtenu sur une échelle de temps k, égale à k périodes d'observation, dans la m^{eme} fenêtre de mesure. A partir de là, l'estimateur du débit du trafic agrégé, ainsi que la variance sur ce débit, est déterminé sur les M dernières fenêtres de mesure comme suit : $\overline{R}_k = \sum_{m=1}^{M} \frac{R_k^m}{M}$ et $\sigma_k^2 = \frac{1}{M-1} \sum_{m=1}^{M} (R_k^m - \overline{R}_k)^2$. L'algorithme d'admission est sujet à deux tests : l'un à court terme qui vérifie qu'aucun paquet n'est trop retardé, et l'autre à long terme qui vérifie que la capacité du lien n'est pas violée avec le flux demandant à entrer. Dans cet article, nous limitons l'algorithme d'admission au seul test à long terme (i.e. en utilisant une seule période d'observation de longueur T) puisque nous cherchons uniquement à comparer les contrôles d'admission dans leur capacité à respecter un taux de perte donné. Dans ce cadre, un nouveau flux avec un débit crête de r est admis sur un lien de capacité C si :

$$\overline{R}_T + r + \alpha_E \sigma_T \leq C \tag{4}$$

où α_E est une constante spécifiant le degré de confiance que nous relions au taux de perte.

4. Evaluation

4.1. *Quel objectif ?*

L'évaluation de performances d'un contrôle d'admission peut traiter de différents aspects. On peut considérer le surcoût en CPU ou en mémoire pour les nœuds du réseau, la simplicité de configuration, la pertinence/qualité des décisions prises, etc. Bon nombre des travaux comparant les contrôles d'admissions entre eux ont visé à quantifier, pour un scénario expérimental donné, le taux d'utilisation atteint par le lien en fonction du taux de perte. Les résultats obtenus tendent à montrer que les différents contrôles d'admission testés suivent des comportements très semblables. En considérant le lien observé comme l'état stationnaire d'une file monoserveur à capacité finie dans laquelle les temps d'inter-arrivées et les temps de service suivent un processus arbitraire (i.e. une file *G/G/1/K*), il apparaît clairement que la relation entre taux d'utilisation et probabilité de rejet ne peut être que structurellement la même pour tous les contrôles d'admission. Ainsi, il nous a semblé plus pertinent dans cet article de s'intéresser surtout au couplage entre la configuration d'un contrôle d'admission et la pertinence de ses décisions. Plus précisément, nous souhaitons mettre en lumière la capacité de chacun des trois contrôles d'admission présentés précédemment à atteindre le taux d'utilisation maximale du lien tout en respectant une contrainte donnée sur le taux de perte. Dans ce travail, nous considérons deux valeurs possibles pour le taux de perte toléré, $Pr : 10^{-2}$ et 10^{-4}.
Dans ce contexte, le contrôle d'admission *« idéal »* est donc clairement défini. Il permet d'accepter le maximum de flux sur le lien, et donc d'atteindre le taux d'utilisation maximal, tout en assurant que le taux de perte subi par chacun des flux reste inférieur à un seuil donné. Ainsi, pour tous nos résultats, nous ferons apparaître en plus des trois contrôles d'admission considérés le comportement du contrôle d'admission « idéal ».

4.2. *Scénarios considérés*

Nous considérons un lien de capacité C égale à 10 Mbps. La taille de la file à l'entrée de ce lien est fixée à 20 ms, soit de 131 paquets car nous considérons que tous les paquets sont de longueur

