NON-LINEAR REGRESSION FOR BIVARIATE SELF-SIMILARITY IDENTIFICATION - APPLICATION TO ANOMALY DETECTION IN INTERNET TRAFFIC BASED ON A JOINT SCALING ANALYSIS OF PACKET AND BYTE COUNTS

Jordan Frecon\textsuperscript{1}, Romain Fontugne\textsuperscript{2,3}, Gustavo Didier\textsuperscript{4}, Nelly Pustelnik\textsuperscript{1}, Kensuke Fukuda\textsuperscript{2}, Patrice Abry\textsuperscript{1,2,3}

\textsuperscript{1} CNRS, Physics Department, ENS Lyon, France, firstname.lastname@ens-lyon.fr
\textsuperscript{2} The National Institute of Informatics, Tokyo, Japan, firstname@nii.ac.jp
\textsuperscript{3} Japanese French Laboratory for Informatics, Tokyo, Japan,
\textsuperscript{4} Mathematics Department, Tulane University, New Orleans, USA, gdidier@tulane.edu

Supported by ANR BLANC 2011 AMATIS BS0101102,
PA and RF acknowledge specific supports from NII\textsuperscript{1}, ENS de Lyon\textsuperscript{3} and JFLI\textsuperscript{2}

ABSTRACT

Internet traffic monitoring is a crucial task for network security. Self-similarity, a key property for a relevant description of Internet traffic statistics, has already been massively and successfully involved in anomaly detection. Self-similar analysis was however so far applied either to byte or Packet count time series independently, while both signals are jointly collected and technically deeply related. The present contribution elaborates on a recently proposed multivariate self-similar model, Operator fractional Brownian Motion (OfBm), to analyze jointly self-similarity in bytes and packets. A non-linear regression procedure, based on an original Branch & Bound resolution procedure, is devised for the full identification of bivariate OfBm. The estimation performance is assessed by means of Monte Carlo simulations. Further, an Internet traffic anomaly detection procedure is proposed, that makes use of the vector of Hurst exponents underlying the OfBm based Internet data modeling. Applied to a large set of high quality and modern Internet data from the MAWI repository, proof-of-concept results in anomaly detection are detailed and discussed.

Index Terms—Internet traffic, anomaly detection, bivariate self-similarity, non linear regression, branch and bound.

1. INTRODUCTION

Internet traffic monitoring. Internet traffic monitoring and modeling constitute crucial tasks for network engineering and design, resource allocation, performance and service optimization, and for security assessment. Notably, anomalous traffic detection has received a considerable amount of attention and research efforts, as malicious traffic may have dramatic consequences both for users and operators. Anomaly detection in Internet traffic context is however highly challenging, because of the strongly heterogeneous natures of networks, applications, protocols and user behaviors. Normal or legitimate traffics may per se show a large diversity, whose actual definition remains a difficult issue. Anomalous behaviors may correspond to an even larger level of heterogeneity, from the known Distributed Denial of Service (DDoS) and port scanning to the potential occurrence of behaviors never encountered before, cf. e.g., \cite{1,2,3} for reviews. In addition, the nature of the available data may depend on the network or on the operator, consisting either of systematic IP (Internet Protocol) packet timestamps, volume in bytes, and 5-tuple\textsuperscript{4} or of higher granularity recordings (applications, protocol...). The present work analyzes times series consisting of the counts of IP Pkt $Y_{Pkt,\Delta}(t)$ (or of bytes $Y_{Byte,\Delta}(t)$) in consecutive time bins, of size $\Delta$, obtained from packet header traces only.

