Une caractérisation non gaussienne et à longue mémoire du trafic Internet et de ses anomalies

A. Scherrer[†], N. Larrieu, P. Owezarski[‡], P. Borgnat, P. Abry[§]

LIP, CNRS UMR 5668, ENS de Lyon. LAAS-CNRS, UPR 8001, Toulouse. Laboratoire de physique, CNRS UMR 5672, ENS de Lyon

L'Internet doit aujourd'hui fournir de très nombreux services garantis pour un grand nombre d'applications diverses et variées. La qualité des services qu'il offre devient donc très sensible aux anomalies du trafic dues par exemple à des pannes, à des «foules subites» ou à des attaques de déni de service (DoS) dont le but est de réduire de façon significative le niveau de qualité de service (QoS). Les systèmes de détection d'intrusion (IDS), et notamment ceux basés sur la détection d'anomalies, ne donnent pas satisfaction pour détecter efficacement les attaques DoS. C'est principalement dû aux difficultés pour distinguer les variations de trafic lourdes mais légitimes de celles dues aux attaques DoS. Le but de cet article est de comparer les caractéristiques statistiques du trafic régulier avec celles du trafic contenant des anomalies. Pour cela, nous introduisons un modèle de trafic non Gaussien et à mémoire longue, pour lequel nous avons développé des estimateurs de ses paramètres. Dans un premier temps, nous montrons que ce modèle décrit de façon précise le trafic Internet pour de très nombreux niveaux d'agrégation, et ce sur un ensemble significatif de traces publiques (Bellcore, LBL, Auckland, UNC, CAIDA) ainsi que sur des données collectées par nos soins. Dans un second temps, nous montrons que le modèle représente également le trafic contenant des anomalies comme des foules subites ou des attaques DoS que nous avons générées et collectées. Nous montrons que le comportement des paramètres du modèle permet de déterminer si le trafic présente ou non des anomalies, et si ces anomalies sont dues à des foules subites ou à des attaques DoS.

Mots-clés: Détection d'intrusion, attaques DoS, foules subites, processus non gaussiens à longue mémoire

1 Motivation

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 doit donc évoluer d'une offre de service best effort unique vers une offre multi-services, ce qui le rend du coup plus sensible aux attaques, et en particulier les attaques DoS simples et distribuées. En effet, les attaques DoS provoquent des changements importants dans les caractéristiques du trafic, ce qui peut réduire de façon significative le niveau de QoS perçu par les utilisateurs du réseau. Notamment, cela peut entrainer une violation des SLA (Service Level Agreement) à la charge de l'ISP, et de lourdes pertes financières pour ce dernier.

Combatre les attaques DoS est une tâche difficile et les systèmes de détection d'intrusion (IDS), notamment ceux basés sur la détection d'anomalies, ne sont pas très efficaces. En premier lieu, leurs limitations sont liées à la multitude de formes que peuvent prendre les attaques DoS et qui rendent difficile une définition globale des attaques. Dans un second temps, il a été observé à de très nombreuses reprises que le trafic Internet normal présente des variations importantes de son trafic à toutes les échelles [PKC96], souvent décrites en terme de longue mémoire [ENW96], auto-similarité [PW00], multifractalité [FGW98].

[†] A. Scherrer est au LIP.
[‡] N. Larrieu et P. Owezarski sont au LAAS-CNRS.
[§] P. Borgnat et P.Abry sont au laboratoire de physique de l'ENSL.

Ces caractéristiques rendent plus delicate et incertaine la detection d'anomalies. Troisièmement, le trafic Internet peut présenter des variations fortes, soudaines mais légitimes (comme des foules subites - ou flash crowds en anglais - par exemple) qu'il peut être difficile de distinguer des variations illégitimes.
Pour ces raisons, les IDS basés sur la détection d'anomalies souffrent souvent de taux de faux positifs, et sont donc peu populaires. L'évolution actuelle du trafic Internet, avec une variété immense de types de trafics rendent encore plus délicate la conception d'un IDS efficace.

Ce travail, réalise dans le cadre du projet MetroSec, a pour objectifs principaux d'analyser l'impact des anomalies sur les caractéristiques statistiques et de mettre en évidence des signatures caractéristiques du trafic contenant des anomalies légitimes (p.ex. foules subites) et illégitimes (p.ex. attaques DDoS). A la fin, ces résultats doivent servir à améliorer les mécanismes réseau et les rendre capable de combattre les anomalies, notamment les malicieuses.

Pour cela, nous proposons d'utiliser un modèle de processus stochastique non Gaussien et à mémoire longue représentant le trafic Internet. Nous montrons expérimentalement que ce modèle est suffisamment versatile pour décrire une grande variété de trafics réguliers ainsi que des trafics comportant des anomalies, légitimes ou non. Nous montrons aussi que les évolutions des estimations des paramètres pour le modèle proposé permettent de différencier le trafic avec et sans anomalies et de classifier ces anomalies.

2 Modélisation de trafic : une introduction

2.1 Trafic sans anomalie

Le trafic des réseaux d'ordinateurs peut se caractériser par un processus d'arrivée de paquets. Il a été montré il y a plus de 10 ans que ces processus d'arrivée des paquets sont très éloignés du modèle de Poisson (voir par exemple [PF95]), en particulier parce que les inter-arrivées de paquets ne sont pas indépendantes. On peut les modéliser en utilisant soit des processus non stationnaires [KMFB04] ou des processus markovien modulés stationnaires [AN98]. Par conséquent, une description générale du processus est $\{(t_l, A_l), l = 0, 1, 2, ...\}$ ou t_l représente l'estampille d'arrivée du l-ème paquet et A_l certains attributs du paquet (comme sa charge utile, ses ports source et destination, ...). Cependant, étant donné le grand nombre de paquets impliqués, cela engendre des ensembles de données énormes.

C'est pourquoi il est souvent préférable de considérer les processus décomptant le nombre d'octets ou de paquets du trafic agrégé, notés $W_\Delta(k)$ et $X_\Delta(k)$. Ils correspondent au nombre d'octets (resp. paquets) qui transitent au cours de la k-ème fenêtre de taille $\Delta > 0$, i.e., dont les estampilles se situent entre $k\Delta \leq t_l < (k+1)\Delta$. D'autres analyses pourraient reposer sur le processus d'arrivée des flux comme dans [BTI+02] par exemple. Dans cet article, nous restons au niveau paquet et nous nous concentrons sur la modélisation conjointe des distributions marginales et de la fonction de covariance de $X_\Delta(k)$. L'adéquation et l'intérêt des processus multifractaux, dont les propriétés d'échelle ne sont pas complètement décrites au second ordre statistique, et implique donc des ordres statistiques supérieurs, ont été étudiés en détail dans de nombreux articles (voir [FGW98, TTW97, ZRMD03]). Cet aspect, qui reste un problème ouvert, ne sera pas étudié dans cet article.

2.2 Détection d'anomalies

Les IDS basés sur la détection d'anomalies n'utilisent pas, en général des modèles statistiques riches. Ils supervisent juste des paramètres simples du trafic comme son débit d'octets ou de paquets, et la plupart de ces IDS recherchent juste des séquences de paquets spécifiques, connues comme des signatures d'attaques [Pax99]. Les alarmes sont essentiellement générées lorsqu'un seuil est dépassé [Bru00, VL89], ce qui conduit à un nombre important de faux positifs [MVS01]. Par conséquent, ces IDS sont souvent assez peu satisfaisants car ils ne peuvent pas différencier les variations légitimes du trafic des attaques.