190 octets. La discipline de service de la file est FIFO (*First In First Out*), les pertes surviennent lorsqu'un paquet arrivant trouve la file pleine (*Drop-Tail*) et le taux d'erreur (*Bit Error Rate*) est supposé nul.
Les flux entrants et soumis au contrôle d'admission sont de type CBR. Ils représentent des flux audio avec un débit de 64 Kbps et des paquets transportant 190 octets, ce qui correspond à l'utilisation du codec G.711. Afin de tenir compte des variations possibles de l'état du réseau, le délai inter-paquets est déterminé par à une constante à laquelle est ajoutée une variable aléatoire prise dans une distribution Normale tronquée[2] au lieu d'une simple constante comme c'est le cas pour un flux CBR "brut". Une originalité de notre étude est que les caractéristiques du flux entrant ne sont pas connues *a priori* mais découvertes par le contrôle d'admission. L'estimation du débit moyen des flux CBR injectés est réalisé après que 20 de leurs paquets soient entrés dans le lien.
Clairement, les décisions prises par un contrôle d'admission sont toujours étroitement liées au trafic agrégé circulant sur le lien et précédant l'arrivée du nouveau flux injecté. Par la suite, nous appellerons ce trafic agrégé, le *trafic de fond*. Il n'existe pas actuellement de modèle universel pour représenter le trafic de fond. Ceci s'explique par le fait que les profils des flux et par conséquent le profil du trafic agrégé circulant dans un réseau varie fortement selon le type de réseau et l'emplacement du lien considérés. Dans les travaux de comparaison existants, comme [JAM 97b, BRE 00a, NEV 08], le trafic de fond transitant sur un lien à l'arrivée d'un nouveau flux correspond à l'agrégation des flux précédemment acceptés ayant tous le même profil. Seule l'étude de [BRE 00a] considère une agrégation de flux ayant des profils hétérogènes mais tous ces flux sont lissés en entrée par le même seau à jetons. Contrairement à ces travaux, notre étude considère diverses conditions possibles du trafic de fond. Plus précisément, le trafic de fond est composé d'une source Poisson ou d'une source PPBP[3] (*Poisson Pareto Burst Process*) [ZUK 03] avec intensité moyenne comprise entre 1 et 7 Mbps et émettant des paquets de taille des paquets 190 octets également, à laquelle s'ajoutent les flux CBR admis par le contrôle d'admission. Dans notre étude, à l'arrivée d'un nouveau flux sur un lien, le trafic de fond sur ce lien n'est donc pas seulement une agrégation de flux individuels acceptés (et ayant le même profil) comme c'est le cas dans les autres études, mais un trafic de fond initial dont on peut maîtriser les caractéristiques plus les flux individuels acceptés par le contrôle d'admission.
Bien qu'étant de même intensité, les propriétés statistiques de ces processus, notamment leur degré d'autocorrélation, diffèrent largement. Comme le montre la Figure 1 , le degré d'autocorrélation est nul pour une source Poisson, modéré pour l'agrégation de 100 flux CBR indépendants ou pour l'agrégation de 20 flux On/Off Pareto indépendants et important pour une source PPBP. Cette approche nous permet donc de tester les solutions de contrôle d'admission sous une diversité de trafic peu explorée dans les études précédentes, puisque seuls les flux On/Off Pareto étaient considérés jusqu'ici pour générer du trafic dépendant à longue portée.

4.3. *Calibrage des contrôles d'admission en fonction d'un taux de perte visé*

Nous détaillons à présent la configuration des contrôles d'admission. Comme nous l'avons dit précédemment, nous les avons calibrés de façon à respecter un objectif sur le taux de perte maximal toléré, Pr. Pour la méthode *S. M.*, en suivant l'analyse proposée par les auteurs, nous avons choisi la

2. Cette distribution est centrée en 0, avec un coefficient de variation de 0.167.
3. Le processus PPBP représentent le comportement d'une infinité de sources On-Off indépendantes avec des durées On distribuées selon une loi de Pareto, avec une durée moyenne de 200 ms et un paramètre de *Hurst*, $H = 0.7$. Chaque source génère du trafic CBR avec un débit fixe de 1 Mbps.

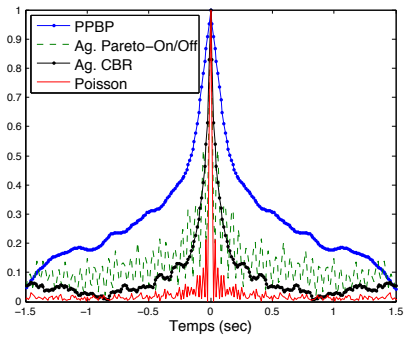


Figure 1. *Fonction d'autocorrélation pour une source Poisson, pour une source PPBP, pour une superposition de 100 flux CBR indépendants et pour une superposition de 20 flux On/Off Pareto.*

