Traffic monitoring in TCP/AQM networks through a time delay observer

Yassine Ariba, Frédéric Gouaisbaut, Sandy Rahme, Yann Labit

▶ **To cite this version:**

Yassine Ariba, Frédéric Gouaisbaut, Sandy Rahme, Yann Labit. Traffic monitoring in TCP/AQM networks through a time delay observer. IET Control Theory and Applications, 2012, 6 (4), pp.506-517. hal-01229615

HAL Id: hal-01229615
https://hal.science/hal-01229615

Submitted on 17 Nov 2015

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

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

Traffic monitoring in TCP/AQM networks through a time delay observer

Yassine Ariba[1,2], Frédéric Gouaisbaut[1,2], Sandy Rahme[1,2] and Yann Labit[1,2]

[1] Université de Toulouse; UPS, INSA, INP, ISAE; LAAS; 118 Route de Narbonne, F-31062 Toulouse, France.

[2] LAAS; CNRS; 7, avenue du Colonel Roche, F-31077 Toulouse, France.

{yariba,fgouaisb,srahme,ylabit}@laas.fr

Abstract

The use of the control theory tools for traffic control in communication networks, e.g. the congestion control in IP (Internet Protocol) routers, has given rise to challenging issues in the time-delay system framework. In this paper, we propose to design a linear time-delay observer for traffic monitoring in TCP/AQM (Transmission Control Protocol/Active Queue Management) networks. More precisely, we focus on a bottleneck topology consisting of long-lived TCP communications through a controlled router. The developed mechanism, located at the router, aims at supervising the network via TCP flow estimations as well as detecting anomalies for a class of DoS (Denial of Service) attacks. This issue is formulated as a stability problem for multiple delayed systems and appropriate robust control tools such as quadratic separation are adopted to address it. Then, some simulations via the network simulator NS-2 and an emulation experiment support the proposed methodology.

1 Introduction

Internet provides the major communication media allowing several network applications ranging from web browsing, file exchanges to on-line games or IP telephony. TCP is currently the dominant transport protocol for end-to-end communications and congestion control. It adjusts its sending rate according to Additive-Increase Multiplicative-Decrease (AIMD) mechanism in response to packet losses in the network [14]. Traffic flows in the Internet are generally classified into two major categories: long-term TCP flows characterized by long duration and controlled by the AIMD algorithm (e.g. FTP bulk file transferts), and short bursty flows (HTTP, UDP short transactions) unresponsive to congestion signals from the network. For the last decade, traffic monitoring has become a critical issue for the communication supervision, the analysis of the QoS (Quality of Service) or even for the detection of security breaches. Two techniques

can be roughly identified:

Active monitoring [24] consists of generating probes into the network, and then observing the impact of network components and protocols on traffic: loss rate, delays, RTT (Round Trip Time), capacity... However, since an additional traffic (probes) is injected into the network, the major drawback is the disturbance induced by a such traffic affecting inevitably the current traffic. Intrusiveness of probe traffic is thus one of the key features that active monitoring tools have to focus on.

Secondly, passive monitoring [5] refers to network measurements with appropriate devices located at some relevant point in the network. Passive monitoring is performed on some traffic captures and an off-line analysis assesses network features. It provides a non-intrusive method but not enough reactive.

Regarding the security problems, network anomalies typically refer to circumstances when network operations deviate from the expected behavior. Network anomalies can be roughly classified into two categories. The first category is related to network failures and performance problems (like file server failures or broadcast storms). The second major category of network anomalies is security-related problems (like DoS or DDoS attacks) in detecting active security threats. A variety of tools for anomaly detection are mainly based on data packet signatures (i.e. specific formats of packages, packet headers) and the use of statistical profiles of the traffic. The natural variability of the traffic [22] produces important fluctuations of these measurements, inducing thus several false positives (false alarms) and false negatives (missed detections). Some studies have taken into account a richer form of the statistical structure of the traffic (correlation, spectral density ...) to design IDS or ADS (Intrusion or Anomaly Detection System) [12], [17].

