Un mécanisme de contrôle de congestion orienté mesures pour une QdS robuste dans l'Internet

Philippe OWEZARSKI et Nicolas LARRIEU

LAAS–CNRS
7, avenue du Colonel ROCHE
31077 TOULOUSE Cedex 4

Offrir une qualité de service (QdS) garantie est un des problèmes majeurs de l'Internet depuis au moins 10 ans, sans succès. Les propositions faites se sont heurtées à une méconnaissance des caractéristiques du trafic Internet qui présente d'importantes variations de son débit, ce qui rend difficile la mise en place de mécanismes pour garantir une QdS stable. L'objectif de cet article est donc de garantir une QdS robuste, i.e. capable de fournir la QdS demandée en toutes circonstances, notamment en présence d'attaque de déni de service (DdS). Cet article propose d'utiliser notre architecture MBA basée sur des mesures du trafic [LO05], et qui s'adapte aux anomalies et ruptures du trafic en temps réel. En particulier, le mécanisme de congestion MBCC associé à MBA, conçu pour générer des trafics réguliers et optimaux montre qu'il rend l'Internet plus robuste que TCP face aux attaques DdS. Ce résultat est démontré au travers de simulations NS-2.

Mots-clés: Caractérisation de trafic, Measurement Based Networking, contrôle de congestion, QdS, robustesse

1 Introduction

L'Internet est en train de devenir le réseau universel pour tous les types d'informations, du transfert simple de fichiers binaires jusqu'à la transmission de la voix, de la vidéo ou d'informations interactives en temps réel. L'Internet se doit donc de fournir de nouveaux services adaptés à ses applications et aux données qu'elles transmettent. L'Internet doit donc évoluer d'une offre de service "best effort" unique vers une offre multi-services. Au cours des dix dernières années, la QdS est apparue comme un enjeu majeur dans l'Internet. De nombreuses propositions ont été faites comme IntServ ou DiffServ mais jusqu'à présent elles n'ont pas été déployées (ou alors de façon limitée).

En effet, les solutions avancées par la communauté Internet pour la mise en place de services différenciés et/ou garantis ne sont pas celles attendues par les utilisateurs ou les opérateurs. Elles se sont heurtées à la complexité de l'Internet, la multitude de ses interconnexions et à l'hétérogénéité technologique de ses systèmes. De plus, ces solutions se sont aussi heurtées à une méconnaissance des caractéristiques du trafic Internet qui sont très éloignées des modèles généralement considérés pour ce trafic.

Le grand dessein de l'Internet est de devenir un réseau multi-services garantissant des qualités de services (QdS), et ceci en toutes circonstances, y compris les plus difficiles. Parmi celles-ci se trouvent notamment les moments où une attaque de déni de service (DdS), simple ou distribuée, est perpétrée, et pendant lesquels le réseau devient incapable de fournir les services demandés. Cette extrême fragilité de l'Internet souligne le lien étroit qui existe entre sécurité informatique et QdS. Plus généralement, l'Internet présente cette même sensibilité face à tous types de ruptures des caractéristiques de son trafic, qu'elles soient liées à des pannes, des comportements byzanthins de certains éléments du réseau, ou plus simplement à des augmentations fortes mais légitimes du trafic liées par exemple à la diffusion sur le réseau d'un événement populaire. En fait, la frontière entre une attaque DdS et du trafic légitime n'est pas claire, expliquant pourquoi il est si

difficile de combattre ces attaques. Par exemple, peut on considérer qu'un utilisateur qui teste régulièrement l'état de la connectivité vers un ensemble de sites génère une attaque ? Est-ce une attaque de réaliser des tests sur un réseau en générant des quantités importantes de données ?

En fait, il n'existe pas de définition adéquate du déni de service dans la littérature. C'est pourquoi, dans notre travail, les attaques DdS sont incluses dans une famille plus large que nous appelons les "ruptures" de trafic. Les ruptures de trafic incluent tous les exemples précédents, et plus généralement tous les événements qui provoquent un changement significatif dans les caractéristiques du trafic et qui ont un impact négatif sur la QdS fournie par le réseau. L'impact des ruptures peut représenter un manque à gagner important pour les opérateurs ou FAI s'ils ne respectent pas le contrat de service (SLA) passé avec leurs clients. L'Internet est aujourd'hui un réseau d'une importance si stratégique qu'il est lui même devenu une cible des pirates. Dans ce contexte, il est important de mettre en œuvre des méthodes pour mesurer et superviser globalement ce réseau. Elles sont essentielles pour détecter et réagir aux ruptures.

Combattre les attaques DdS est très complexe. Comme nous l'avons mentionné, le simple fait de savoir ce qui constitue une attaque DdS est délicat. De plus, il est difficile de distinguer une attaque DdS d'un trafic qui présente des variations légitimes. Ce sont entre autres les conclusions du projet METROPOLIS[†], ainsi que de nombreux autres projets de métrologie de l'Internet et de son trafic dans le monde qui ont montré que le trafic Internet est loin d'être régulier et qu'il présente des variations importantes dans son débit, et ce à toutes les échelles [PKC96]. Ces projets ont montré notamment que le trafic Internet présente des caractéristiques d'auto-similarité [PW00], de (multi-)fractalité [FGW98] et de dépendance longue (LRD) [ENW96], ce qui signifie dans tous les cas que le trafic peut varier de façon importante.