	Somme Mesurée	Capacité Equivalente	Enveloppes
Débit agrégé	R	$\hat{r}$	$\overline{R_T}$
Historique	Une seule fenêtre de mesure	Moyenne glissante exponentielle	20 dernières fenêtres de mesure
Écart-type	*Non mesurée*	σ	σ_T
Historique	*Non mesurée*	20 dernières fenêtres de mesure	20 dernières fenêtres de mesure
Fenêtre de mesure	$T = 4$ s *période d'observation* de 200 ms	$T = 200$ ms	$T = 200$ ms
$Pr : 10^{-2}$	$\nu = 0.9543$	$\alpha = 2.7152$	$\alpha_E = 2.325$
$Pr : 10^{-4}$	$\nu = 1.0045$	$\alpha = 4.0722$	$\alpha_E = 3.620$

Tableau 1. *Synthèse des différents paramètres utilisés dans les solutions étudiées*

valeur de ν comme étant le rapport du taux moyen d'arrivée sur le taux moyen de service produisant un taux de perte Pr dans une file *M/M/1/K* avec K égale à 131 paquets ici.
Pour la méthode *C. E.*, la valeur de ϵ représente la probabilité que le taux d'arrivée instantané du trafic agrégé modélisé par un processus Gaussien dépasse la capacité équivalente. Les auteurs ne fournissent qu'une plage de valeurs possibles concernant le choix de la valeur à donner à ϵ. En supposant que cette probabilité s'apparente à celle d'avoir la file pleine (ce qui serait le cas pour une taille de file égale à 1) et que les probabilités vues à l'arrivée des paquets dans la file sont celles à tout instant en régime stationnaire (ce qui serait le cas si les instants d'arrivées des paquets dans le lien suivent un processus de Poisson), la probabilité ϵ représente également la probabilité de rejet d'un paquet. Ainsi, nous avons fixé la valeur de ϵ égale à Pr et nous en avons dérivé la valeur de α.
Enfin, pour la méthode *Env.*, en modifiant la valeur du degré de confiance, α_E, on détermine la probabilité qu'aucune perte ne soit observée pour l'ensemble des flux entrant. Nous approchons la valeur de cette probabilité à celle d'avoir un taux de perte égal à Pr pour tous les flux acceptés (ce qui est toujours le cas si le degré de confiance estimé est vérifié). Le tableau 1 récapitule l'ensemble

des valeurs des paramètres choisis pour les différentes solutions testées.

4.4. *Performances comparées*

Dans cette section, nous évaluons, par voie analytique quand c'est possible et par simulation sinon, les performances de chacun des 3 contrôles d'admission pour différentes conditions de trafic de fond en les comparant au contrôle d'admission idéal. Notre démarche est la suivante. Les instants d'arrivée des flux CBR suivent un processus de Poisson avec une moyenne de quatre arrivées de flux par seconde. Lorsqu'un flux est accepté, il transmet des paquets pendant toute la durée de la simulation. Dès l'instant où un flux CBR entrant se voit refuser l'accès au lien, nous considérons que l'utilisation maximale du lien pour ce contrôle d'admission a été atteinte. Rappelons que nous avons paramétré chacun des contrôles d'admission avec l'objectif d'un taux de perte toléré égal à Pr. En plus de la déviation en pourcents sur le nombre maximal de flux CBR acceptés par rapport au contrôle d'admission idéal, nous présentons le taux de perte réellement subi par les flux pour ce niveau d'utilisation. Les intervalles de confiance représentés sur les figures ont été calculés à partir de 7 réplications indépendantes pour un degré de confiance de 95%.

4.4.1. *Trafic de fond initial modélisé par une source Poisson*

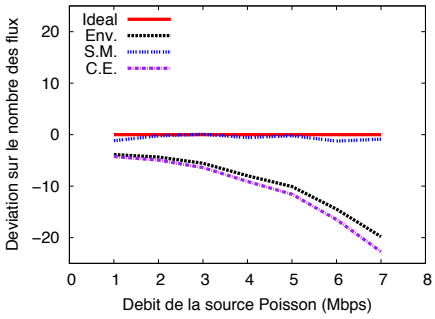


Figure 2. *Déviation sur le nombre de flux acceptés par rapport à un contrôle d'admission « idéal » pour* Pr=10^{-2}