Recent works [8], [2] have suggested to deal with the anomalies diagnosis in a control theory framework. The authors of [8] have developed a nonlinear analysis based on flatness methods to detect a fault signal in TCP/RED networks. In [2], an observer for time-delay systems, based on the Lyapunov method, is designed for traffic estimation. However, these results are restricted to homogeneous users that experienced the same RTT and use a simplistic model of TCP [20] that neglects some delays. In this paper, we pursue the work of [2] considering now different communication delays associated to the different users. We focus our study on the supervision over a bottleneck supporting long-lived TCP flows and an AQM system for congestion control [25]. First, a dynamical model that describes the TCP flow rates behavior as well as a class of anomalies is introduced. Then, the problem is formulated as a stability problem and robust control tools are used to derive a convergence condition for the time-delay observer. Basically, the observer, embedded in a router, uses the queue length measurement of the buffer to reconstruct the whole state composed of the flow rates. However, this latter being related to the linearized model of TCP, traffic has to be regulated around an equilibrium point to ensure the validity of the observer model and a congestion control mechanism (as AQM, Active Queue Management [25]) is

thus required. Next, the model is extended in order to take into account a class of anomalies and short bursty traffic. In that case, the associated observer is endowed with a "detector" of a class of anomalies. Note that the proposed methodology allows on-line and non-intrusive monitoring. It thus belongs to the active monitoring methods but does not require to inject any probes into the network. Even if our study focuses on specific and static networks as explained in the next section, it shows encouraging results.

The paper is organized as follows. The problem statement introducing the model of a network supporting TCP and the AQM congestion control is presented in the second section. Then, the third part is dedicated to the design of an observer for the estimation of data flow rates as well as anomaly detection. The fourth section shows an illustrative example of the proposed theory using NS-2 simulations and emulations. Finally, the fifth section concludes the paper and proposes future works.
means that $A-B$ is (semi-) positive definite. A^T denotes the transpose of A. $\mathsf{1_n}$ and $\mathsf{0_{m\times n}}$ denote respectively the identity matrix of size n and null matrix of size $m \times n$. If the context allows it, the dimensions of these matrices are often omitted. $B \in \mathsf{R^{m\times n}}$ such that $rank(B) = r$, we define $B^{\perp} \in \mathsf{R^{n\times(n-r)}}$ the right orthogonal complement of B by $BB^{\perp} = 0$.

2 NETWORK DYNAMICS

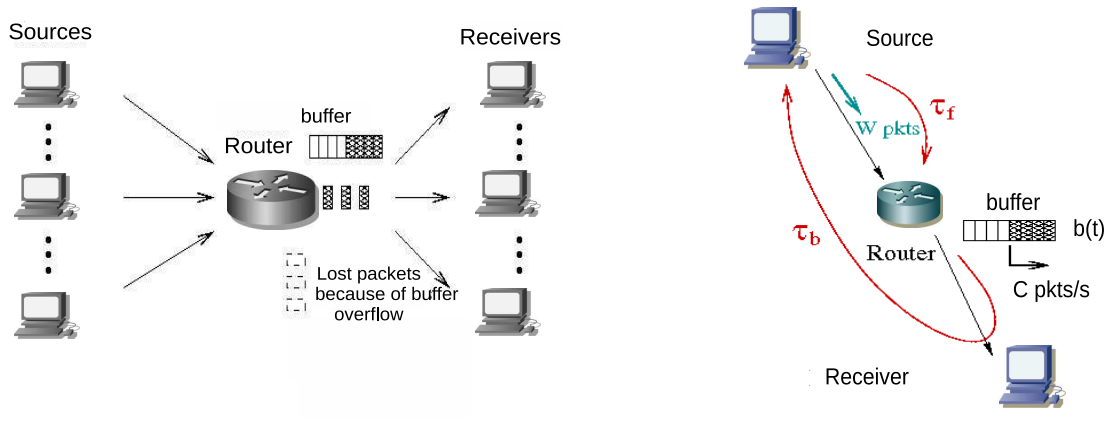
2.1 Fluid-flow model of TCP

This section is devoted to the introduction of the network model that describes the traffic behavior. In this paper, we consider networks consisting of a single router and N heterogeneous TCP sources. By heterogeneous, we mean that each source is linked to the router with different propagation time (see Figure 1a).

Since the bottleneck is shared by N flows, TCP applies the congestion avoidance algorithm to avoid the network saturation [14]. Following the AIMD mechanism, the congestion window of TCP sources varies according to the network load state (packet losses and delays). Hence, various deterministic fluid-flow models have been developed (see [18], [20] and [26] and references therein) to describe the behavior of the transmission protocol.