Related works: anomaly detection. The literature dedicated to anomaly detection in Internet traffic is huge (cf. e.g., \cite{1,2,3,4,5} for reviews) and an exhaustive description is out of the present scope. The focus here is on anomaly detection based on aggregated time series, thus respecting privacy, as opposed to techniques that rely on packet payload examination. Because of the ever changing nature of Internet traffic, extracting a reference for normal traffic against which anomalies could be compared is an almost impossible task. Instead, random projection tools, also referred to as hashing procedures or sketching, were used for the automated construction of self-referenced traffic \cite{6} and \cite{7}. Often, anomaly detection relies on the statistical modeling of regular traffic. Amongst numerous attempts, self-similarity and fractional Brownian motion (fBm) \cite{8} have been shown to provide relevant and robust models for Internet traffic statistics across a large variety of networks, traffics and from the early ages of Internet to the most recent data collections \cite{9,10,11,12,13}. In essence, self-similarity implies that Internet traffic temporal dynamics are not driven by specific and characteristic time scales, but rather involve a large continuum of time scales, whose relation is quantified by the so-called Hurst parameter $H$, often empirically found in $H \in (0.8, 1)$). So far, however, in most anomaly detection procedures relying on self-similarity, analysis and modeling remained univariate: Byte and Pkt aggregated count time series were analyzed independently, cf. \cite{9,10,11,12,13}. It is even often much debated and controversial to decide whether self-similarity analysis should be conducted on byte-counts or packet-counts time series. Often, parameters $H$ measured on each type of data differ, thus calling into question the validity of the celebrated queuing mechanism that relates self-similarity to the heavy tailed nature of the distributions of the objects to be distributed on the Internet (cf. e.g., \cite{14,15,16,17}) or raising questions such as: Do the mechanisms apply to packet, bytes, both? if so, why should $H$ differ between packet and bytes? To address such issues, the joint availability of Pkt and Byte count time series has rarely been exploited in bivariate self-similarity analysis, see a contrario \cite{18} and \cite{7} for a

\textsuperscript{1}The standard 5-tuple consists of five IP packet header fields: IP address and port number for source and destination, and IP protocol carried (TCP, UDP or ICMP).
preliminary comparisons of self-similarity exponents computed independently on $Y_{p(t)}(t)$ and $Y_{H(t)}(t)$.  

**Goals, contributions and outline.** The present contribution makes use of a recently proposed multivariate self-similar model, Operator Fractional Brownian motion (OBFM) [19, 20], to model joint self-similarity of bytes and packets as well as to construct an anomaly detection procedure that exploits OBFM parameters. The definition of OBFM is detailed in Section 4 and complemented with the study of its wavelet analysis, that incorporates an original tunable *fractional integration* parameter that permits coping with the specific nature of Internet data. Another specificity of the present work consists in formulating the estimation of the full set of OBFM parameters as a non linear regression (cf. Section 5). In addition, an original Branch & Bound procedure is devised to minimize the corresponding functional. The estimation performance is assessed by means of Monte Carlo simulations conducted on synthetic OBFM, that Mimic Internet data properties. An anomaly detection procedure is then constructed on OBFM parameters estimated from bytes and packets time series, and applied to a large set of high quality and recent Internet data, from the MAWI repository [21], described in Section 5. Results are discussed in Section 6.

2. BIVARIATE OBFM AND WAVELET ANALYSIS

**Definitions.** The general definitions of OBFM can be found in [22] as the only multivariate Gaussian self-similar process with stationary increments. The definitions here are restricted to the class of bivariate time-reversible OBFM $\{Y(t) = (Y_1(t), Y_2(t))\} \subset \mathbb{R}$. Let $\{X(t) = (X_1(t), X_2(t))\} \subset \mathbb{R}$ denote 2 fBms, with auto and cross-covariance functions written as: $\Sigma_X(p,p')/2[t]^{H+H'+\rho} = \Sigma_H^{H+H'+\rho}[t-s]^{H+H'}$. (1) 

with $(p, p') \in \{1, 2\}^2$, $0 < H_1 \leq H_2 < 1$, and where $\Sigma_X = EX_1X_1'(1)$. Process $X$ is well defined if and only if [23]:

$$g(H_1, H_2, \rho_X) = [2H_1 + 1]^{1/2} \pi (\pi H_1 \pi H_2 - \rho_X^2 (\pi H_1 + H_2 + 1)^2 sin^2 \pi (H_1 + H_2)/2)] > 0. \quad (2)$$

Further, let $W$ denote a $2 \times 2$ invertible matrix, then $\{Y(t) = (Y_1(t), Y_2(t))\} \subset \mathbb{R}$ defined as $\{Y(t)\} \subset \mathbb{R}$ is called processes parameterized of $Y(t)$, in 7 parameters accounting for under-determinations, $\Theta = (H_1, H_2, \rho_X, \sigma_{x_1}, \sigma_{x_2}, \beta, \gamma)$, has been proposed [24, 25]:

$$W = \left( \begin{array}{c} 1 \sqrt{1 + \gamma^2} \\ \sqrt{1 + \beta^2} \end{array} \right) . \quad (3)$$