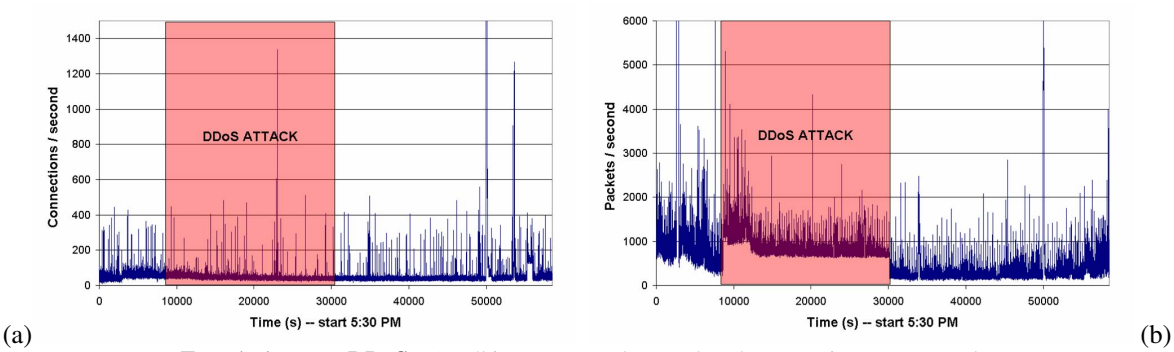
Les progrès récents en modélisation obtenus dans les projets de métrologie du trafic ont cependant renouvelé les stratégies de conception des nouveaux IDS. Même si ces derniers restent encore à des étapes de développement peu avancées, des résultats très intéressants utilisant des caractérisations statistiques ont été publiés. Par exemple, Ye a proposé dans [Ye00] un modèle Markovien pour le comportement temporel du trafic, et génère des alarmes lorsque le trafic s'éloigne significativement du modèle. D'autres auteurs [JY04, YM04] ont montré que les attaques DoS augmentent la corrélation dans le trafic, ce qui pourrait

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

TAB. 1: Description des Données. Paramètres généraux des traces étudiées. T est la durée de la trace, en secondes. # Pkts (10^6) est le nombre de paquets dans la trace, en millions. IAT est le temps d'inter-arrivées moyen, en ms.

représenter une technique de détection robuste. A partir de l'évaluation de l'inter-corrélation de trafics sur différents liens, Lakhina *et al.* ont proposé une méthode pour détecter les anomalies dans les matrices de trafic à l'échelle du réseau global [LCD04]. Hussain et ses co-auteurs utilisent la densité spectrale pour identifier des signatures pour différentes attaques [HHP03]. De la même façon, l'estimation spectrale a été utilisée pour comparer des trafics avec et sans attaques [CKT02]. Alors que la densité spectrale met en évidence des pics autour du RTT pour du trafic normal, ces pics disparaissent en cas d'attaque. Cette caractéristique peut ainsi être utilisée pour concevoir de nouveaux IDS. Enfin, Li and Lee ont utilisé les techniques à base d'ondelettes développées dans [VA99] pour calculer une distribution d'énergies. Ils ont observé que cette distribution d'énergies présente des pics lorsque le trafic contient des attaques qui n'existent pas pour le trafic régulier [LL03]. Le travail présenté en [BKPR02] exploite les qualities d'analyse multi-résolutions des decompositions en ondelettes pour détecter les anomalies du trafic pour un intervalle d'échelles moyennes. De nombreux travaux prometteurs ont déjà été publiés dans le domaine des attaques DoS [BKPR02, JKR02].

La détection d'anomalies pourrait reposer sur des analyses dépendantes des applications [FBGO05], ou sur les mécanismes des attaques [KKJB05]. Dans ce travail, nous nous focalisons sur le niveau paquet. Cependant, et parce que nous observons le trafic avec différentes échelles de temps, la méthode d'analyse proposée est principalement basée sur la détection de changements dans les caractéristiques statistiques du trafic. En comparant les distributions marginales et les fonctions de covariance obtenues d'abord sur du trafic régulier, puis sur des trafics présentant une large variété d'anomalies incluant notamment des anomalies légitimes, nous pouvons différencier les changements du trafic dus à des actions légitimes d'actions illégitimes.



(a) (b)

FIG. 1: Attaque DDoS. (a) Débit paquets et (b) Nombre de connexions par seconde.

3 Données et Expériences

3.1 Trafic sans anomalie

Le modèle et les analyses proposés plus loin ont d'abord été illustrés sur des traces de trafic ne présentant pas d'anomalies, et décrites en détails dans la table 1. Nous utilisons à la fois des données standards pu-

bliques (Bellcore, LBL, UNC, Auckland Univ, Univ North Carolina, CAIDA), et des séries temporelles de trafics capturées par nos soins dans le cadre du projet de recherche MetroSec. Par conséquent, nous couvrons un ensemble significatif de traces de trafics, provenant de différents types de réseaux (LAN, WAN, ... et des réseaux de bordure, de cœur, ...) et de liens, capturées ces 16 dernières années (de 1989 à 2005). Dans chaque base de données, un grand nombre de traces sont disponibles. Nous nous concentrons dans cet article sur quelques traces qui sont représentatives de ces collections de traces.

3.2 Trafic (ou traces) avec des anomalies

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

• **Attaque DDoS.** L'attaque DDoS étudiée ici est une attaque en UDP flooding distribuée. Elle a été générée depuis 5 sites différents : l'IUT De Mont de Marsan, le LIAFA Paris, l'ENS Lyon, l'ESSI Nice, en France et l'université de Coimbra au Portugal, à l'encontre du LAAS à Toulouse qui était le site ciblé. Le LAAS est connecté à RENATER par l'intermédiaire d'un lien Ethernet 100 Mbps qui n'a pas été saturé pendant l'attaque. Une trace du trafic a été capturée sur le lien d'accès du LAAS. L'attaque a démarré à 20h le 9 décembre 2004 et a duré plus de 5h30. Les caractéristiques de base du trafic sont décrites sur les Figures 2.2(a) et 2.2(b) qui montrent respectivement le nombre de flux et de paquets sur le réseau d'accès du LAAS. Alors que le premier reste très stable, le second présente une augmentation significative du débit des paquets (il est multiplié par presque 3 pendant l'attaque).

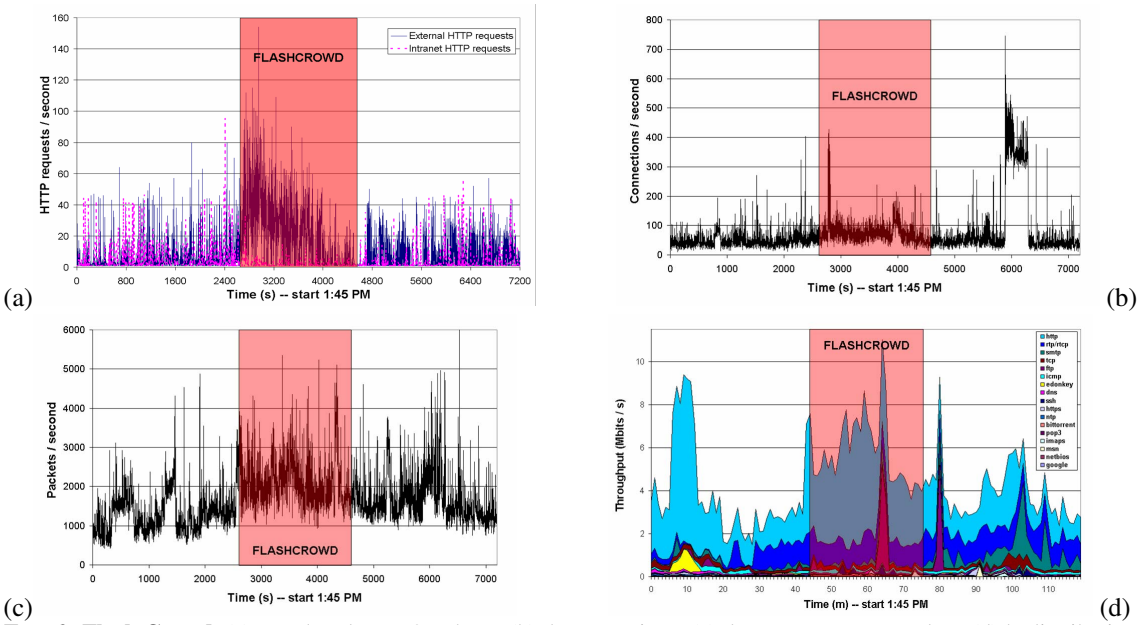


FIG. 2: Flash Crowd. (a) Nombre de requêtes http , (b) de connexions, (c) de paquets par seconde et (d) la distribution des débits par application. La figure (d) suit une approche descendante : l'application apparaissant au plus haut de la légende est celle qui génère le plus de trafic.