While many studies dealing with network control in the automatic control theory framework consider the model proposed by [20], we use a more accurate one, introduced in [18] and described by (1) which takes into account the forward and backward delays. The model and notations are as follow:

$$\begin{cases} \dot{W}_i(t) &= \frac{W_i(t-\tau_i)}{\tau_i(t-\tau_i)}(1-p_i(t-\tau_i^b))\frac{1}{W_i(t)} - \frac{W_i(t-\tau_i)}{\tau_i(t-\tau_i)}\frac{W_i}{2}p_i(t-\tau_i^b), \\ \dot{b}(t) &= -c + \sum_{i=1}^{N}\eta_i\frac{W_i(t-\tau_i^f)}{\tau_i(t-\tau_i^f)}, \\ \tau_i &= \frac{b(t)}{c} + T_{p_i} = \tau_i^f + \tau_i^b, \end{cases} \tag{1}$$



(a) (b)

Figure 1: (a) Network topology, (b) a single connection

where $W_i(t)$ is the congestion window size of the source i, $b(t)$ is the queue length of the buffer at the router, τ_i is the RTT perceived by the source i. This latter quantity can be decomposed as the sum of the forward and backward delays (τ_i^f and τ_i^b), standing for, respectively, the trip time from the source i to the router (the one way) and from the router to the source via the receiver (the return) (see Figure 1b). c, T_{p_i} and N are parameters related to the network configuration and represent, respectively, the link capacity, the propagation time of the path taken by the connection i and the number of TCP sources. η_i is the number of sessions established by source i. The first equation of (1) describes the AIMD behavior of the congestion window size of the transmission protocol applied by the source i. Roughly, the first part of the right-hand side represents the additive-increase, whereas the second follows the multiplicative decrease [18]. Expressed by the second equation of (1), the length of the FIFO queue integrates the difference between incoming traffic and the link capacity. The RTTs, in the third equation, include the queueing delay $b(t)/C$ and the propagation delay. The signal $p_i(t)$ corresponds to the dropping probability of a packet at the router buffer. Note that the network variables mentionned above in the model (1) are considered as mean values [18] (for instance, $W_i(t)$ represents the average congestion window size).

In this paper, the objective is to develop a method which computes, at the router, an estimation of the different flow rates passing through it. The congestion window W_i does not provide a relevant index of the traffic intensity since it only refers to the amount of data sent by the source at a given instant. Consequently, additional frequent measures of the corresponding RTT are required. Hence, we propose to reformulate the model (1) such that the state vector is expressed in terms of aggregate flows instead of congestion windows. To this end, rates of each flow x_i, expressed as $x_i(t) = \frac{W_i(t)}{\tau_i(t)}$, will be considered. The dynamic of this new quantity becomes of the form $\dot{x_i}(t) = \frac{d}{dt}\left(\frac{W_i(t)}{\tau_i(t)}\right) = \frac{\dot{W}_i(t) - x_i(t)\dot{\tau}_i(t)}{\tau_i(t)}$. Based on the expressions of $\dot{W}(t)$, $\dot{b}(t)$, $\tau_i(t)$ (see equation (1)) and $\dot{\tau}(t) = \frac{\dot{b}(t)}{c}$, a new model of the TCP behavior is derived:

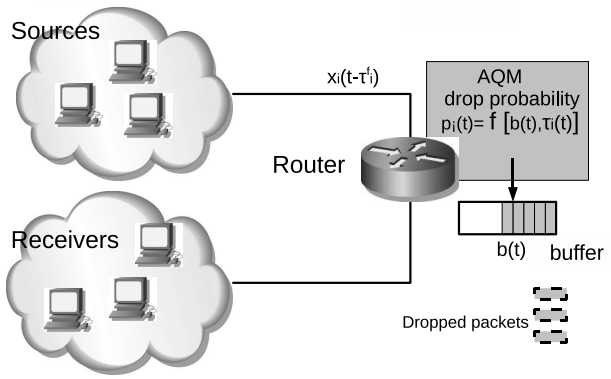


Figure 2: Implementation of an AQM

$$\begin{cases} \dot{x}_i(t) &= \frac{x_i(t-\tau)}{x_i(t)\tau(t)^2}(1-p(t-\tau^b)) - \frac{x_i(t-\tau)x_i(t)}{2}p(t-\tau^b) + \frac{x_i(t)}{\tau(t)} - \frac{x_i(t)}{\tau(t)c}\sum_i \eta_i x_i(t-\tau_i^f), \\ \dot{b}(t) &= -c + \sum_{i=1}^N \eta_i x_i(t-\tau_i^f). \end{cases} \tag{2}$$