De telles variations sont préjudiciables à une QdS stable et de haut niveau. [OL04a] analyse l'impact de la variabilité du trafic Internet sur les réseaux. En particulier, ces travaux montrent qu'une telle variabilité est essentiellement due aux mécanismes de contrôle de congestion de TCP (le protocole de transport le plus utilisé dans l'Internet). Ce dernier montre une inefficacité évidente dans la transmission des gros flux sur les réseaux à hauts débits. Or l'évolution récente des usages de l'Internet se traduit notamment par l'explosion des applications Pair-à-Pair (P2P) pour échanger des fichiers comme de la musique ou des films dont les tailles varient de quelques MegaOctets à plusieurs GigaOctets. Face à de tels flux (appelés éléphants), le trafic généré par TCP est extrêmement variable et composé de nombreuses et importantes rafales, que l'on peut comparer à des "oscillations". [OL04a] a montré la relation qui existe entre ces oscillations et la LRD, en particulier que plus la LRD est élevée (i.e. plus le trafic est variable), plus la QdS est dégradée. Ainsi, le trafic Internet actuel a tendance à se comporter comme une attaque DdS, i.e. les rafales de trafic stressent de façon importante le réseau, ce qui conduit à des périodes où les délais augmentent et la fiabilité baisse. Les attaques de Syn flooding, par exemple, telles qu'elles ont été observées dans [Owe03], ou d'UDP flooding, ont finalement le même mode de fonctionnement : leur objectif est d'augmenter la charge de travail des composants du réseau ou des machines d'extrémité pour que le service ne soit plus rendu. Avec les besoins actuels en terme de QdS élevée, il n'est plus nécessaire pour un pirate de bloquer complètement toutes les communications ; il suffit qu'il les ralentisse suffisamment pour que le SLA ne soit plus assuré et la communication inutile. Ainsi, il suffit, en augmentant la charge de travail du réseau, de provoquer l'augmentation des délais et des taux de pertes pour réussir un déni de service.

Etant donnés ces résultats sur l'analyse du trafic, cet article propose d'utiliser des techniques de métrologie / supervision, et d'utiliser en temps réel ces résultats de mesure pour proposer une nouvelle architecture de communication basée sur des mesures (MBA) afin d'adapter les mécanismes de contrôle du trafic aux fréquents changements dans le trafic, et notamment les anomalies et ruptures. Les techniques de mesure et de métrologie sont la base de cette nouvelle approche pour gérer les communications, le trafic et la QdS. Cet article propose ainsi d'utiliser notre architecture MBA, introduite récemment dans [LO05], et son mécanisme de contrôle de congestion associé MBCC, et pour lequel il a été montré dans [LO05] qu'il permettait de générer un trafic plus régulier et une QdS plus élevée et plus stable. Dans cet article, nous allons montrer que MBCC est aussi capable d'améliorer le niveau de QdS et sa stabilité lorsque le trafic présente des ruptures ou des anomalies, et contribue ainsi à améliorer la robustesse du réseau (i.e. il contribue à continuer à fournir une QdS de haut niveau en cas d'anomalies dans le trafic, comme des attaques DdS). Cet article présente donc brièvement notre approche orientée mesures, appelée MBN (Measurement Based Networking) (partie 2), ses principes et son mécanisme de contrôle de congestion associé (partie 3), qui, en

[†] http://www.lip6.fr/metrologie/

plus de limiter le nombre de congestions et de pertes dans le réseau, améliore aussi la régularité du trafic, et optimise l'utilisation des ressources de communication. En particulier, cet article a pour but de montrer que MBCC est très robuste à toute anomalie / rupture du trafic, et plus particulièrement aux attaques DdS (qui apparaissent comme le cas pire pour le maintien d'une QdS garantie de haut niveau). La robustesse de MBCC a été évaluée à l'aide de simulation NS-2. La partie 4 montre ainsi que les attaques DdS ont un impact limité sur la QdS du réseau lorsque MBCC est utilisé à la place de TCP. Les résultats comparatifs entre TCP et MBCC en présence d'attaques sont présentés dans la partie 4. Enfin, la partie 5 conclut le papier.

2 Principes de l'approche MBN

2.1 Définition de l'architecture MBA s'appuyant sur des mesures

Conscients des différents aspects relatifs à la problématique de l'amélioration de la robustesse de la QdS dans l'Internet exposés précédemment, il est aisé de comprendre qu'une solution statique optimale pour l'ensemble des connexions n'est pas possible à établir. Cette constatation nous a amené à proposer l'approche MBN qui permet de réagir en temps réel, globalement, localement et ponctuellement à différents événements se produisant dans le réseau. Ainsi, l'approche MBN nécessite de guetter des changements qui se produisent dans le réseau où le trafic par l'intermédiaire de techniques de mesure des paramètres de QdS et de trafic. La figure 1 décrit comment ces outils de mesure doivent être déployés dans le réseau. Elle détaille le cas plus spécifique d'une connexion MBCC basée sur le principe de l'approche MBN entre une source et une destination, traversant deux SA Internet ainsi que les routeurs de bordure et de coeur. Ces routeurs intègrent le mécanisme MSP (Measurement Signaling Protocol) permettant de mesurer et de signaler aux équipements réseaux concernés ces résultats de mesure faits en différents points du réseau. Il est à noter que les équipements de mesure sont de plus en plus déployés au sein des différents SA Internet à l'heure actuelle. Néanmoins, même si tous les nœuds du réseau ne seront sans doute jamais tous équipés d'outils de mesure, nous pensons qu'en collectant et en utilisant les résultats de mesure des sondes effectivement déployées dans l'Internet, nous pouvons améliorer considérablement la gestion du réseau et de son trafic. Ainsi, MBN est basé sur le principe suivant : les performances et la QdS peuvent être grandement améliorées et même devenir optimales en utilisant des informations de mesure sur le réseau mais même si en certains points du réseau l'information de mesure n'est pas disponible, le réseau doit continuer à fonctionner avec de bonnes performances et une bonne QdS.