• **Flash Crowd (FC) ou foule subite.** Pour comparer l'impact sur les caractéristiques du trafic d'attaques DDoS et de variations légitimes du trafic, nous avons créé des foules subites sur un serveur web. Pour les rendre réalistes, i.e. humainement aléatoires, nous avons choisi de ne pas utiliser un programme automatique, mais au contraire, de demander à de nombreux collègues académiques de consulter le site web du LAAS (http ://www.laas.fr). Les résultats présentés sont ceux obtenus pour la foule subite du 14 avril 2005 qui a duré 30 minutes et à rassembler plus de 100 participants. La figure 3.2(a) montre le nombre

de requêtes reçues par le serveur web du LAAS (HTTP GET requests), en faisant la distinction entre les requêtes venant de l'intérieur et de l'extérieur du LAAS. Il apparaît clairement que de nombreux utilisateurs ont commencé à naviguer sur le site web du LAAS à 14h30 (augmentation importantes du nombre de requêtes), mais également que la plupart ne sont pas restés les 30 minutes. Les Figures 3.2(b) et 3.2(c) montrent respectivement le nombre de flux et le debit des paquets sur le réseau d'accès du LAAS. Comme c'était attendu, les deux courbes présentent une augmentation du nombre moyen de flux et du débit moyen de paquets, respectivement, durant la foule subite. Cependant, il apparaît aussi une augmentation importante du nombre de flux et du débit paquets après la fin de l'expérience de foule subite. La figure 3.2(c) montre aussi une augmentation du débit paquets moyen avant l'expérience de foule subite. Pour comprendre ces augmentations, nous avons analysé différentes composants du trafic en utilisant l'outil Traffic Designer de la société QoSMOS [QoS] (cf. figure 3.2(d)). L'analyse a montré que l'augmentation autour de 14h (avant notre experience) est due à des membres du LAAS qui naviguent sur le web juste après le déjeuner. Un tel comportement a été observé systématiquement sur toutes les traces collectées au LAAS depuis. Le second pic, après l'expérience, est dû à du trafic SMTP. Il peut s'expliquer de deux façons. En premier lieu, il faut savoir que de nombreux chercheurs au LAAS utilisent webmail. Comme le serveur a été très ralenti pendant l'expérience de foule subite, ils ont donc arrêté d'envoyer des e-mails jusqu'à ce que le serveur recommence à fonctionner avec des performances satisfaisantes. Dans un second temps, il faut savoir que le mécanisme de « grey listing » (utilisé pour réduire le nombre de spam) retarde certains e-mails, et les émet tous ensemble lors des ouvertures planifiées des portes. La première ouverture après l'expérience s'est produite à 15h15.

4 Processus non Gaussien à mémoire longue

4.1 Le modèle Gamma farima

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

• **Statistiques du premier ordre (Marginale) : Distribution Gamma.** $X_\Delta(k)$ est par définition une variable aléatoire positive ; plusieurs travaux ont proposé de décrire sa loi marginale avec des lois positives bien connues comme les lois exponentielle, log-normale, Weibull ou des distributions Gamma [Mel93]. A cause de la nature du trafic, ($X_\Delta(k)$ est conçu à partir d'un processus d'arrivées de paquets [EHP00]), des distributions Poisson ou exponentielle sont attendues pour les niveaux de faible agrégation Δ. Pour des données fortement agrégées (pour des Δ plus grands), les lois Gaussiennes constituent de bonnes approximations. Cependant, aucune d'elles ne peut modéliser de façon satisfaisante les lois marginales du trafic pour un spectre large de (petits et grands) Δ. Nos études empiriques montrent qu'une distribution Gamma $\Gamma_{\alpha,\beta}$ représente mieux les marginales de X_Δ.
Une distribution $\Gamma_{\alpha,\beta}$ est définie pour des variables aléatoires positives X par

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

où $\Gamma(u)$ est la fonction Gamma standard (voir [EHP00]). Elle dépend de deux paramètres : la forme α et l'échelle β. Sa moyenne est $\mu = \alpha\beta$ et sa variance $\sigma^2 = \alpha\beta^2$. A noter que l'inverse du paramètre de forme, $1/\alpha$, agit comme un indicateur de la distance avec une loi Gaussienne.

• **Statistiques du second ordre (covariance) : Dépendance à long terme.** Après les travaux présentés dans [LTWW94], il est aujourd'hui communément accepté que le trafic sur un réseau d'ordinateurs se caractérise par des propriétés de mémoire longue ou de dépendance à long terme (cf. [Ber94]). La dépendence à long terme (LRD) est généralement définie par une densité spectrale en puissance $f_{X_\Delta}(\nu)$ du processus qui se

comporte à l'origine comme :

$$f_{X_\Delta}(\nu) \sim C|\nu|^{-2d}, |\nu| \to 0, \text{ with } 0 < d < 0.5. \quad (2)$$

La dépendance à long terme dans le trafic Internet est une propriété d'importance car elle entraine des baisses de performance et de QoS (voir par exemple [TG98]). Considérer précisément la LRD est une condition importante pour concevoir des réseaux adaptés aux besoins (taille des buffers, dimensionnement, ...) et en prédire les performances. Il est donc crucial d'incorporer la LRD dans les modèles de description du trafic. Cela élimine de fait les processus Poissonnien ou Markovien ainsi que leurs déclinaisons.

Par conséquent, les processus à longue mémoire comme les mouvement Browniens fractionnaires, les bruits Gaussiens fractionnaires [Nor95] ou les modèles *Fractionally Integrated Auto-Regressive Moving Average* (FARIMA) ont été largement utilisés pour décrire et / ou analyser les séries temporelles extraites du trafic Internet (voir [PW00] et les références associées).

Cependant, à cause de la multitude de mécanismes réseaux et de sources de trafic différents, le trafic présente aussi des caractéristiques de dépendance à court terme (SRD) qui se superposent à celles de mémoire longue (cela a été étudié pour le trafic vidéo VBR [HDLK95]). Par conséquent, utiliser le processus FARIMA [Ber94] est naturel car il permet de décrire à la fois les dépendances courtes et longues.

Un modèle farima(P,d,Q) est défini par deux polynômes d'ordres P et Q et d'une intégration fractionnaire $\mathbf{D}^{-d}$, d'ordre $-1/2 < d < 1/2$:

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

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

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

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

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

4.2 Analyse

• **Stationarité des données.** Pour chaque niveau d'agrégation Δ on réalise une analyse de X_Δ. Etant donné l'hypothèse de stationnarité de X_Δ dont nous avions besoin pour la modélisation théorique, nous commençons par une vérification empirique des analyses et estimations obtenues sur des sous-blocs adjacents et disjoints. Ensuite, nous analysons seulement les ensembles de données pour lesquels la stationnarité est une hypothèse raisonnable. C'est une approche dont l'esprit est très proche de celles développées dans [VA01]. Il ne reste plus alors qu'à estimer les paramètres du modèle pour chacun des Δ choisis.

• **Estimation des paramètres de la loi Gamma.** Plutôt que d'utiliser la technique classique des moments, $\hat{\beta} = \hat{\sigma^2}/\hat{\mu}$, $\hat{\alpha} = \hat{\mu}/\hat{\beta}$ où $\hat{\mu}$ et $\hat{\sigma^2}$ sont les estimateurs standard pour la moyenne et la variance, nous utilisons une technique basée sur le maximum de vraisemblance pour estimer α et β [HS94]. La distribution conjointe de n variables $\Gamma_{\alpha,\beta}$ indépendantes et identiquement distribuées peut être obtenue comme le produit des n termes, comme dans l'équation. 1. La dérivation de ce produit conduit aux estimations de α et β. Il faut noter que le terme ML qui est attribué en standard à cette méthode est utilisé abusivement ici car, dans notre cas, les $X_\Delta(k)$ sont fortement dépendants. Il a d'ailleurs été vérifié de façon empirique à partir de simulations numériques que cette procédure d'estimation donne des résultats très précis, même lorsqu'elle est appliquée à des processus à longue mémoire [SA05].