**Wavelet analysis.** Let $Y^\delta(t)$ denote the increment process of $Y: Y^\delta_p(t) = Y_p(t+1) - Y_p(t)$, $p = 1, 2$. The multivariate discrete wavelet transform (DWT) of $Y^\delta$, $(D_{\psi}(\psi, k, j), D_{\psi}(j, k))$, is defined as:

$$D_{\psi}(j, k) = \int_{\mathbb{R}} \psi_{j,k}(t) Y^\delta_p(t) dt. \quad (4)$$

where $\{\psi_{j,k}(t) = 2^{-j(0.5 - \mu)} \psi_0(2^{-j/2}t - k)\}$ denotes the collection of dilated and translated templates of $\psi_0$, an oscillating reference pattern with joint time and frequency localization. It is referred to as the mother wavelet and further characterized by its number of vanishing moments $N_0$, a positive integer, defined as $N_0 = 0, 1, \ldots, N_0 - 1, \int_{\mathbb{R}} t^N \psi_0(t) dt = 0$ and $\int_{\mathbb{R}} t^N \psi_0(t) dt \neq 0$. For a detailed introduction to wavelet transforms, interested readers are referred to e.g., [24]. We have introduced an additional parameter $\mu$ (compared to classical definition) which acts as a fractional integration parameter [23] and whose practical crucial role is detailed in Section 5.

**Univariate analysis.** Let $Y^\delta_p(t)$ denote the increment process of $Y: Y^\delta_p(t) = Y_p(t+1) - Y_p(t)$, $p = 1, 2$. The multivariate discrete wavelet transform (DWT) of $Y^\delta$, $(D_{\psi}(\psi, k, j), D_{\psi}(j, k))$, is defined as:

$$\Theta_d = \arg \min_{\Theta \in \mathbb{Q}} \left\{ \sum_{p'=1}^2 \sum_{j=0}^2 \left( \log_g \left| (S_p, \psi_{p,n}) \theta - \log \left| (E_{p,\mu}(\Theta)) \right| \right) \right\}^2, \quad (10)$$

where the linear logarithm ensures that all scale $2^j$, $j \in \{1, \ldots, j_2\}$ contribute equally. Minimizing Eq. 10 is intricate because of the non convexities of both the implied functional (as a mixture of power laws) and the search space (due to Constraint 4).

$$Q = \{ \Theta = (H, H_2, \rho_X, \sigma_{x_1}, \sigma_{x_2}, \beta, \gamma) \in \mathbb{R}^7 : \Theta \in [0, 1]^3 \times [0, \sigma_{x_1}]^2 \times [-1, 1], g(H, H_2, \rho_X) > 0, H_1 \leq H_2 \}, \quad (11)$$

Branch & Bound optimization. To find the global minimizer $\Theta$ in Eq. 10 the second originality of this work is to resort to a Branch & Bound (B&B) procedure [23], as devised and studied in [25]. The B&B procedure avoids greedy searches by smart enumerations that stem from the repetition of the following steps until a stopping criterion is reached: 1) Partitioning: Choose any region $\mathbb{R}$ from the search
space and divide it into two smaller regions $R_a$ and $R_b$; ii) Bound-
ing: Compute lower and upper bounds of the objective function in
Eq. 10 on $R_a$ and $R_b$. Lower bounds are obtained by interval arith-
metic (cf. [10]), a technique that combines elementary operations to
produce rough lower bounds; iii) Pruning: Discard regions that do
not satisfy Eq. 2 and regions whose lower bound is larger than the
smallest upper bound. The corresponding algorithm solving (10) is
fully detailed in [26] and MATLAB routines will be made publicly
available at the time of publication.

**Estimation performance.** The estimation performance of the
proposed B&B procedure is assessed by Monte Carlo simulation.
The procedure is applied to independent copies of synthetic
OdBm, whose sample size ($N \simeq 3600$) and parameter settings
($1 \simeq H_2 \simeq H_1 \simeq 0.8$, cf. Fig. 4) and $\hat{\rho} = 0.8$ match those observed
or expected for the Internet traffic analyzed here $|H_2 - H_1| = 0$
or $|H_2 - H_1| \simeq 0.2$, with or without mixing $W$. Synthesis and
analysis procedures were devised by ourselves. The quality of the
estimation performance is quantified in Fig. 4 which shows that
whereas correlation and mixing parameters remain difficult to esti-
mate for short time series, and settings that mimic Internet traffic,
while $H_1$ and $H_2$ are always well estimated.