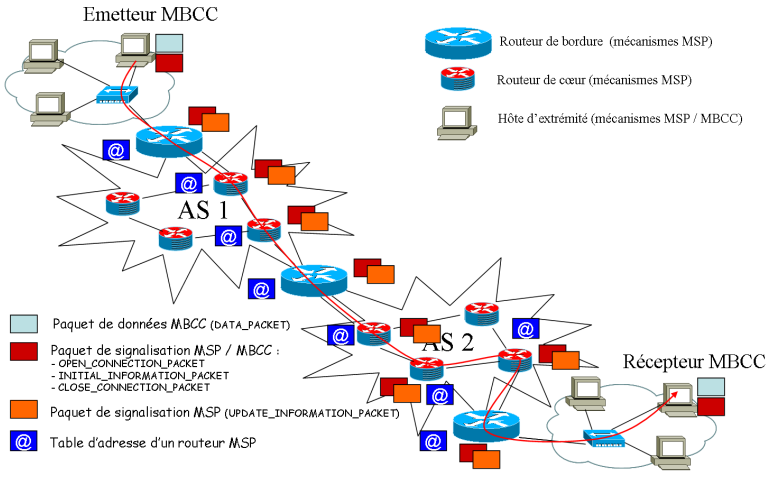


FIG. **1 –** *Déploiement architectural de MBN : exemple du contrôle de congestion MBCC*

La structure administrative de l'Internet nous amène à considérer différentes techniques de mesure. En effet, les mesures intra-domaines peuvent être réalisées par des équipements passifs (systèmes basés sur

SNMP, NetFlow, DAG...) déployés par l'opérateur qui souhaite réaliser une gestion du réseau plus pertinente. Il pourra ainsi disposer d'information sur le niveau de bande passante utilisée et disponible, le nombre de flux actifs dans son réseau, le taux de perte... A l'inverse la mesure du délai sera plus facile en employant des techniques actives. Pour ce qui est de la mesure inter-domaine, le problème est différent. En effet, l'opérateur considéré (qui peut être réduit à un simple utilisateur du réseau) ne disposera pas facilement d'information fiable sur un SA concurrent. Dans ce cas, il est nécessaire d'utiliser des techniques de mesures actives, le principe étant d'émettre des paquets sondes à travers les domaines pour lesquels on souhaite estimer les ressources ou la QdS en observant ce qui arrive à ces paquets sondes.

Ainsi, l'ensemble de ces mesures réalisées en temps réel et signalées à l'ensemble des équipements réseaux concernés (les sources de trafic par exemple), donne une connaissance précise de l'état du réseau et du trafic et permet ainsi de parfaitement adapter leur débit d'émission (dans le cas de MBCC par exemple) aux ressources disponibles. Il est important de noter qu'un aspect primordial de MBN à trait à la définition d'un protocole permettant de signaler les informations de mesure dans le réseau à la fois en intra-domaine mais aussi éventuellement entre différents opérateurs ou FAI (Fournisseurs d'Accès Internet) si ceux-ci décident de coopérer étroitement pour un objectif commun de fourniture de QdS.

2.2 Principes du protocole de signalisation des mesures (MSP)

MSP est un composant clé de l'architecture MBA qui nécessite de trouver le compromis entre efficacité et capacité à fonctionner à large échelle. En effet, il est nécessaire de fournir des informations sur le trafic le plus rapidement possible pour permettre aux composants du réseau de réagir suite à la réception d'informations très récentes sur l'état du réseau tout en évitant de saturer le réseau avec des informations de signalisation. Ce bon fonctionnement à grande échelle nécessite aussi que les composants MSP ne stockent pas une trop grande quantité d'informations : les tables de correspondance à rajouter pour MBN dans les routeurs doivent être aussi petites que possible (avec un nombre limité d'entrées) pour permettre de minimiser le temps de recherche d'une information.

La figure 1 présente le mode de fonctionnement de MSP dans ses grandes lignes pour permettre d'atteindre ces objectifs d'efficacité et de passage à l'échelle. Tout d'abord, MSP est orienté connexion, c'est à dire que le chemin signalé doit être le même pour tous les paquets d'une connexion choisie. Pour cela, nous avons utilisé le principe de RSVP [BZ97] avec un premier paquet qui découvre le chemin de la source à la destination et ensuite un paquet de retour qui revient à la source. Les différences existent pour le paquet de retour qui est un paquet de réservation dans RSVP mais un paquet de signalisation dans MSP : il transporte des informations de mesure. D'autre part, les paquets de signalisation sont envoyés à chaque fois que nécessaire, alors que dans RSVP ils sont juste envoyés lorsque la connexion est ouverte. MSP utilise simplement le principe de RSVP qui consiste à trouver un chemin et à revenir le long de ce chemin. Cette méthode permet à MSP de parfaitement identifier quels sont les composants réseaux (les routeurs) rencontrés sur le chemin et de limiter le nombre de sources et de destinations pour les messages de mesure.