• **Estimation des paramètres Farima.** Il est établi aujourd'hui que l'estimation du paramètre de mémoire longue est une tâche difficile en statistiques qui a pourtant été largement étudiée (voir [DOT03] par exemple, pour une présentation actualisée). Par conséquent l'estimation conjointe des paramètres de mémoire courte et longue du processus farima(ϕ, d, θ) est une tâche très ardue. Une méthode d'estimation basée sur le maximum de vraisemblance des formes analytiques du spectre dont l'expression est rappelée par l'équation 3 est possible mais sont lourdes en puissance de traitement.

Nous avons donc développé une procédure d'estimation en deux étapes : tout d'abord, nous estimons le paramètre de LRD d en utilisant une méthode basée sur une décomposition en ondelettes. Cette méthode n'est pas détaillée dans cet article. Le lecteur pourra se référer à [AV98, VA99].

Ensuite, à partir de cette estimation à base d'ondelettes $\hat{d_W}$, nous opérons une dérivation fractionnaire d'ordre $\hat{d_W}$ de X_Δ. On élimine ainsi la LRD du processus de sorte qu'il ne reste plus que les composants ARMA. Une procédure itérative classique (basée sur l'algorithme de Gauss-Newton) [Lju99] est alors appliquée pour estimer les paramètres ARMA. Evidemment, la principale faiblesse de cette procedure d'estimation en deux phases se situe au niveau de la qualité de l'estimation de d. Si d est mal estimé, les paramètres ARMA le seront aussi. Toutefois, la qualité des estimations obtenues avec cette procédure a été étudiée numériquement dans [SA05] à partir d'un processus de synthèse de trafic $\Gamma_{\alpha,\beta}$ farima(ϕ, d, θ). Les résultats obtenus sont très bons et valident ainsi cette méthode d'estimation.

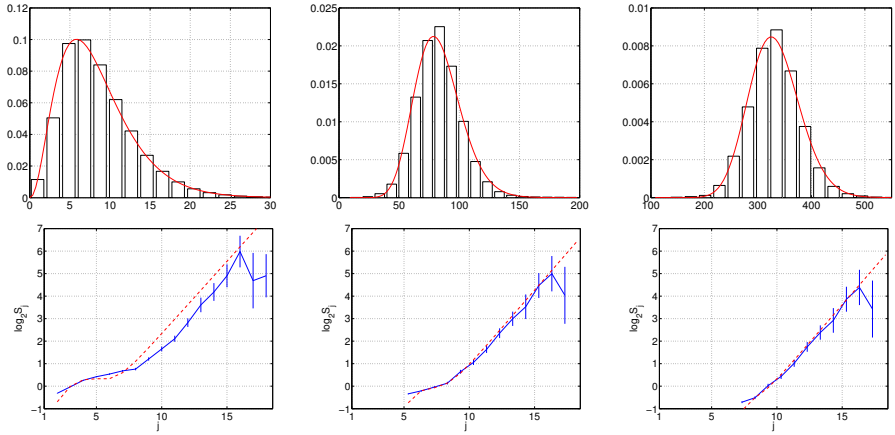


FIG. 3: AUCK-IV. Adéquation des marginales (en haut) et des covariances (en bas) du processus $\Gamma_{\alpha,\beta}$ - farima(ϕ, d, θ) pour $\Delta = 10, 100, 400$ ms (de gauche à droite) ; $j = 1$ correspond à 10 ms.

5 Résultats et discussions

5.1 Trafic sans anomalie

Les procédures d'analyse $\Gamma_{\alpha,\beta}$ - farima(ϕ, d, θ) décrite plus haut ont été appliquées aux séries temporelles du trafic indépendamment pour différents niveaux d'agrégation. Nous présentons ici les résultats détaillés pour les séries issues des traces **AUCK-IV** et **Metrosec-ref1**. Des résultats similaires ont été obtenus pour

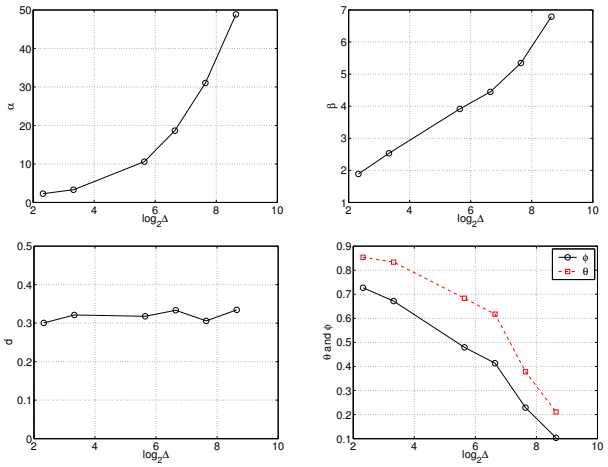


FIG. 4: AUCK-IV. Paramètres estimés du processus $\Gamma_{\alpha,\beta}$ - farima(ϕ, d, θ) en function de $\log_2 \Delta$ (avec Δ en ms).

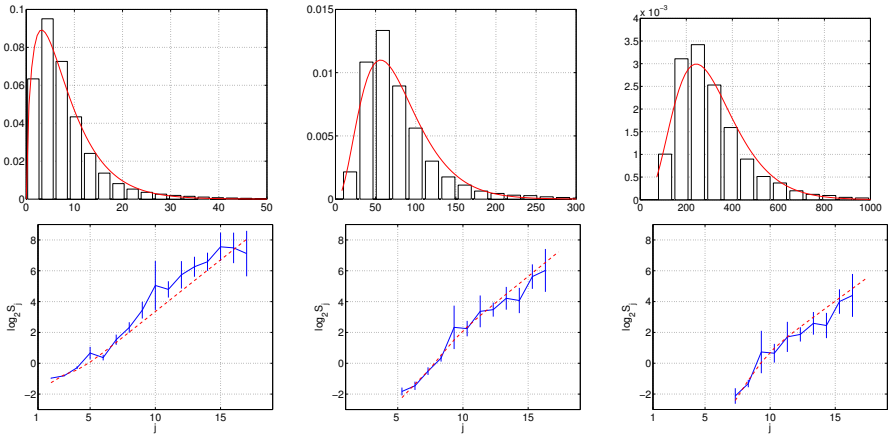


FIG. 5: METROSEC-ref1. Adéquation des marginales (en haut) et des covariances (en bas) du processus $\Gamma_{\alpha,\beta}$ - farima(ϕ, d, θ) pour $\Delta = 10, 100, 400$ ms (de gauche à droite en bas). $j = 1$ correspond à 10 ms.

les autres traces citées dans le tableau 1, mais nous ne les présentons pas dans cet article par manque de place.

• **Marginales.** Pour ces deux séries temporelles, la ligne du haut des Figures 3 et 5 (le modèle et les histogrammes empiriques correspondent), illustrent respectivement l'adéquation des distributions marginales des processus $\Gamma_{\alpha,\beta}$ avec X_Δ pour un large spectre de niveaux d'agrégation : 1ms $\leq \Delta \leq$ 10 s. Cette adéquation a été caractérisée au moyen de tests de χ^2 et de Kolmogorov-Smirnow (non décrits dans l'article). Les distributions Gamma démontrent en général une meilleure adéquation par rapport à celles obtenues avec des lois exponentielles, log-normales ou de χ^2. Pour certaines des séries analysées et certains niveaux d'agrégation, l'une ou l'autre de ces lois peut approximer plus précisément les données que la loi Gamma. Toutefois, les distributions Gamma ne sont jamais très éloignées des données réelles, et même si une distribution particulière approxime mieux les données que la loi Gamma pour un Δ donné, cela n'est pas le cas sur un tout un ensemble de valeurs Δ. A l'opposé, l'adéquation des lois Gamma reste très satisfaisante pour un large spectre de valeurs de Δ, et cela montre une caractérisation des marginales du trafic dépendante de l'échelle d'observation. Les lois $\Gamma_{\alpha,\beta}$, en faisant varier leurs paramètres de formes et d'échelles, offrent une évolution continue et stable d'une loi exponentielle pure vers une loi Gaussienne.