2.2 AQM for congestion control

To achieve high efficiency and high reliability of communications in computer networks, many investigations have been done regarding the congestion control issue. Since the congestion window size of the transmission protocol depends on packet losses (specified by $p_i(t)$), a proposal was to use this feature in order to control the source sending rates. Hence, a mechanism, called AQM (*Active Queue Management*, see Figure 2), has been developed to provoke losses avoiding then severe congestion, buffer overflow, time-out... This strategy allows the regulation of TCP flows with an implicit control (or explicit if the ECN, *Explicit Congestion Notification*, protocol is enabled). Various AQM have been proposed in the literature such as Random Early Detection (RED) [9], Random Early Marking (REM) [3], Adaptive Virtual Queue (AVQ) [26] and many others [25]. Their performances have been evaluated in [25] and empirical studies have shown their effectiveness. Recently, significant studies initiated by [11] have redesigned AQMs using control theory and P, PI have been developed in order to cope with the packet dropping problem. Then, using dynamical model developed by [20], many researches have been devoted to deal with congestion problem in a control theory framework (for examples see [16], [15], [27] and references therein).

So, AQM supports TCP for congestion control and regulates the queue length of the buffer as well as flow rates around an equilibrium point [16], [15], [11]. An efficient control allows thus to approximate the TCP dynamics (2) as a linear model (4) around an equilibrium point (3). Our work focuses on traffic monitoring at a router with a static topology (N and η_i are constant). Moreover, for the mathematical tractability, we make the usual assumption [18], [11], [15] that all delays (τ_i, τ_i^f and τ_i^b) are time invariant

when they appear as arguments of variables (for example $x_i(t-\tau_i(t)) \equiv x_i(t-\tau_i)$). This latter assumption keeps its validity as long as the queue length remains close to its equilibrium value and when the queueing delay is smaller than propagation delays. Defining an equilibrium point

$$\begin{cases} \tau_{i_0} & = T_p + b_0/c, \\ \dot{b}(t) & = 0 \;\Rightarrow\; \sum_{i=1}^{N} \eta_i x_{i_0} = c, \\ \dot{x}_i(t) & = 0 \;\Rightarrow\; p_{i_0} = \frac{2}{2+(x_{i_0}\tau_{i_0})^2}. \end{cases} \tag{3}$$

model (2) can be linearized to obtain:

$$\begin{bmatrix} \dot{x}_1(t) \\ \vdots \\ \dot{x}_N(t) \\ \dot{b}(t) \end{bmatrix} = A \begin{bmatrix} \delta x_1(t) \\ \vdots \\ \delta x_N(t) \\ \delta b(t) \end{bmatrix} + A_d \begin{bmatrix} \delta x_1(t-\tau_1^f) \\ \vdots \\ \delta x_N(t-\tau_N^f) \\ \delta b(t) \end{bmatrix} + B \begin{bmatrix} \delta p_1(t-\tau_1^b) \\ \vdots \\ \delta p_N(t-\tau_N^b) \end{bmatrix}, \tag{4}$$

where $\delta x_i \doteq x_i - x_{i_0}$, $\delta b \doteq b - b_0$ and $\delta p_i \doteq p_i - p_{i_0}$ are the state variations around the equilibrium point (3). Matrices of the equation (4) are defined by

$$A = \begin{bmatrix} a_1 & 0 & 0 & h_1 \\ 0 & \ddots & 0 & \vdots \\ 0 & 0 & a_N & h_N \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} e_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & e_N \\ 0 & 0 & 0 \end{bmatrix}, \quad A_d = \begin{bmatrix} f_1\eta_1 & \dots & f_1\eta_N & 0 \\ \vdots & \vdots & \vdots & 0 \\ f_N\eta_1 & \dots & f_N\eta_N & 0 \\ \eta_1 & \dots & \eta_N & 0 \end{bmatrix},$$

with $a_i = -\frac{1-p_{i_0}}{x_{i_0}\tau_{i_0}^2} - \frac{x_{i_0}p_{i_0}}{2}$, $h_i = -\frac{2(1-p_{i_0})}{c\tau_{i_0}^3}$, $f_i = -\frac{x_{i_0}}{\tau_{i_0}c}$ and $e_i = -\frac{1}{\tau_{i_0}^2} - \frac{x_{i_0}^2}{2}$. Remark that a multiple time delay system (4) is obtained with a particular form since each component of the state vector is delayed by a different quantity related to the communication path.