![Fig. 1. Estimation performance on synthetic OdBm, for four
configurations potentially matching Internet Traffic: $(H_1, H_2) = (0.9, 0.9)$ or $(0.7, 0.9), (\beta, \gamma) = (0, 0)$ or $(0.5, 0.5)$.](image)

4. MAWI DATABASE AND RANDOM PROJECTIONS

**MAWI database.** The MAWI repository [21, 31] is an on-going
collection of Internet traffic traces, captured within the WIDE back-
bone network (AS2500) that connects Japanese universities and
research institutes to the Internet. Packet 5-tuple and timestamps,
collected daily from 14:00 to 14:15 (Japanese Standard Time),
are anonymized and made publicly available. Each trace contains
roughly 100 to 150 million IP packets.

**Random projections.** As discussed in Section 4 a major issue in
anomaly detection consists in defining and computing a reference
normal traffic for comparisons. Yet, the ever varying nature of
Internet traffic precludes the use of traffic collected another day or from
another network [4, 7]. Instead, the use of random projections (or
sketches) [6] has been shown to be a relevant procedure to con-
struct self-reference of normal traffic. In random projections, each IP
packet is attributed to one of the $M$ outputs of a hash table [32],
acting on one selected element of the 5-tuple (here the IP Source
address). Therefore, all packets of any given flow with the same IP
Source address are allocated together to the same randomly chosen
entry in the hashtable. Traffic is hence split into $M$ sub-traffic.
When traffic contains no anomaly, all sketches are expected to be
statistically equivalent. When traffic contains some anomalies, asso-
ciated to one same IP Source address, all corresponding packets are
associated to the same sketch, while all other sketches are anomaly
free. Comparisons across sketches can then be used to construct
reference statistics for normal traffic and hence to detect anomalies.

**Fractional integration.** While in OdBm model, theoretically
$0 < H_1 \leq H_2 < 1$, estimated $H$ for normal traffic takes large
values, close to 1, as well documented in [4, 7]. This practically
raises severe issues with respect to the proposed B&B procedure
described above, as some data may randomly and accidentally lead
to $H$ that exceeds the allowed range. This is illustrated in the reports
of univariate based estimates of $H$ (bottom row in Fig. 3), since
univariate wavelet based estimation does not force $H \in (0, 1)$ (cf.
[4, 5]). Fig. 3 both shows that the practical possibility of decoupling
and tuning parameters $0 < H_{BW} = 1/2$ and $|\mu_B - \mu_W|$ is an original
and practically efficient trick in the proposed procedure that permits
to adjust to the specificities of real world data.

5. ODBM MODELING AND ANOMALY DETECTION

**Setting.** Results are reported here for four traces collected on four
different days, in 2008, 2013, 2014 and 2015, as typical and very
recent examples of Internet traffic for the case study intended here.
Hash tables with $M = 16$ outputs are used. Sketches are aggregated
at $\Delta t = 0.258$ as it is now well documented that in Internet
traffic, self-similarity develops across scales ranging from seconds
to hours [12, 4, 7]. Examples of aggregated sketches are illustrated
in Fig. 2 both for packets (first column) and bytes (last column).
Wavelet analysis is conducted using least asymmetric orthogonal
Daubechies wavelets with $N_\psi = 2$ vanishing moments [27]. The
minimization of Eq. 10 is conducted using scales $j_1 = 3$ to $j_2 = 8$,
corresponding respectively to time scales ranging from 2s to 1min
(as available data are limited to 15min durations). Although the
full identification of Biv-OfBm requires 7 parameters, we focus here
on the estimation of the 5 most interesting parameters, namely
$\Theta = (H_1, H_2, \beta, \gamma, \rho_B)$ and set $\sigma_2 = \sigma_{x_2} = 1$ by a priori data
normalization. Estimation of $\Theta$ is done based on the proposed B&B
procedure for each sketch of each dataset.

**Metadata and ground truth.** Metadata regarding anomalies in
Internet MAWI traffic were provided to us by experts via the out-
puts of a computerized procedure, MawiLab [33], inspecting the
content of Internet traffic in an automated and systematic manner:
MawiLab relies on the combined use of several benchmark anomaly
estimators. It is worth emphasizing that these metadata thus do not
constitute the ground truth but only indications against which the
outputs of the proposed detection procedure can be compared.