Ensemble, ces observations militent en faveur de l'utilisation de lois Gamma pour modéliser les mar-

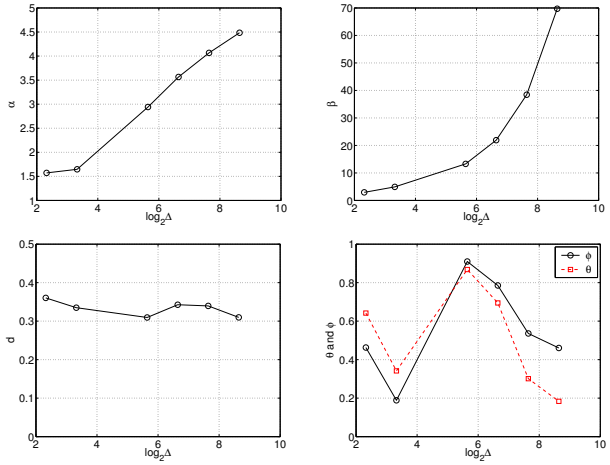


FIG. 6: METROSEC-ref1. Paramètres estimés du processus $\Gamma_{\alpha,\beta}$ - farima(ϕ,d,θ), en fonction de $\log_2\Delta$ (Δ en ms).

ginales du trafic notamment aussi parce que les lois Gamma forment une famille qui reste stable par l'opération d'addition : pour des variables aléatoires indépendantes X_i (avec $i=1,2$), de lois $\Gamma_{\alpha,\beta}$, leur somme $X=X_1+X_2$ suit une loi $\Gamma_{\alpha_1+\alpha_2,\beta}$. Pour l'agrégation $X_{2\Delta}(k)=X_\Delta(2k)+X_\Delta(2k+1)$. En utilisant la propriété de stabilité par addition, et en supposant l'indépendance des lois, α augmente de façon linéaire avec Δ alors que β reste constant. La première ligne (haute) des Figures 4 et 6, montre l'évolution de $\hat{\alpha}$ et $\hat{\beta}$ en fonction de $\log_2\Delta$. Pour toutes les séries temporelles, des écarts significatifs par rapport à ces comportements idéaux sont observés. Une analyse attentive montre que $\hat{\alpha}(\Delta)$ n'augmente pas pour les petites valeurs de Δ, puis augmente quasiment comme $\log_2\Delta$ pour des valeurs de Δ plus grandes, alors que le comportement de $\hat{\beta}(\Delta)$ est proche d'une augmentation en loi de puissance. Ces faits constituent des preuves de l'existence de dépendance dans les données. De plus, il faut noter que $\Delta\simeq 1$ s, correspond au seuil de longue mémoire (comme cela sera discuté plus loin). Cela signifie que les évolutions de α etβ en fonction de Δ montrées ici s'accommodent de la SRD.
Les variations conjointes de α et β en fonction du niveau d'agrégation Δ représentent une propriété significative du trafic normal. Nous allons dans la suite utiliser cette propriété pour caractériser et classifier le trafic avec anomalies.

• **Covariances.** Pour les deux séries de référence, la ligne du bas des figures 3 et 5, comparent respectivement les diagrammes (à échelles logarithmiques) obtenus à partir des données avec ceux obtenus avec le modèle. Ces courbes illustrent l'adéquation des covariances du processus farima(ϕ,d,θ) et de X_Δ.
Lorsque Δ augmente, on peut remarquer que les diagrammes sont quasiment obtenus à partir des diagrammes obtenus pour des Δ plus petits que l'on aurait décalés vers les échelles plus grandes. Ceci s'explique facilement car l'agrégation de données consiste à lisser les détails qui apparaissent à des petites échelles, mais qui n'affectent en rien les grandes échelles. Comme on s'y attendait, l'agrégation n'élimine ni n'altère la caractéristique de longue mémoire. On peut le vérifier sur les Figures 4 et 6 (en bas à gauche), pour lesquelles $\hat{d_W}$ reste indépendant de Δ. Ceci, une nouvelle fois, souligne que la LRD capture un attribut de longue durée sur le trafic qui n'apparait pas pour des échelles intermédiaires.
D'un autre côté, les corrélations à courts termes sont éliminées lorsque le niveau d'agrégation augmente. On peut voir sur les Figures 4 et 6, en bas à droite, que $\hat{\phi}$ et $\hat{\theta}$ baissent de façon significative lorsque Δ augmente. Ils devraient devenir nuls si le niveau d'agrégation Δ devient plus grand que les échelles des caractéristiques de SRD. La covariance converge théoriquement vers celle d'un bruit Gaussien fractionnaire qui s'avère, pratiquement, être extrêmement proche de celle d'un processus farima$(0,d,0)$. Pour toutes les séries temporelles de référence étudiées ici, l'échelle temporelle pour laquelle la mémoire longue est dominante (mesurée comme le niveau d'agrégation approximatif Δ pour lequel la partie SRD du modèle disparait) correspond à 600 ms $\leq\Delta\leq$ 2 s .

• **Conclusions.** En conclusion (partielle), nous avons mis l'accent sur le fait que pour un large ensemble de traces de trafic différentes collectées sur des réseaux différents, le modèle $\Gamma_{\alpha,\beta}$ - farima(ϕ,d,θ) proposé

reproduit précisément les marginales ainsi que les corrélations à court et long terme des séries temporelles. Le fait que le modèle proposé est suffisamment versatile pour travailler efficacement sur tous les niveaux d'agrégation est un élément clé pour deux raisons : 1) un problème récurrent de la modélisation du trafic concerne le choix d'un niveau d'agrégation Δ adapté. C'est une question délicate dont la réponse doit tenir compte des caractéristiques des données, l'objectif de la modélisation, ainsi que de problèmes techniques comme les contraintes de temps réel, de taille des tampons ou les contraintes de coûts de traitement. Par conséquent, choisir Δ a priori peut être très difficile ; l'utilisation d'un processus qui offre une modélisation évolutive en fonction de Δ est donc d'un grand intérêt. 2) les valeurs des paramètres du modèle varient, souvent de façon importante d'un trafic à l'autre. Mais ce ne sont pas les valeurs elles-mêmes qui sont importantes dans ces travaux et pour d'éventuels mécanismes de détection, mais les courbes d'évolution de ces paramètres en fonction de Δ qui offrent des éléments statistiques importants pour l'analyse du trafic.

5.2 Trafic avec anomalies

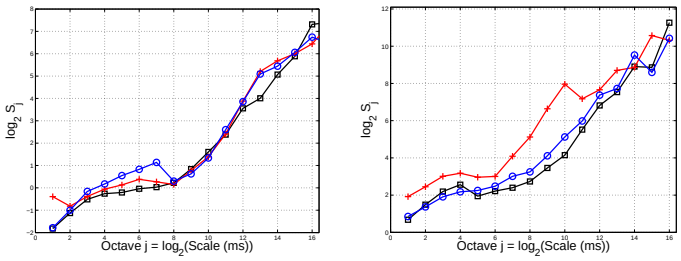


FIG. 7: Diagrammes logarithmiques. Pour la DDoS (gauche) et la Flash Crowd (droite). Pour les deux événements, les courbes sont données pour la période de l'anomalie (croix rouges sur la courbe), avant l'anomalie (carrés noirs) et après (cercles bleus), ces deux derniers cas constituant des références de trafic normal.