3 OBSERVER FOR TRAFFIC MONITORING

3.1 Preliminaries

First, and before designing the oberver, it is necessary to introduce the following theorem [23] that provides stability condition for interconnected systems as illustrated in Figure 3. This result is then used to cope with the delayed part of (4) and to provide conditions for the convergence of the observer state to (4).

Theorem 1 *Given two possibly non-squared matrices $\mathcal{E}$, $\mathcal{A}$ and an uncertain matrix ∇ belonging to a set Ξ. The uncertain system represented by Figure 3 is stable for all matrices $\nabla \in \Xi$ if and only if there*

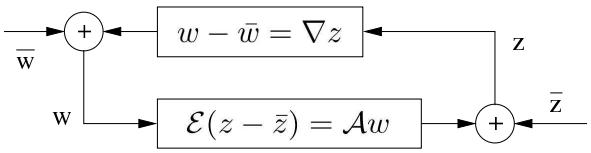


Figure 3: An interconnected system

exists a matrix $\Theta = \Theta^*$ *satisfying conditions*

$$\begin{bmatrix} \mathcal{E} & -\mathcal{A} \end{bmatrix}^{\perp *} \Theta \begin{bmatrix} \mathcal{E} & -\mathcal{A} \end{bmatrix}^{\perp} > 0 \tag{5}$$

$$\begin{bmatrix} 1 & \nabla^* \end{bmatrix} \Theta \begin{bmatrix} 1 \\ \nabla \end{bmatrix} \leq 0. \tag{6}$$

The considered feedback system having the same form of Figure 3 is a linear equation connected to a linear uncertainty ∇. This result comes from robust control theory using the quadratic separation tools [13]. The second inequality (6) is constructed based on some knowledge about the uncertain matrix ∇ (for instance upperbounds, convex hull). Then, the first one (5) is solved to assess the stability of the interconnection. Previous works [10] have shown that such a framework provides convenient tools and a good insight into time delay systems stability issue. In that case, the delay system is represented as in Figure 3 where ∇ consists of some appropriate operators related to the delay.

In the next part, Theorem 1 leads to conceive an observer that tracks the state of the multiple time delays system (4).

3.2 Design of the observer

Consider a network as illustrated in Figure 1a consisting of N TCP pairs, the traffic dynamic regulated by an AQM can be modeled around the equilibrium point as (see (4)):

$$\begin{cases} \dot{x}(t) &= Ax(t) + A_d x_d(t) + Bu(t) \\ y(t) &= Cx(t) \end{cases} \tag{7}$$

where

$$x(t) = \begin{bmatrix} \delta x_1(t) \\ \vdots \\ \delta x_N(t) \\ \delta b(t) \end{bmatrix}, \; x_d(t) = \begin{bmatrix} \delta x_1(t - \tau_1^f) \\ \vdots \\ \delta x_N(t - \tau_N^f) \\ \delta b(t) \end{bmatrix}, u(t) = \begin{bmatrix} \delta b(t - \tau_1^b) \\ \vdots \\ \delta b(t - \tau_N^b) \end{bmatrix}, \; C = \begin{bmatrix} 0 & \dots & 0 & 1 \end{bmatrix},$$

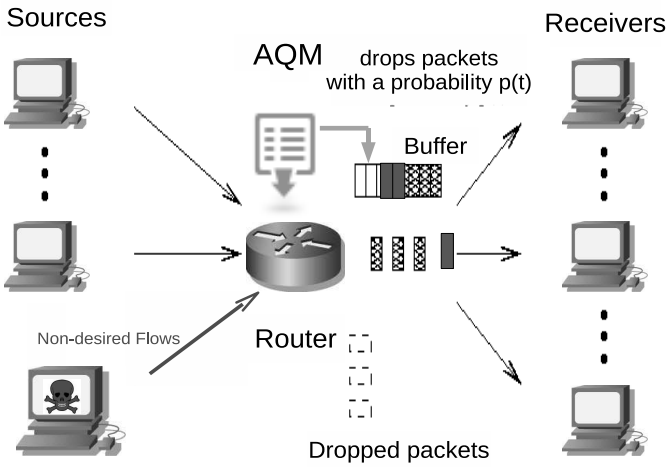


Figure 4: Introduction of an additional non-TCP traffic as anomaly

and $y(t)$ is the measured output *i.e.* the queue length at the router. In order to take into account extra traffic or non-modeled traffic (for example, traffics coming from applications over UDP protocol, see Figure 4), an additional signal $d(t)$ should be added to the queue dynamic (second equation in (2)):