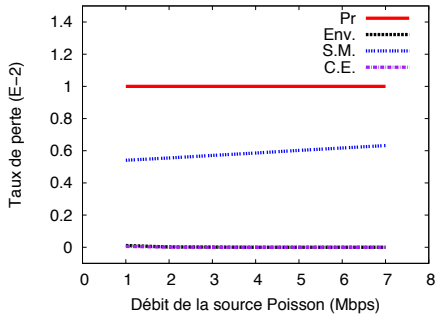
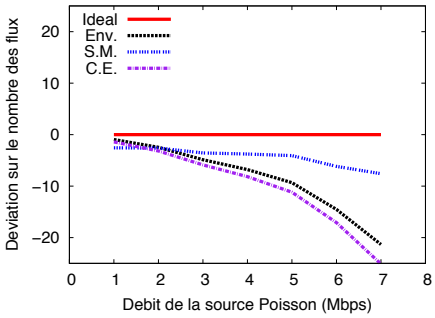


Figure 3. *Évolution du taux de perte pour* Pr=10^{-2}

Pour démarrer, nous considérons que le taux de perte maximal toléré, Pr, vaut 10^{-2}. Le nombre de flux idéalement admis est évalué analytiquement en déterminant le nombre maximum de flux CBR qui peuvent entrer dans une file *G/G/1/K* tout en maintenant le taux de perte inférieur à Pr. Nous avons choisi les paramètres des lois d'inter-arrivée et de service de façon à ce que le taux moyen des arrivées et le temps de service moyen et sa variance reproduisent ceux issus de la combinaison de la source Poisson avec les flux CBR. Pour évaluer le nombre de flux CBR que peuvent admettre chacun des contrôles d'admissions, nous avons simplement fait appel aux formules (1), (2) et (4) en profitant du fait que la variance des flux CBR, aux perturbations près, est nulle et que celle d'un flux Poisson est connue. Pour évaluer le taux de perte associé, nous l'avons approché par celui observé dans une file *G/G/1/K* à ce niveau d'utilisation. Nous avons également implanté ces scénarios dans le simulateur NS-3, et les résultats obtenus concordent avec ceux obtenus analytiquement. La Figure 2 présente, en fonction de l'intensité du trafic de fond initial, la déviation sur le nombre



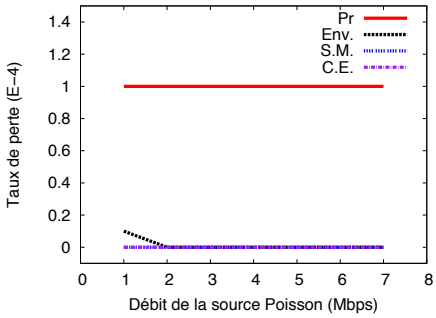
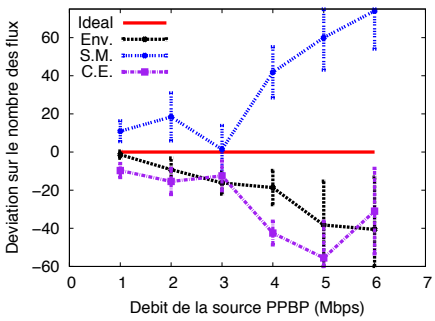


Figure 4. *Déviation sur le nombre de flux acceptés* **Figure 5.** *Évolution du taux de perte pour* Pr=10^{-4} *par rapport à un contrôle d'admission « idéal » pour* Pr=10^{-4}

total de flux CBR acceptés pour chacun des 3 contrôles d'admission par rapport au contrôle d'admission idéal. Dans cet exemple, nous observons que les écarts observés restent relativement faibles (inférieur à 10%) pour des intensités du trafic de fond initial généré par la source Poisson allant jusqu'à environ 5 Mbps. Il n'est pas surprenant que les résultats des contrôles d'admission soient meilleurs pour des faibles niveaux de charge du trafic Poisson, car les aspects aléatoires dans les arrivées des paquets tendant à se réduire, l'estimateur du débit moyen et de sa variance tendent donc à être plus fiables. Comme le montre la Figure 3, lorsque le trafic de fond initial est modélisé par une source Poisson, les flux CBR acceptés éprouvent un taux de perte très inférieur à 10^{-2} quels que soient l'intensité du trafic de fond et le contrôle d'admission considéré.
Nous avons également répété ces tests pour une valeur de Pr égale à 10^{-4}. Les résultats obtenus, présentés dans les Figures 4 et 5, sont qualitativement semblables à ceux obtenus pour $Pr = 10^{-2}$. Dans les simulations, nous avons observé que, pour certaines réalisations, le taux de perte pour la solution *S.M.* dépasse la valeur Pr, allant jusqu'à des valeurs proches de 5×10^{-3}.