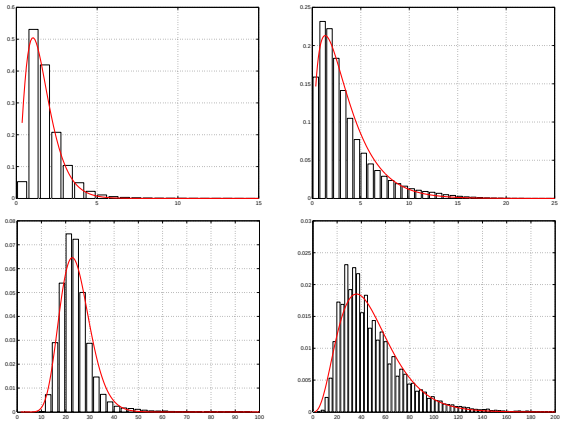


FIG. 8: Marginales. Pour l'attaque DDoS (gauche) et pour la Flash Crowd (droite), adéquation des histogrammes empiriques de X_Δ et les marginales $\Gamma_{\alpha,\beta}$ pour $\Delta = 2$ms (haut) and $\Delta = 32$ms (bas).

• **Attaque DDoS.** Les courbes à gauche de la figure 7, présentent les diagrammes logarithmiques pour des blocs de données d'une heure pendant l'attaque DDoS ($\Delta = 1$ms), par rapport à des blocs d'une heure correspondant à du trafic régulier capturé deux heures avant et après l'attaque. Ces courbes montrent 1) que le modèle farima(ϕ, d, θ) décrit de façon satisfaisante le trafic contenant une attaque DDoS. D'autres courbes, non présentées ici, montre que c'est également le cas pour de nombreux niveaux d'agrégation.
De plus, pour des échelles supérieures à 500 ms ($j = 9$ sur la courbe gauche de la figure 7), aucune différence n'est visible pour les périodes avant/après et pendant l'attaque. En particulier, le paramètre de LRD $\hat{d}_W$ reste étonnamment constant. Cela signifie que la LRD n'est pas créée par l'attaque, mais également qu'elle lui est complètement insensible. La seule différence que l'on remarque sur le diagramme logarithmique est une

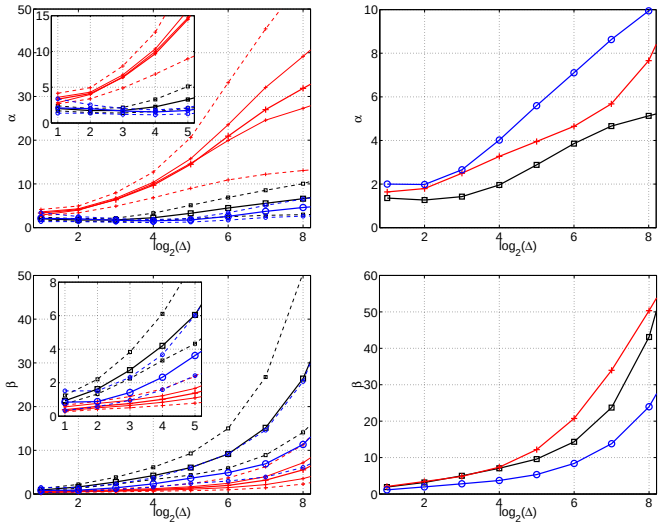


FIG. 9: Estimation des paramètres $\Gamma_{\alpha,\beta}$. Estimation de $\hat{\alpha}$ (haut) et $\hat{\beta}$ (bas) en fonction de $\log_2 \Delta$ pour l'attaque DDoS (gauche) et pour la Flash Crowd (droite). Dans les deux cas, les courbes sont données pour les périodes de l'anomalie (croix rouges), avant (carrés noirs) et après (cercles bleus). Pour l'attaque **DDoS**, l'évolution moyenne des paramètres (ligne épaisse) sur différents blocs de données de 15 min est dessinée et superposée avec les valeurs extrêmes prises pendant chaque période (lignes pointillées). Dans l'exemple, deux évolutions typiques sur un bloc pendant l'attaque sont présentées sur le graphe (lignes fines). Un zoom sur les petites échelles est ajouté. Pour la **FC**, dont la durée est plus courte, une estimation sur une fenêtre de 15 min est rapportée pour chaque période (avant, pendant et après la FC).

augmentation relative du composant de SRD (pour les échelles 4 à 7 de j) après l'attaque : C'est dû au fait que les séries du trafic après l'attaque ont été capturées la nuit, et donc avec une charge de trafic plus faible. Le diagramme logarithmique a été décalé vers le haut pour montrer que le paramètre de LRD $\hat{d_W}$ (donné par la pente) ne change pas, même lorsque la charge du réseau est plus faible, et que par conséquent la partie correspondant aux petites échelles augmente. On ne peut donc pas détecter l'anomalie à partir du diagramme logarithmique.

Les deux courbes de la colonne de gauche sur la figure 8 illustrent que les distributions $\Gamma_{\alpha,\beta}$ se superposent parfaitement aux marginales du trafic avec attaque. Les deux courbes gauche de la figure 9 comparent les évolutions des estimations des paramètres $\hat{\alpha}$ et $\hat{\beta}$ en fonction de Δ pour du trafic pendant (croix rouges), avant (carrés noirs) et après (cercles bleus) l'attaque DDoS. Elles représentent les estimations expérimentales moyennes sur des blocs de données disjoints de 15 minutes, superposées avec les valeurs extrêmes prises par ces estimations durant chaque période. Les fenêtres avant et après l'anomalie correspondent à des comportements nominaux pertinents pour le trafic régulier. On peut voir que les fonctions $\hat{\alpha}(\Delta)$ et $\hat{\beta}(\Delta)$ pendant l'attaque s'écartent significativement des comportements réguliers. Nous insistons sur le fait que les valeurs des paramètres peuvent varier d'un bloc à l'autre, même pendant l'attaque DDoS, mais que les évolutions en fonction de Δ restent comparables et définissent un schéma différent par rapport à celui des traffics normaux.

L'attaque produit une augmentation immédiate et brutale de α dès les petites valeurs de Δ alors que dans des conditions normales α reste constant ou ne présente que des variations limitées, et ce pour $\Delta \simeq 20$ ms. L'évolution de β est à l'opposé : il diminue de $\Delta \simeq 1$ ms à $\Delta \simeq 30$ ms pendant l'attaque DDoS, alors qu'il augmente régulièrement avec Δ dans des conditions normales de trafic.

Ces évolutions peuvent être interprétées différemment, en termes d'occurrence d'un *événement 0 paquet* et d'un effet de *Gaussianisation*. Premièrement, comme pendant l'attaque un grand nombre de paquets sont émis avec un débit le plus élevé possible, une conséquence majeure est la possibilité pour un observateur de ne voir aucun paquet (*0 paquet*) dans une fenêtre de taille Δ qui diminue très vite jusqu'à 0 dès que Δ atteint 1 ms. Plus précisément, on observe que les marginales du trafic avec attaque DDoS ne sont pas nulle seulement au delà d'un seuil qui dépend de Δ. C'est une différence majeure avec les marginales du trafic régulier qui décroissent lentement vers 0 lorsque $X_\Delta \to 0$ (comparer les figures 3 ou 5 avec la figure

8). Cet effet a précisément un impact sur les valeurs prises par le paramètre de forme α en fonction de Δ, impliquant que α croît lentement avec Δ pour le trafic régulier et beaucoup plus rapidement pour celui qui contient une attaque.
Deuxièmement, comme c'est mentionné dans la partie 4.1 plus haut, $1/\alpha$ contrôle l'écart entre les distributions $\Gamma_{\alpha,\beta}$ et Gaussiennes. Avec le niveau d'agrégation, α tend à toujours croître. Toutefois, les attaques DDoS accélèrent cette croissance avec l'effet de *Gaussianisation*. Ceci constitue une particularité statistique majeure qui différencie le trafic avec attaque du trafic régulier. Pour finir, il faut noter que cet effet implique des échelles pour le trafic allant de 1 ms à 0.5 s, et que la partie ARMA du modèle de covariance (les courbes ne sont pas représentées dans cet article par manque de place) ne peut que très difficilement voir cette partie de la covariance.