**Internet traffic statistical modeling with Biv-OfBm.** Fig. 2 illus-
trates a posteriori that the joint statistics of packet and byte counts,
empirically estimated using $S_{p,p'}(j)$, match well Biv-OfBm model
$E_{p,p'}(\Theta)$, with parameters $\Theta$ estimated using the proposed B&B
minimization procedure. It also shows that OdBm models equally
relevantly sketch with and without anomalies, yet with obviously
different estimated parameters $\Theta$. Fig. 2 shows that the use of the
chosen 5 parameter parametrization is satisfactory.

**Anomaly detection.** Parameters $\Theta$ estimated for each sketch and
each trace were compared with the available MawiLab anomaly
metadata. First inspections, not reported here for space reasons,
show that the estimated correlation $\rho$ and mixing $\beta$ and $\gamma$ parame-

Packets do not seem to correlate well with the occurrence of anomalies. This may partly be explained by the poor estimation performance for these parameters, as observed in Monte Carlo simulations, in a comparable setting. This analysis however clearly indicates that mixing parameters $\beta$ and $\gamma$ significantly depart from 0, thus showing the need for bivariate estimation for a non-biased estimation of parameters $H_1$ and $H_2$. Comparison of top and bottom rows in Fig. 4 shows significant discrepancies between the univariate estimates ($H^U_{byt}$, $H^U_{pkt}$) and the bivariate ones ($H_1$, $H_2$), which clearly illustrate the limitations and biases of univariate analysis.

The inspection of $H_1$ and $H_2$ estimated from the bivariate B&B procedure tends to show that large departures of $|H_2 - H_1|$ from 0, match a significant number of sketches marked by MawiLab as containing a large number of anomalous packets, cf. Fig. 5 top row. A close inspection of Fig. 5 shows that the agreement between departures from 0 and occurrences of anomaly is not perfect, which may have two origins: As mentioned above, metadata are not the ground truth, and some anomalies might have been missed by MawiLab procedure. Alternatively, some anomalies relevantly detected by MawiLab may not be signalled by a departure of $|H_2 - H_1|$ from 0 which may in turn indicate specific subclasses of anomalies. These discrepancies, requiring deeper expert inspection, will be further investigated. However, expert inspections indicate that i) the Trinocular anomaly, specific to a computer network experiment being run on the MAWI network [34], is systematically detected; ii) 96% of Deny-of-Service attacks were detected for 2013; and iii) 100% of Heavy Hitter anomalies were detected in 2014.

These case study results are altogether very encouraging and consistent with the queuing mechanism connecting self-similarity to heavy tail distribution of Internet objects proposed in [15, 16, 17] that leads to predict identical Hurst exponents for packets and bytes. They are also consistent with prior empirical results, relying on univariate analysis of bytes and packets that tend to comfort $H^U_{byt} \approx H^U_{pkt}$ for normal traffic, while departures of $H^U_{byt}$ from $H^U_{pkt}$ may indicate anomalies [18, 19].

6. CONCLUSIONS AND PERSPECTIVES

The present contribution promotes the use of multivariate models for self-similarity, such as OBFm and proposes, to the best of our knowledge, the first procedure for the full identification of OBFm. It consists of a non-linear regression on log wavelet coefficients, solved by an original Branch and Bound procedure. Numerical simulations conducted on independent copies of synthetic OBFm show that the propose procedure achieves, in parameter settings that match those observed in Internet traffic, satisfactory performance for the estimation of the Hurst exponents $H_1$ and $H_2$, while the estimation of the correlation and mixing parameters turns more difficult in such settings. MATLAB procedures implementing analysis and synthesis will be made publicly available at the time of publication.

It is then shown that bivariate OBFm constitutes a relevant model to describe jointly the scale invariance properties observed in Internet traffic for both packet and byte time series. It also shows that OBFm is relevant both for regular or normal traffic and for traffic with anomalies. These per se original results permit to conduct an anomaly detection case study, which in turn provides significant evidence that certain types of anomalies are marked by a significant discrepancy between $H^U_{byt} \approx H^U_{pkt}$. Results are satisfactory enough to call for a large scale systematic study, with enriched metadata, that may permit not only the detection of anomalies but also the classification of the types of anomalies that can be detected by a change in their scale invariance properties. This is under current investigation.
7. REFERENCES