4.4.2. *Trafic de fond initial modélisé par une source PPBP*



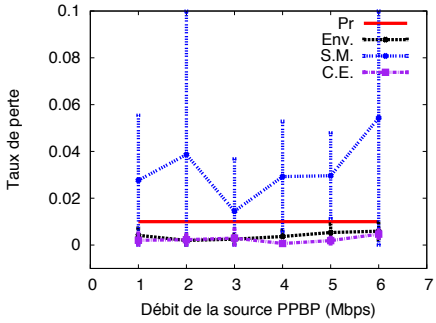


Figure 6. *Déviation sur le nombre de flux acceptés* **Figure 7.** *Évolution du taux de perte pour* Pr=10^{-2} *par rapport à un contrôle d'admission « idéal » pour* Pr=10^{-2}

A présent, le trafic de fond initial est composé d'une source PPBP. Contrairement à une source Poisson, une source PPBP présente un degré d'auto-corrélation important (cf. Figure1, Section 4.2). A cause de la complexité de ce modèle de trafic, le nombre maximal de flux CBR acceptés sur le lien est évalué uniquement par simulation et nous l'avons comparé à celui préconisé par un contrôle d'admission idéal. Nous avons également évalué le taux de perte réellement subi par les paquets sur le lien pour chacun des contrôles d'admission une fois tous les acceptés .
Pour un objectif de perte toléré $Pr = 10^{-2}$, la Figure 6 montre que cette fois-ci la solution *S.M.* admet un nombre sensiblement trop important de flux CBR, surtout lorsque l'intensité de la source PPBP augmente. A l'inverse, les solutions *Env.* et *C.E.* autorisent elles un nombre de flux CBR inférieur à celui du contrôle d'admission idéal à circuler sur le lien. Cet écart est d'autant plus grand que le débit de la source PPBP est important. Nous pensons que cet écart résulte du fait que seuls *Env.* et *C.E.* prennent en compte un estimateur de l'écart-type sur le débit courant dans leur algorithme d'admission. Comme nous l'expliquons en Annexe A, il est bien plus difficile d'inférer à partir de mesures le débit réel moyen d'une source PPBP que celui d'une source Poisson quelle que soit l'échelle de temps considérée. En introduisant un estimateur sur l'écart-type du débit courant, les solutions *Env.* et *C.E.* tendent à mieux faire face aux variabilités intrinsèques de la source PPBP. Le taux de perte réellement subi sur le lien à utilisation maximale autorisée par chacun des contrôles d'admission est représenté sur la Figure 7. Nous observons que les solutions *Env.* et *C.E.* permettent toutes les deux de garantir un taux de perte inférieur à Pr quelle que soit l'intensité de la source PPBP, tandis que la solution *S.M.*, elle, ne satisfait jamais à cette contrainte. Enfin, notons que pour un objectif sur le taux de perte [4] de $Pr = 10^{-4}$, aucun contrôle d'admission, y compris l'idéal, n'est en mesure d'accepter des flux CBR au-delà de 3 Mbps.

5. Conclusion

Dans le contexte des réseaux sémantiques, nous avons comparé trois solutions de contrôle d'admission basé sur les mesures en (1) ne supposant aucune connaissance explicite *a priori* sur les flux entrants, et (2) en les paramétrant de telle sorte qu'elles aient un objectif identique en termes de taux de perte toléré. Nous avons évalué les performances de chacune de ces solutions par voie analytique et par simulation en les rapportant au contrôle d'admission « idéal ». Nous avons considéré diverses conditions possibles du trafic de fond. Ainsi, le trafic de fond est composé d'une source Poisson ou d'une source PPBP (*Poisson Pareto Burst Process*), à laquelle s'ajoutent progressivement les flux entrants admis par le contrôle d'admission. Les résultats obtenus indiquent que la prise en compte d'un estimateur de l'écart-type sur le débit, comme le font certaines solutions, semble nécessaire à une bonne caractérisation du trafic déjà admis sur ce lien quelles que soient sa nature et son intensité. Toutefois, aucune solution testée n'est pleinement satisfaisante pour un opérateur car bien que certains satisfont à l'objectif sur le taux de perte maximal toléré, elles restreignent trop le nombre de flux acceptés, impliquant ainsi une sous-utilisation des capacités de transmissions de l'opérateur.