• **Flash Crowd.** Les deux courbes de droite de la figure 8 illustrent que les distributions $\Gamma_{\alpha,\beta}$ correspondent bien aux marginales du trafic en présence d'une Flash Crowd (FC) et ce pour un large ensemble de niveaux d'agrégation (de 1ms à 1s). Les deux courbes de droite de la figure 8 comparent les évolutions des courbes de $\hat{\alpha}(\Delta)$ et $\hat{\beta}(\Delta)$ pour le trafic pendant (courbe rouge) avant (courbe noire) et après (courbe bleue) la FC. Chaque courbe correspond à des blocs de données de 15 min qui ne se chevauchent pas. Les formes des courbes $\hat{\alpha}(\Delta)$ et $\hat{\beta}(\Delta)$ observées pendant l'événement ne s'écartent pas de façon significative de celles du trafic normal. Quelques écarts existent pour les grandes valeurs de Δ (de 0.5 à 1 s), ce qui est consistent avec les observations faites sur les diagrammes logarithmiques. Cette différence sur $\hat{\alpha}(\Delta)$ observée entre une attaque DDoS et une FC est consistante avec le fait que la FC n'intègre pas de mécanisme tendant à empêcher le phénomène *0 paquet par fenêtre* contrairement à l'attaque DDoS.
La courbe de droite de la figure 7 présente les diagrammes logarithmiques de deux blocs de données de 15 min pendant la FC ($\Delta = 1$ ms) à comparer avec les blocs de données, de 15 min aussi, enregistrés quelques minutes avant et après la FC. Sur cette courbe, on voit nettement un changement sur le diagramme logarithmique pendant la FC. Pour les octaves $j = 8$ à $j = 10$, i.e., pour les échelles de temps allant de 250 ms à 1 s, un fort pic d'énergie apparaît (un tel pic n'a jamais été observé pour du trafic régulier). Naturellement, le processus farima(ϕ, d, θ) (les courbes ne sont pas présentées par manqué de place) échoue à représenter tout à la fois la SRD, la LRD et ce pic d'énergie. Les tests de concordance entre les données et le modèle associé conduit à un rejet, ce qui nous offre en fait un outil pertinent pour détecter ces anomalies. Notons également que le paramètre de LRD d, lorsqu'il est estimé pour des octaves supérieures à celles correspondant au pic d'énergie ne s'écartent pas significativement des valeurs estimées avant et après la FC. Cela signifie que la LRD n'est pas due à la FC et qu'elle n'est pas affectée par la FC. Au pire, le pic d'énergie agit comme un effet masquant dans un sous intervalle d'échelles temporelles, de 250 ms à 2 s.

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

• **Détection.** Une application majeure de ce travail concerne donc la détection en temps réel d'anomalies dans le trafic. Pour une bonne caractérisation statistique, les analyses de la partie 5.1 ont été réalisées sur des blocs d'une heure pour les séries temporelles de référence, et de 15 min pour les séries liées aux attaques et aux FC. De telles durées permettaient des descriptions statistiques précises, mais correspondent naturellement à des durées d'observation trop longues pour satisfaire aux besoins d'une détection rapide des anomalies. Nous développons donc actuellement des outils de surveillance de α, β, θ et ϕ, ainsi que des formes globales des marginales et des diagrammes logarithmiques pour des périodes d'observation plus courtes.

La figure 10 montre l'estimation de $\hat{\alpha}(\Delta)$ sur des fenêtres d'une minute. L'évolution de la moyenne $\hat{\alpha}$ reproduit les caractéristiques soulignées pour des fenêtres de 15 minutes (voir la figure 8), pendant l'attaque

ou pour le trafic de référence (avant et après l'attaque). On voit clairement que la forme de la courbe $\hat{\alpha}(\Delta)$ subit un changement drastique à toutes les échelles pendant l'attaque DDoS. Ce changement pourrait être quantifié au moyen de distances (de type Kullback ou Bhattacharyya par exemple) ou de divergences [Bas89]. De plus, l'analyse étant faite sur des blocs d'une minute, une détection fiable sur un temps très court pourrait être effectuée. Ceci pourrait servir comme un des éléments de base à la conception d'un IDS.

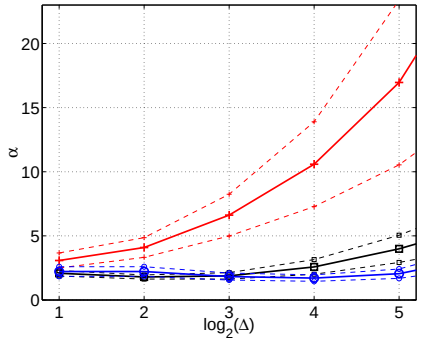


FIG. 10: Attaque DDoS : Moyenne de $\hat{\alpha}$ sur des fenêtres d'une minute. $\hat{\alpha}$ (ligne pleine), et écart maximum (lignes pointillées) en fonction de $\log_2 \Delta$, pendant (croix rouges), avant (carrés noirs) ou après (cercles bleus) l'anomalie.

6 Conclusions et travaux futurs

Dans cet article nous avons introduit un processus non gaussien dépendant à long terme, le $\Gamma_{\alpha,\beta}$ - farima(P,d,Q), Pour modéliser les statistiques de premier et second ordre du trafic des réseaux d'ordinateurs. Nous avons également décrit des procédures d'estimation des paramètres correspondants. Nous avons montré sur un grand nombre de trafics standards de référence qu'il constitue un modèle à la fois pertinent et versatile, et ce pour un grand nombre de niveaux d'agrégation Δ. De plus, ses paramètres évoluent régulièrement avec Δ fournissant ainsi une caractérisation statistique utile du trafic régulier. Nous avons également montré que des écarts par rapport à ces comportements de référence (selon Δ) nous permet de distinguer des trafics avec ou sans anomalies, et aussi de déterminer si les anomalies sont légitimes (flash crowds) ou illégitimes (attaque DDoS).

Ce travail peut être étendu selon plusieurs axes de recherche. En premier, nous allons continuer à explorer le bestiaire des trafics réguliers et avec anomalies en analysant des traces de trafic très récentes, ainsi qu'en provoquant une plus grande variété d'anomalies (attaques DDoS plus avancées et plus diffuses, des flash crowds plus importantes, des pannes de réseau,...). Dans ce but, une plate-forme expérimentale a été mise en place dans le cadre du projet METROSEC. Nous voulons à la fois explorer les possibilités pour notre modèle de caractériser significativement ce grand nombre d'anomalies, et l'enrichir. Deuxièmement, en utilisant les caractérisations statistiques que nous avons faites, nous espérons mettre au point dans un futur proche un mécanisme de détection capable d'identifier automatiquement les changements dans ces caractéristiques statistiques et de les classifier en anomalies légitimes ou illégitimes. Il devrait fonctionner comme un IDS, et se baser sur des fenêtres d'observation temporelle courtes. Notre but ultime est de développer des mécanismes et stratégies réseaux (protocoles, architectures, ...) pour améliorer la robustesse des réseaux aux attaques. Cette insensibilité accrue devrait permettre de maintenir le niveau de QoS requis. Ce travail constitue une première étape vers cet objectif global.