Pour permettre de prendre en compte le problème du facteur d'échelle rencontré par RSVP dans son déploiement Internet, nous avons choisi :

- De ne considérer que les flux éléphants. En fait, les souris ne créent pas de réel problème dans le trafic et la grande majorité des dommages sont générés par des éléphants [BAG03]. Ainsi, les routeurs MSP conservent juste une information sur les flux éléphants les traversant. Cette technique permet de limiter le nombre d'entrées dans la table de connexion étant donné que les éléphants ne représentent qu'une très petite proportion du nombre total de flux [LO04] ;

- D'envoyer les informations de mesure seulement lorsqu'une rupture est détectée dans le trafic. Cette technique permet de générer du trafic de signalisation seulement quand les conditions du réseau changent[‡]. Ce principe va donc limiter la quantité de données de signalisation et permettre aux émetteurs et aux routeurs de disposer très rapidement d'informations importantes sur l'évolution du réseau et du trafic : rappelons que les mesures sont réalisées tout au long du chemin entre la source et la destination et potentiellement très près de la source.

[‡] Evidemment, un envoi périodique d'information de mesure est aussi intégré dans MSP pour détecter les variations lentes dans les fluctuations du trafic (c'est à dire un trafic sans rupture forte mais avec une composante de non-stationarité). Etant donné son principe de réaction basé sur la détection de rupture, la période pourra être très grande, induisant ainsi un faible trafic de signalisation.

En procédant de la sorte, nous souhaitons résoudre le problème du facteur d'échelle qui a été précédemment rencontré dans l'Internet dans les tentatives d'amélioration et de garantie de la QdS.

3 Principes du contrôle de congestion orienté mesures (MBCC)

Les objectifs de MBCC sont conjointement d'améliorer les caractéristiques du trafic et la performance du réseau en lissant le trafic (de façon à limiter les effets de variabilité du trafic) et d'optimiser l'utilisation des ressources (la bande passante disponible) en utilisant l'infrastructure de mesure MBA / MSP. De plus, MBCC sera capable d'assurer une certaine équité à des flux concurrents et de continuer à fonctionner avec de bonnes performances même si certaines mesures manquent.

Dans les travaux [LO03] [OL04a] sur l'analyse des caractéristiques du trafic, la nature oscillatoire du trafic Internet a été mise en évidence. En particulier, il a été montré que ces oscillations persistantes dans le temps (sources de la LRD observée dans le trafic) étaient dues à l'inadéquation de TCP pour la transmission des fichiers très volumineux sur des réseaux à haut débit. Ainsi, le problème le plus immédiat concerne la réduction des oscillations et plus précisément la régulation des oscillations persistantes qui ont un impact dramatique sur la QdS du trafic et les performances du réseau. C'est pour cela qu'un des objectifs de MBCC est d'offrir plus de stabilité aux flux éléphants. Pour supprimer les comportements oscillatoires observables à toutes les échelles de temps, le mécanisme de contrôle de congestion TFRC (TCP Friendly Rate Control) est capable d'apporter une contribution importante. TFRC a été défini pour fournir un service adapté aux applications orientées flux qui ont besoin d'un débit lisse et régulier. Il essaie donc, d'éviter au maximum les variations brutables de débit qui apparaissent avec TCP dans le cas d'une reprise d'émission qui suit la détection d'une séquence de pertes. En associant un tel mécanisme au transfert des flux éléphants, représentant la majorité en volume du trafic, nous souhaitons contrôler les oscillations du trafic et augmenter la QdS et les performances globales du réseau. Les bénéfices de l'utilisation de TFRC à la place de TCP ont été démontrés dans [LO03]. Cependant, si TFRC est capable de réduire les oscillations de TCP, il n'est pas capable de s'adapter aux ruptures brutales du trafic (pannes sur des liens impliquant un rééquilibrage du trafic, pics de trafic dus à un trafic légitime lié à la diffusion d'un évènement très populaire par exemple). L'approche MBN est proposée comme une solution pour faire face à ces ruptures. Ainsi, nous souhaitons que MBCC soit une solution optimale permettant d'améliorer TFRC, qui en moyenne est un petit peu moins efficace que TCP New Reno avec SACK [§] (Selective ACKnowledgement [MMFR96]) [LO03]. Pour bénéficier des avantages de TFRC, nous avons défini MBCC comme une de ses extensions en le dotant d'une capacité à utiliser les résultats de mesure qui émanent des équipements de métrologie déployés dans le réseau. En faisant ce choix, nous sommes capables de produire de bons résultats (meilleurs que ceux de l'Internet actuel) même si les informations de mesure sont temporairement indisponibles.

Le principe de MBCC consiste à utiliser l'algorithme de TFRC pour calculer le taux d'émission nominal de chaque connexion et de corriger cette valeur grâce à la connaissance du niveau de bande passante disponible et consommée dans le réseau. Ainsi, si une fraction de la bande passante est disponible, les sources pourront générer plus de trafic que celui correspondant au débit d'un flux TCP [AAB00] sans pour autant créer des pertes et des congestions dans le réseau. Ainsi, le niveau de congestion du réseau devrait être significativement réduit en déployant des sources de trafic "pro-actives", capables d'adapter en temps réel leur débit d'émission en fonction des ressources disponibles. Un tel mécanisme devrait aussi aider à augmenter l'équité entre les flux, étant donné que la correction réalisée sur le débit d'émission ne devrait pas dépendre de la valeur du RTT mais de la réelle fraction de bande passante disponible équitablement partagée entre les flux concurrents.