$$\dot{b}(t) = -c + d(t) + \sum_i \eta_i x_i(t - \tau_i^f).$$

This signal represents flows that pass through the router and fill up the buffer $b(t)$ in addition to the expected traffic (N TCP connections). Notice that this feature can be used to model anomalies or DoS attacks (*Denial of Service*, [4]). In this paper, we consider some class of anomalies that are CBR (*Constant Bit Rate*) based applications which can be modeled as piecewise-constant functions. Such applications are met in streaming applications, video conferencing, telephony (voice services). Furthermore, the same modeling can also be used for some class of attacks [19] as traditional *flooding-based DoS* (for example *Shrew*) or *PDoS* (see [19] and references therein). Consequently, assuming that $d(t)$ is a piecewise-constant function, we propose to consider now the following augmented system which embeds the anomaly feature:

$$\left\{ \begin{array}{rcl} \dot{\tilde{x}}(t) & = & \bar{A}\tilde{x}(t) + \bar{A}_d\tilde{x}_d(t) + \bar{B}u(t) \\ \tilde{y}(t) & = & \bar{C}\tilde{x}(t) \end{array} \right. \tag{8}$$

where $\tilde{x}(t) = \left[\begin{array}{c} x(t) \\ \hline d(t) \end{array}\right]$, $\tilde{x}_d(t) = \left[\begin{array}{c} x_d(t) \\ \hline d(t) \end{array}\right]$, $\bar{C} = \left[\begin{array}{c|c} C & 0 \end{array}\right]$,

$$\bar{A} = \left[\begin{array}{ccc|c} & & & 0 \\ & A & & \vdots \\ & & & 0 \\ & & & 1 \\ \hline 0 & \dots & 0 & 0 \end{array}\right], \quad \bar{A}_d = \left[\begin{array}{ccc|c} & & & 0 \\ & A_d & & \vdots \\ & & & 0 \\ \hline 0 & \dots & 0 & 0 \end{array}\right], \quad \bar{B} = \left[\begin{array}{c} B \\ \hline 0_{1\times N} \end{array}\right].$$

Let construct an observer for the augmented system (8) defined by:

$$\dot{\hat{\tilde{x}}}(t) = \bar{A}\hat{x}(t) + \bar{A}_d\hat{x}_d(t) + \bar{B}u(t) + L\left(y - \bar{C}\hat{x}(t)\right) \tag{9}$$

where $\hat{x}(t)$ is the observer state and L is the observer gain. This latter matrix has to be designed such that $\hat{x}(t)$ converges to $\tilde{x}(t)$. Notice that the pair $(\bar{A}+\bar{A}_d, \bar{C})$ is observable which implies that there exists an observer (depending eventually on the delay) allowing the reconstruction of the states of system (8).

Theorem 2 *If there exists* $(N+2)\times(N+2)$ *positive definite matrices* P, Q_i *and* S_i *for* $i = \{1, ..., N\}$ *and a matrix* $X \in \mathsf{R}^{(N+2)\times 1}$ *such that the following inequality holds*

$$\left[\begin{array}{cccc} \Xi_1 + \Xi_3 & Y & \dots & Y \\ Y^T & \frac{1}{\tau_1^{f^2}} S_1 & & 0 \\ \vdots & & \ddots & \\ Y^T & 0 & & \frac{1}{\tau_N^{f^2}} S_N \end{array}\right] > 0 \tag{10}$$

with

$$\Xi_1 = \begin{bmatrix} \Psi & -P\bar{A}_{d_1} & \dots & -P\bar{A}_{d_N} \\ -\bar{A}_{d_1}^T P & Q_1 & & 0 \\ \vdots & & \ddots & \\ -\bar{A}_{d_N}^T P & 0 & & Q_N \end{bmatrix}, \tag{11}$$

$$\Xi_3 = \sum_{i=1}^{N} M_i (2P - S_i) M_i^T, \tag{12}$$

$$Y = \begin{bmatrix} (P\bar{A} - X\bar{C}) & P\bar{A}_{d_1} & \dots & P\bar{A}_{d_N} \end{bmatrix}^T \tag{13}$$