6. Bibliographie

[BRE 00a] BRESLAU L., JAMIN S., SHENKER S., « Comments on the Performance of Measurement-Based Admission Control Algorithms », *Infocom*, 2000, p. 1233–1242.

4. La grande taille des intervalles de confiance s'explique par le fait que le nombre de flux acceptés varie selon les réalisations du simulateur

[BRE 00b] BRESLAU L., KNIGHTLY E. W., SHENKER S., STOICA I., ZHANG H., « Endpoint admission control : architectural issues and performance », *Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, SIGCOMM '00, 2000, p. 57–69.

[FLO 96] FLOYD S., « Comments on Measurement-based Admissions Control for Controlled-Load Services », rapport, 1996.

[GEO 08] GEORGOULAS S., TRIMINTZIOS P., PAVLOU G., HO K., « An integrated bandwidth allocation and admission control framework for the support of heterogeneous real-time traffic in class-based IP networks », *Computer Communications*, vol. 31, 2008, p. 129-152.

[GUE 91] GUERIN R., AHMADI H., NAGHSHINEH M., « Equivalent capacity and its application to bandwidth allocation in high-speed networks », *IEEE JSAC*, vol. 9, n° 7, 1991, p. 968-981.

[JAM 97a] JAMIN S., DANZIG P. B., « A measurement-based admission control algorithm for integrated services packet networks », *IEEE/ACM Transactions on Networking*, vol. 5, n° 1, 1997, p. 56–70.

[JAM 97b] JAMIN S., SHENKER S., DANZIG P. B., « Comparison of Measurement-based Admission Control Algorithms for Controlled-Load Service », *Infocom*, 1997.

[lex10] « `http://www.lexpansion.com/high-tech/at-t-sonne-la-fin-des-forfaits-mobiles-internet-illimites_233562.html` », online, June 2010.

[NEV 08] NEVIN A., JIANG Y., EMSTAD P. J., « Robustness Study of MBAC Algorithms », *ISCC*, 2008.

[NOI 09] NOIRIE L., DOTARO E., CAROFIGLIO G., DUPAS A., PECCI P., POPA D., POST G., « Semantic Networking : Flow-Based, Traffic-Aware, and Self-Managed Networking », *Bell Labs Technical Journal*, vol. 14, n° 2, 2009, p. 22-38.

[QIU 01] QIU J., KNIGHTLY E. W., « Measurement-Based Admission Control with Aggregate Traffic Envelopes », *IEEE/ACM Transactions on Networking*, vol. 9, n° 2, 2001, p. 199-210.

[ZUK 03] ZUKERMAN M., NEAME T. D., ADDIE R. G., « Internet Traffic Modeling and Future Technology Implications », *Proceedings of INFOCOM*, 2003.

A. Annexe

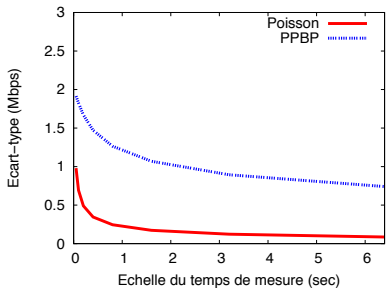


Figure 8. *Evolution de l'écart-type du débit moyen mesuré pour différentes échelles de temps*

Dans la Figure 8, nous avons représenté pour un taux moyen d'arrivées de 4 Mbps de la source Poisson et de la source PPBP, l'écart-type du débit moyen calculé théoriquement pour des échelles de temps grandissantes. On observe que pour le cas d'une source Poisson, l'écart-type sur le débit moyen devient faible dès que l'échelle de temps considérée dépasse $1/3$ de seconde. En revanche pour la source PPBP, même pour des échelles de temps importantes (supérieures à 5 sec.), l'écart-type sur le débit moyen mesuré demeure important (proche de 1). Cette différence illustre la difficulté que rencontrent les contrôles d'admission pour estimer correctement le débit courant du trafic de fond lorsqu'il est modélisé par une source PPBP.