Comme dans [LO03], MBCC sera uniquement utilisé pour les flux éléphants qui sont les flux qui génèrent le plus de perturbations dans le réseau. A l'opposé, comme le trafic "souris" représente un bruit blanc Gaussien [BAG03], il n'induit pas de problème de transfert important et il n'est donc pas nécessaire de modifier leur protocole de transport. Ainsi, pour une période normale (quand les informations de mesure sont correctement reçues, qu'il n'y a pas de congestion et que de la bande passante est disponible dans le réseau), chaque flux éléphant peut utiliser une fraction supplémentaire des ressources qui sont disponibles. Cette fraction est calculée en divisant la bande passante totale disponible par le nombre de flux moyens

[§] Cette version de TCP a été choisie comme référence car elle est considérée comme la version la plus performante de ce protocole de transport.

éléphants dans le réseau à ce moment (ces informations étant fournies par les équipements de mesure rencontrés tout au long du chemin). Il est logique de diviser la bande passante disponible par le nombre moyen de flux actifs (N) traversant ce lien car il a été démontré que les arrivées de flux éléphants sont proches d'un processus Poissonien [BAG03]. En effet, pour un processus de Poisson, comme la moyenne est égale à la variance, le nombre moyen est significatif car les valeurs du processus ne seront jamais très éloignées de cette valeur moyenne. A l'inverse pour une période de congestion, les émetteurs MBCC devront réduire leur débit d'émission pour résorber la congestion et ceci en essayant d'être aussi équitable que possible. Dès lors, les sources MBCC envoient la valeur minimale entre le débit TFRC et le débit effectif obtenu par un flux à ce moment au niveau du goulot d'étranglement sur son chemin.

Ainsi, les équations de cet algorithme peuvent être résumées de la façon suivante :

- Pour une période sans congestion ($p = 0$) : $X_{MBCC} = X_{TFRC} + BPd_{flux}$;
- Pour une période de congestion ($p \neq 0$) : $X_{MBCC} = min(X_{TFRC}; BPc_{flux})$;

Avec :

- BPd_{flux} qui correspond à la bande passante disponible dans le(s) goulot(s) d'étranglement rencontré(s) sur le chemin. Il est calculé par l'intermédiaire du rapport $\frac{\text{bande passante totale disponible}}{N}$, cette information étant fournie par les routeurs MSP rencontrés sur le chemin ;
- BPc_{flux} qui correspond à la bande passante consommée par le flux au travers du goulot d'étranglement, cette information est fournie par le récepteur MBCC avec les autres informations de bout-en-bout comme le RTT ou le taux de perte.

4 Validation expérimentale de la contribution de MBN à la robustesse du réseau

Dans cette section, nous présentons les résultats expérimentaux qui illustrent les capacités de MBCC pour améliorer la robustesse du réseau. En particulier, nous comparons la QdS du réseau lorsque MBCC ou TCP sont confrontés à un trafic contenant des attaques DdS.

4.1 Principes de la simulation

Les mécanismes MBCC et MSP ont été implémentés et évalués en utilisant NS-2 [NS-]. Il a été nécessaire de développer un ensemble d'outils pour mesurer la bande passante disponible et consommée dans le réseau simulé et pour échanger les résultats de mesure entre les routeurs et les sources de trafic.

4.1.1 Topologie de simulation

La topologie utilisée est décrite dans la figure 2. Dans ces simulations, nous avons créé un goulot d'étranglement pour augmenter les comportements concurrents entre les différents flux. Les flux éléphants, utilisant soit MBCC, soit TCP SACK ainsi que le trafic de fond utilisant TCP New Reno sont échangés de façon à entrer en compétition dans ce goulôt d'étranglement[¶]. L'objectif est donc de mesurer l'impact réciproque des flux MBCC en théorie réguliers sur les flux TCP beaucoup plus variables et de comparer l'impact des attaques DdS sur la QdS du réseau quand MBCC ou TCP sont utilisés pour émettre les flux élephants. De plus, le lien de coeur représente le lien le plus "congestionné" sur le chemin considéré : c'est à dire celui qui aura le plus d'influence sur les débits d'émission de MBCC et TCP. Chaque simulation s'appuie sur des traces de trafic collectées sur le réseau Renater. Elles sont rejouées dans le simulateur NS-2 avec une méthodologie spécifique détaillée dans [OL04b] dont l'objectif est de produire des simulations réalistes[‖].

En simulation, les flux courts et longs sont différenciés. Les premiers (flux souris) n'induisent pas de problème de transfert dans le réseau. Ainsi, ils seront transmis avec TCP New Reno qui est la version la plus fréquente de ce mécanisme dans l'Internet. A l'inverse, les flux éléphants créent dans le réseau des

[¶] Le trafic de fond peut contenir potentiellement des attaques DdS.

[‖] Il s'agit de rejouer en simulation des échantillons de trafic Internet pour reproduire toutes les caractéristiques statistiques du trafic réel.

oscillations à long terme qui vont entrainer des congestions. C'est la raison pour laquelle MBCC a été défini pour transmettre efficacement les flux éléphants. Dès lors, les simulations comparent la configuration où les éléphants sont transmis en utilisant notre nouveau mécanisme de contrôle de congestion et celle dans laquelle ils sont échangés avec TCP SACK **.