7 Remerciements

Les auteurs remercient le CRI de l'ENS Lyon, L. Gallon (IUT GTR de Mont de Marsan, France) et L. Bernaille (LIP6, Paris 6) pour leur aide dans la collecte de données de trafic et dans la conduite des expérimentations d'attaques. Ils remercient aussi tous les collègues qui ont gracieusement accepté de prendre part à l'expérimentation de foule subite étudiée dans cet article. Enfin, ils remercient ceux qui rendent leurs traces de trafic publiques (Bellcore, LBL, UNC, Auckland Univ, Univ North Carolina,

CAIDA). Ils remercient spécialement S. Marron, F. Hernandez-Campos et C. Park de l'UNC, USA, D. Veitch et N. Hohn du CubinLab, University of Melbourne, Australie pour avoir pré-formaté certaines des series temporelles utilisées ici. Ce travail a été rendu possible grace au support financier du MNRT dans le cadre du programme ACI *Sécurité et Informatique* 2004, qui soutient le projet METROSEC.

Références

[AN98] A. Andersen and B. Nielsen. A Markovian approach for modelling packet traffic with long range dependence. *IEEE journal on Selected Areas in Communications*, 5(16) :719–732, 1998.

[AV98] P. Abry and D. Veitch. Wavelet analysis of long-range dependent traffic. *IEEE Trans. on Info. Theory*, 44(1) :2–15, January 1998.

[Bas89] M. Basseville. Distance measures for signal processing and pattern recognition. *Signal Processing*, 18 :349–369, 1989.

[Ber94] J. Beran. *Statistics for Long-memory processes*. Chapman & Hall, New York, 1994.

[BKPR02] P. Barford, J. Kline, D. Plonka, and A. Ron. A signal analysis of network traffic anomalies. In *ACM/SIGCOMM Internet Measurement Workshop*, Marseille, France, November 2002.

[Bru00] J. Brutlag. Aberrant behavior detection in time series for network monitoring. In *USENIX System Administration Conference*, New Orleans, December 2000.

[BTI+02] C. Barakat, P. Thiran, G. Iannaccone, C. Diot, and P. Owezarski. A flow-based model for internet backbone traffic. In *ACM/SIGCOMM Internet Measurement Workshop*, pages 35–47, New York, NY, USA, 2002. ACM Press.

[CKT02] C-M. Cheng, H.T. Kung, and K-S. Tan. Use of spectral analysis in defense against DoS attacks. In *IEEE Globecom*, Taipei, Taiwan, 2002.

[DOT03] P. Doukhan, G. Oppenheim, and M.S. Taqqu. *Long-Range Dependence : Theory and Applications*. Birkhäuser, Boston, 2003.

[EHP00] M. Evans, N. Hastings, and B. Peacock. *Statistical Distributions*. Wiley (Interscience Division), June 2000.

[ENW96] A. Erramilli, O. Narayan, and W. Willinger. Experimental queueing analysis with long-range dependent packet traffic. *ACM/IEEE transactions on Networking*, 4(2) :209–223, 1996.

[FBGO05] S. Farraposo, K. Boudaoud, L. Gallon, and P. Owezarski. Some issues raised by DoS attacks and the TCP/IP suite. In *SAR' 2005*, Batz-sur-mer, France, June 2005.

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

[HDLK95] C. Huang, M. Devetsikiotis, I. Lambadaris, and A. Kaye. Modeling and simulation of self-similar Variable Bit Rate compressed video : a unified approach. In *ACM SIGCOMM*, Cambridge, UK, August 1995.

[HHP03] A. Hussain, J. Heidemann, and C. Papadopoulos. A framework for classifying denial of service attacks. In *SIGCOMM*, Karlsruhe, Germany, 2003.

[HS94] G.J. Hahn and S.S. Shapiro. *Statistical Models in Engineering*, page 88. Wiley (Interscience Division), June 1994.

[JKR02] J. Jung, B. Krishnamurthy, and M. Rabinovich. Flash Crowds and Denial of Service Attacks : Characterization and Implications for CDNs and Web Sites. In *International WWW Conference*, Honolulu, HI, May 2002.

[JY04] S. Jin and D. Yeung. A covariance analysis model for DDoS attack detection. In *IEEE International Conference on Communications*, Paris, France, June 2004.

[KKJB05] S. Kandula, D. Katabi, M. Jacob, and A. Berger. Botz-4-sale : survicing organized DDoS attacks that mimic Flash Crowds. In A. Vahdat and D. Wetherall, editors, *USENIX' NSDI'05*, Boston, MA, May 2005.

[KMFB04] T. Karagiannis, M. Molle, M. Faloutsos, and A. Broido. A non stationary Poisson view of the internet traffic. In *INFOCOM*, 2004.

[LCD04] A. Lakhina, M. Crovella, and C. Diot. Diagnosing network-wide traffic anomalies. In *SIGCOMM*, August 2004.

[Lju99] L. Ljung. *System identification : theory for the user*, chapter 10.2. PTR Prentice Hall, 1999.

[LL03] L. Li and G. Lee. DDoS attack detection and wavelets. In *International Conference on computer communications and networks*, August 2003.

[LTWW94] W. E. Leland, M. S. Taqqu, W. Willinger, and D. V. Wilson. On the self-similar nature of ethernet traffic (extended version). *ACM/IEEE transactions on Networking*, 2(1) :1–15, February 1994.

[Mel93] Benjamin Melamed. An overview of TES processes and modeling methodology. In *Performance/SIGMETRICS Tutorials*, pages 359–393, 1993.

[MVS01] D. Moore, G.M. Voelker, and S. Savage. Inferring internet denial-of-service activity. In *Usenix Security Symposium*, 2001.

[Nor95] I. Norros. On the use of fractional Brownian motion in the theory of connectionless networks. *IEEE journal on Selected Areas in Communications*, 13(6), 1995.

[Pax99] V. Paxson. Bro : a system for detecting network intruders in real-time. *Computer Networks Journal*, 31(23–24) :2435–2463, 1999.

[PF95] V. Paxon and S. Floyd. Wide-area traffic : The failure of Poisson modeling. *ACM/IEEE transactions on Networking*, 3(3) :226–244, June 1995.

[PKC96] K. Park, G. Kim, and M. Crovella. On the relationship between file sizes, transport protocols, and self-similar network traffic. In *International Conference on Network Protocols*, page 171, Washington, DC, USA, 1996. IEEE Computer Society.

[PW00] K. Park and W. Willinger. Self-similar network traffic : An overview. In Kihong Park and Walter Willinger, editors, *Self-Similar Network Traffic and Performance Evaluation*, pages 1–38. Wiley (Interscience Division), 2000.

[QoS] QoSMOS Traffic Designer. http ://www.qosmos.net.

[SA05] A. Scherrer and P. Abry. Marginales non gaussiennes et longue mémoire : analyse et synthèse de trafic Internet. In *Colloque GRETSI-2005*, Louvain-la-Neuve, Belgique, September 2005.

[TG98] B. Tsybakov and N.D. Georganas. Self similar processes in communications networks. *IEEE Trans. on Info. Theory*, 44(5) :1713–1725, 1998.

[TTW97] M. Taqqu, V. Teverosky, and W. Willinger. Is network traffic self-similar or multifractal ? *Fractals*, 5(1) :63–73, 1997.

[VA99] D. Veitch and P. Abry. A wavelet based joint estimator of the parameters of long-range dependence. *IEEE Trans. on Info. Theory special issue on "Multiscale Statistical Signal Analysis and its Applications"*, 45(3) :878–897, April 1999.

[VA01] D. Veitch and P. Abry. A statistical test for the time constancy of scaling exponents. *IEEE Transactions on Signal Processing*, 49(10) :2325–2334, October 2001.

[VL89] H.S. Vaccaro and G.E. Liepins. Detection of anomalous computer session activity. In *IEEE Symposium on Security and Privacy*, pages 280–289, Oakland, California, May 1989.

[Ye00] N. Ye. A Markov chain model of temporal behavior for anomaly detection. In *Workshop on Information Assurance and Security*, West Point, NY, June 2000.

[YM04] J. Yuan and K. Mills. DDoS attack detection and wavelets. Technical report, National Institute of Standards and Technology, 2004.

[ZRMD03] Z. Zhang, V. Ribeiro, S. Moon, and C. Diot. Small time scaling behavior of internet backbone traffic : an emprirical study. *INFOCOM*, March 2003.