$$\Psi = -P\bar{A} - \bar{A}^T P + X\bar{C} + \bar{C}^T X^T - \sum_{i=1}^{N} Q_i, \tag{14}$$

$$M_i = \begin{bmatrix} -1_{\mathsf{N+2}} \\ 0_{(\mathsf{N+2})(\mathsf{i-1})\times(\mathsf{N+2})} \\ 1_{\mathsf{N+2}} \\ 0_{(\mathsf{N-i})(\mathsf{N+2})\times(\mathsf{N+2})} \end{bmatrix}, \tag{15}$$

then system (9) is an observer for system (8), i.e $\hat{x}(t)$ converges asymptotically to $\tilde{x}(t)$. The observer gain L is given by $L = P^{-1}X$.

Proof 1 *In order to prove the asymptotic convergence of $\hat{x}(t)$ to $\tilde{x}(t)$, let us define the error between the state of (8) and the one of the observer (9): $e(t) = \tilde{x}(t) - \hat{x}(t)$. We aim at ensuring that the error $e(t)$ converges toward zero. Hence, the first problem can be recast as the stability issue of the system*

$$\dot{e}(t) = \left(\bar{A} - L\bar{C}\right) e(t) + \bar{A}_d e_d(t). \tag{16}$$

where $e_d(t) = \tilde{x}_d(t) - \hat{x}_d(t)$. System (16) is then rewritten as

$$\dot{e}(t) = \mathbb{A}e(t) + \sum_{i=1}^{N} \bar{A}_{d_i} e(t - \tau_i^f) \tag{17}$$

with $\mathbb{A} = \left(\bar{A} - L\bar{C}\right)$,

$$\bar{A}_{d_i} = \eta_i \left[\begin{array}{c|c|c} & f_1 & \\ & \vdots & \\ 0_{(\mathsf{N+2})\times(\mathsf{i-1})} & f_N & 0_{(\mathsf{N+2})\times(\mathsf{N-i+2})} \\ & 1 & \\ & 0 & \end{array}\right].$$

Next, transforming the system (17) into an interconnected system of the form of Figure 3, Theorem 1

may be applied to derive the stability condition. System (17) is thus expressed as the interconnection of

$$w(t) = \underbrace{\begin{bmatrix} s^{-1}1_{N+2} & 0 & 0 \\ 0 & \mathcal{D} \otimes 1_{N+2} & 0 \\ 0 & 0 & (1-\mathcal{D})s^{-1} \otimes 1_{N+2} \end{bmatrix}}_{\nabla} z(t) \tag{18}$$

and equation (19)

$$\underbrace{\left[\begin{array}{c|c} 1_{(N+2)(N+1)} & 0_{(N+2)(N+1)\times(N+2)N} \\ \hline \begin{matrix} -1_{(N+2)} \\ \vdots \\ -1_{(N+2)} \end{matrix} & \begin{matrix} 0_{(N+2)N} & 1_{(N+2)N} \end{matrix} \\ \hline 0_{(N+2)N\times(N+2)(2N+1)} \end{array}\right]}_{\mathcal{E}} \underbrace{\begin{bmatrix} \dot{e}(t) \\ e(t) \\ \vdots \\ e(t) \\ \dot{e}(t) \\ \vdots \\ \dot{e}(t) \end{bmatrix}}_{z(t)} = \underbrace{\left[\begin{array}{c|c} \mathbb{A} \quad \bar{A}_{d_1} \quad \dots \quad \bar{A}_{d_N} \quad 0 & \\ \hline \begin{matrix} 1_{(N+2)} \\ \vdots \\ 1_{(N+2)} \end{matrix} & 0_{N(N+2)\times 2N(N+2)} \\ \hline 0_{(N+2)N\times(N+2)(2N+1)} & \\ \hline \begin{matrix} 1_{(N+2)} \\ \vdots \\ 1_{(N+2)} \end{matrix} & \begin{matrix} -1_{(N+2)N} & -1_{(N+2)N} \end{matrix} \end{array}\right]}_{\mathcal{A}} \underbrace{\begin{bmatrix} e(t) \\ e(t-\tau_1^f) \\ \vdots \\ e(t-\tau_N^f) \\ e(t)-e(t-\tau_1^f) \\ \vdots \\ e(t)-e(t-\tau_N^f) \end{bmatrix}}_{w(t)} \tag{19}$$

where $\mathcal{D} = diag\left(e^{-\tau_1^f s}, ..., e^{-\tau_N^f s}\right)$.