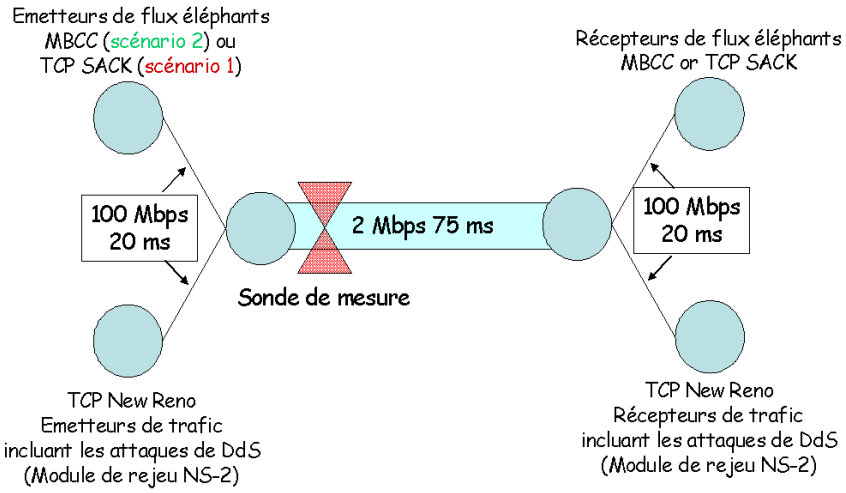


FIG. **2** – *Topologie réseau utilisée pour les simulations NS-2*

Pour évaluer la robustesse de la QdS quand MBCC ou TCP sont utilisés, nous avons rejoué une trace de trafic contenant des attaques DdS. Cette trace a été capturée sur le réseau d'accès Internet du LAAS le jour où nous avions lancé une attaque de "flooding" UDP vers notre laboratoire. La trace rejouée dure 40 minutes. Cette capture a été réalisée avec des équipements DAG [CDG+00]. Les caractéristiques de débit de cette trace sont représentées dans la figure 3. Les seize premières minutes (cf. intervalle 1 de la figure 3) représente un trafic Internet classique contenant en majorité les applications suivantes : web, mail, ftp, etc. Le reste de la trace (cf. intervale 2) contient en plus du même trafic initial plusieurs attaques DdS générées à partir d'une machine située à l'extérieur du réseau du LAAS et à destination d'un ordinateur spécifique situé dans notre réseau de recherche. Plus précisément, les attaques DdS sont des "floods" UDP constitués chacune de 10 000 paquets et dont les paramètres de force et d'intensité d'attaque varient de la façon suivante :

– la force de l'attaque représente la taille des paquets UDP émis (0, 20 40, 100, 1000 ou 1500 octets) ;

– la fréquence de l'attaque représente la période de temps entre deux émissions consécutives de paquets UDP : 100 ns, 1 000 ns ou 10 000 ns.

Deux attaques consécutives sont séparées par une période de silence de 30 secondes.

L'objectif principal de cette étude est de comparer les capacités d'adaptation de MBCC face aux anomalies du réseau comme une attaque DdS et de comparer les résultats avec les autres mécanismes de contrôle de congestion. Pour réaliser l'évaluation de MBCC et estimer sa contribution à la robustesse de la QdS, plusieurs paramètres ont été étudiés en simulation :

– l'évolution du débit par type de trafic (TCP ou MBCC) en étudiant la variabilité du trafic. Pour cela, nous calculons le débit moyen (D), l'écart-type (σ) et un coefficient de stabilité défini de la façon suivante : $CS = \frac{D}{\sigma}$;

– l'évolution du processus de perte permettant d'évaluer les capacités d'adaptation de MBCC et de les comparer à TCP ;

** TCP SACK sert de référence étant donné qu'il est la version la plus performante de TCP.

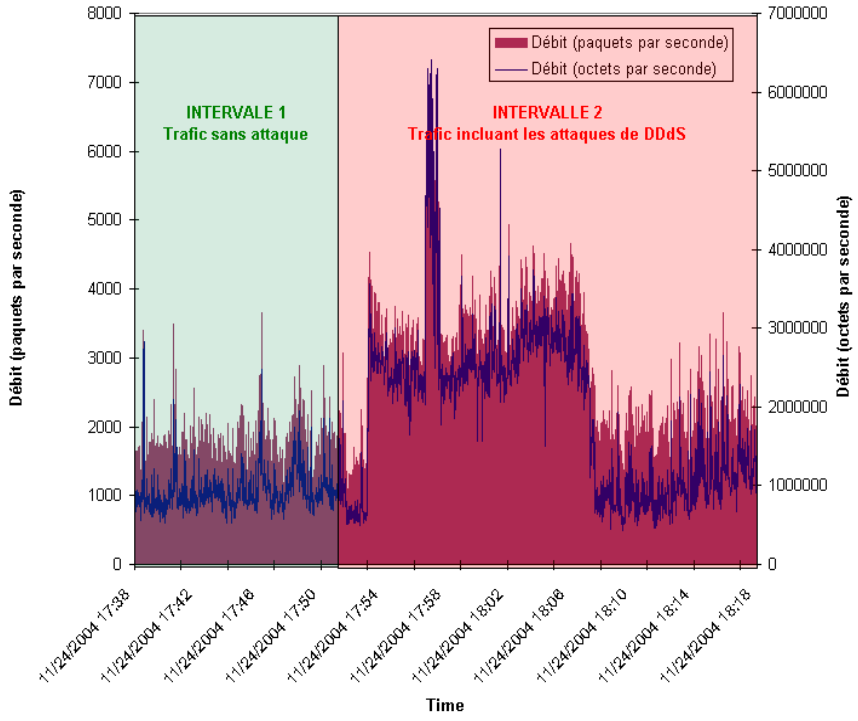


FIG. **3 –** *Caractéristiques de l'attaque DdS*

4.2 Contribution de MBCC à la QdS en présence d'attaques

Cette simulation inclut deux scénarios différents : dans le premier, les flux éléphants sont transmis en utilisant TCP SACK tandis que dans le second, ils utilisent MBCC. Le premier scénario est utilisé comme référence expérimentale. Dans ces deux scénarios, le trafic de fond (si nous ne prenons pas en compte les attaques DdS) constitué d'un trafic Internet normal, mélange de flux souris et éléphants, est émis en utilisant TCP version New Reno.

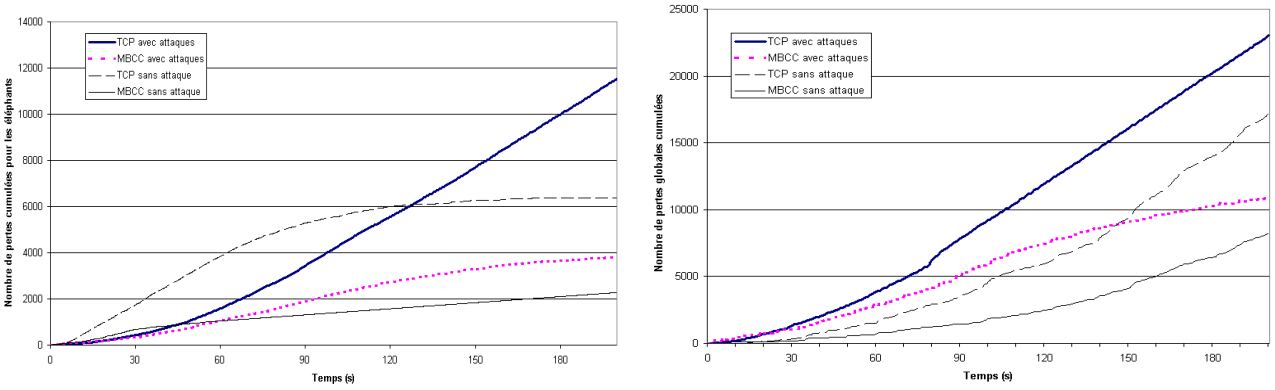
Chaque simulation dure 200 secondes. 100 éléphants, 4000 flux de fond (constitués de flux souris et éléphants) et les paquets représentant l'attaque DdS ont été rejoués. Les résultats de simulation sont les suivants : premièrement, le débit du trafic a été calculé pour l'intervalle 2 (trafic contenant des attaques DdS). La table 1 représente les valeurs numériques pour les scénarios 1 et 2. Cette expérimentation met en évidence que MBCC fonctionne mieux que TCP SACK étant donné que son débit et l'utilisation qu'il fait des ressources disponibles sont plus élevés. De plus, le trafic est plus régulier. D'autre part, une autre information intéressante apparait dans ces résultats qui concernent le trafic de fond dans le goulôt d'étrangement quand le trafic éléphant MBCC est présent dans le réseau (cf. scénario 2). Nous pouvons observer que comparativement au cas où TCP SACK est utilisé pour transmettre les éléphants (scénario 1), le débit moyen du trafic de fond est plus bas et met en évidence plus de variabilité que quand MBCC est utilisé dans le réseau (cf. par exemple $SC(\text{TCP New Reno}_{\text{Scenario 1}}) < SC(\text{TCP New Reno}_{\text{Scenario 2}})$). Ceci démontre que MBCC est capable de rendre le réseau plus robuste et le trafic plus régulier que TCP SACK dans le cas d'attaques DdS.

Ce résultat est confirmé avec l'analyse du processus de perte. En effet, la figure 4 met en évidence un niveau de perte plus important dans le réseau lorsque TCP SACK est utilisé comparativement à MBCC. Ce résultat a été analysé à la fois sur le trafic éléphant seul (cf. figure 4(a)) mais aussi sur le trafic global échangé dans le réseau (cf. figure 4(b)). En effet, il apparait que la variabilité du trafic avec TCP est plus importante, ceci créant plus de congestion et augmentant le nombre de pertes dans le réseau.

En conclusion, ces résultats prouvent que MBCC (comparativement à TCP) rend la QdS du réseau plus robuste aux attaques. En effet, l'impact d'une attaque d'UDP "flooding" est beaucoup plus limité avec

TAB. **1 –** *Analyse de la variabilité du trafic*

	INTERVALLE 2 : trafic incluant les attaques de DDdS					
	Scénario 1 (TCP)			Scénario 2 (MBCC)		
	Trafic global	*Trafic de fond*	*Trafic Eléphant (TCP SACK)*	*Trafic global*	*Trafic de fond*	*Trafic Eléphant (MBCC)*
Débit moyen (octets / s)	243.872,13	221.827,32	22.044,81	248.004,64	227.691,13	22.313,51
Ecart-type du débit (octets / s)	31.553,07	83.943,63	44.704,32	22.690,51	57.127,70	31.840,41
Coefficient de stabilité pour le débit (SC)	7,73	2,64	0,49	10,93	3,99	0,70



(a) Trafic éléphant

(b) Trafic global

FIG. **4 –** *Analyse du niveau de congestion*

MBCC qu'avec TCP : le débit est plus important, les pertes et le niveau de congestion sont plus faibles. Ceci induit pour le réseau un trafic plus régulier et une meilleure QdS. En particulier, les résultats illustrent que les performances de MBCC avec et sans attaques sont très proches et démontrent ainsi une relative insensibilité de MBCC aux attaques qui permet d'améliorer la robustesse de la QdS du réseau.

5 Conclusion et travaux futurs

Dans ce papier, nous avons proposé une nouvelle approche qui utilise en temps réel les résultats de métrologie pour améliorer la QdS Internet avec l'objectif final de pouvoir améliorer la robustesse du réseau, pour permettre de fournir de façon continue des services de haute qualité même dans le cas où le réseau est attaqué. Cette approche a été appliquée pour la conception d'un mécanisme de contrôle de congestion (MBCC) dont l'objectif est de lisser le trafic (un besoin primordial pour pouvoir fournir des services stables et garantis), limiter le nombre de pertes, optimiser l'utilisation des ressources et fournir de l'équité. Au final, il est clair que les résultats de MBCC démontrent les bénéfices de notre approche MBN pour améliorer la robustesse de la QdS, en particulier dans le cas d'attaques, MBCC continuant à fournir aux utilisateurs le même niveau de QdS.

Cependant, ces travaux devront être poursuivis. Premièrement, ce papier se focalise uniquement sur les attaques de flooding UDP. Ainsi, le travail futur incluera l'analyse de l'impact des autres types d'attaques DdS et en particulier la nouvelle famille des attaques "légères". En se basant sur les résultats d'analyse des attaques DdS, nous allons donc continuer à étudier de nouvelles solutions orientées MBN pour améliorer la QdS du réseau et le rendre plus robuste. Ainsi, MBCC sera amélioré mais nous souhaitons aussi adapter dans un deuxième temps, les mécanismes des routeurs et les protocoles de routage pour mieux combattre l'impact des attaques DdS sur le réseau.

Références

[AAB00] E. Altman, K. Avrachenkov, and C. Barakat. A stochastic model of tcp/ip with stationary random losses. In *Proceedings of ACM SIGCOMM*, 2000.

[BAG03] N. Ben Azzouna and F. Guillemin. Analysis of adsl traffic on an ip backbone link. In *Proceedings of Globecom 2003*, December 2003.

[BZ97] R. Braden and L. Zhang. Resource reservation protocol (rsvp) – version 1 message processing rules. *RFC*, (2209), September 1997.

[CDG+00] J. Cleary, S. Donnely, I. Graham, A. McGregor, and M. Pearson. Design principles for accurate passive measurement. In *PAM (Passive and Active Measurements) Workshop*, April 2000.

[ENW96] A. Erramilli, 0. Narayan, and W. Willinger. Experimental queuing analysis with long range dependent packet traffic. In *IEEE/ACM Transactions on Networking, Vol. 4, No. 2*, pages 209–223, 1996.

[FGW98] A. Feldmann, A. Gilbert, and W. Willinger. Data networks as cascades: Investigating the multifractal nature of internet wan traffic. In *Proceedings of ACM SIGCOMM'98*, 1998.

[FHPW00] S. Floyd, M. Handley, J. Padhye, and J. Widmer. Equation-based congestion control for unicast applications. In *Proceedings of ACM SIGCOMM'00*, 2000.

[LO03] N. Larrieu and P. Owezarski. Tfrc contribution to internet qos improvement. In *Proceedings of the fourth COST 263 international workshop on Quality of Future Internet Services (QoFIS'2003)*, October 2003.

[LO04] N. Larrieu and P. Owezarski. De l'utilisation des mesures de trafic pour l'ingénierie des réseaux de l'internet. *Techniques et Sciences Informatiques*, (5-6, RSTI, volume 23), 2004.

[LO05] N. Larrieu and P. Owezarski. Measurement based networking approach applied to congestion control in the multi-domain internet. In *Proceedings of the 9th IEEE / IFIP International Symposium on Integrated Network Management (IM'2005)*, May 15th-19th, 2005.

[MMFR96] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanov. Tcp selective acknowledgement options. *RFC*, (2018), October 1996.

[NS-] NS-2. Site web : http://www.isi.edu/nsnam.

[OL04a] P. Owezarski and N. Larrieu. Internet traffic characterization – an analysis of traffic oscillations. In *Proceedings of the 7th IEEE International Conference on High Speed Networks and Multimedia Communications (HSNMC'2004)*, July 2004.

[OL04b] P. Owezarski and N. Larrieu. A trace based method for realistic simulations. In *Proceedings of the IEEE International Conference on Communications (ICC'2004)*, June 2004.

[Owe03] P. Owezarski. Métrologie des réseaux de l'internet et analyse des attaques. In *2nde rencontres francophones sur le thème Sécurité et Architecture Réseaux (SAR'2003)*, 30 juin - 4 juillet 2003.

[PKC96] K. Park, G. Kim, and M. Crovella. On the relationship between file sizes, transport protocols, and self-similar network traffic. In *IEEE ICNP*, 1996.

[PW00] K. Park and W. Willinger. *Self-similar network traffic: an overview*. In Self-similar network traffic and performance evaluation, J.Wiley & Sons, 2000.