First, it can be proved that the separator (20) satisfies the inequality (6) according to the matrix ∇ *defined as (18) (the proof is omitted because of the space limitation, it is an extension of [10] to the case of multiple delays).*

$$\Theta = \left[\begin{array}{c|c} \Theta_{11} & \Theta_{12} \\ \hline * & \Theta_{22} \end{array}\right] \tag{20}$$

with

$$\Theta_{11} = diag\left(0_{N+2}, -Q_1, \dots, -Q_N, -R_1\tau_1^{f^2}, \dots, -R_N\tau_N^{f^2}\right)$$

$$\Theta_{12} = diag\left(-P, 0_{2N(N+2)}\right)$$

$$\Theta_{22} = diag\left(0_{N+2}, Q_1, \dots, Q_N, R_1, \dots, R_N\right)$$

P, Q_i and R_i $\forall i \in [1, N]$ are positive definite matrices. So, system (16) is stable if the inequality (5) with $\mathcal{E}$ and $\mathcal{A}$ defined as (19) is verified. Some algebraic calculations show that this latter is of the form

$$\bar{\Xi}_1 - \Xi_2 + \bar{\Xi}_3 > 0 \tag{21}$$

with $\bar{\Xi}_3 = \sum_{i=1}^{N} M_i R_i M_i^T$,

$$\bar{\Xi}_1 = \begin{bmatrix} -P\mathbb{A} - \mathbb{A}^T P - \sum_i Q_i & -P\bar{A}_{d_1} & \dots & -P\bar{A}_{d_N} \\ -\bar{A}_{d_1}^T P & Q_1 & & 0 \\ \vdots & & \ddots & \\ -\bar{A}_{d_N}^T P & 0 & & Q_N \end{bmatrix}, \quad \Xi_2 = \begin{bmatrix} \mathbb{A}^T \\ \bar{A}_{d_1}^T \\ \vdots \\ \bar{A}_{d_N}^T \end{bmatrix} \sum_{i=1}^{N} \tau_i^{f^2} R_i \begin{bmatrix} \mathbb{A}^T \\ \bar{A}_{d_1}^T \\ \vdots \\ \bar{A}_{d_N}^T \end{bmatrix}^T.$$

and M_i *is defined in (15).* Ξ_2 *and* $\bar{\Xi}_3$ *are then equivalently rewritten respectively as*

$$\begin{bmatrix} \mathbb{A}^T P \\ \bar{A}_{d_1}^T P \\ \vdots \\ \bar{A}_{d_N}^T P \end{bmatrix} \sum_i \tau_i^{f^2} P^{-1} R_i P^{-1} \begin{bmatrix} \mathbb{A}^T P \\ \bar{A}_{d_1}^T P \\ \vdots \\ \bar{A}_{d_N}^T P \end{bmatrix}^T \quad \textit{and} \quad \sum_i \begin{bmatrix} -P \\ 0_{(N+2)(i-1)\times(N+2)} \\ P \\ 0_{(N-i)(N+2)\times(N+2)} \end{bmatrix} P^{-1} R_i P^{-1} \begin{bmatrix} \\ * \\ \\ \end{bmatrix}^T.$$

Defining $S_i = PR_i^{-1}P$ *and since* $(P - S_i)^T S_i^{-1} (P - S_i) \geq 0$, $PS_i^{-1}P \geq 2P - S_i$ *is verified, and the inequality* $\bar{\Xi}_1 - \Xi_2 + \Xi_3 > 0$ *with* Ξ_3 *defined in (12), implies (21). Applying a schur complement to this latter inequality and defining* $X = PL$, *condition (10) is recovered.*

4 SIMULATION AND EMULATION

4.1 NS-2 simulation

This section is dedicated to elucidate the proposed methodology through an illustrative example. As shown in Figure 5, a network consisting of three communicating pairs through a congested router, *i.e.* a bottleneck, is considered. Propagation times are as illustrated and the link bandwidth is fixed to $10Mbps$, that is 2500 packet/s considering packet size of 500 bytes. Each of the three sources uses TCP/Reno and establishes 20 connections generating long lived TCP flows (like FTP connections). Simulations have been performed with the network simulator NS-2 [7] (release 2.30) to validate the exposed theory.

The three TCP sources share the single link and a congestion phenomenon occurs at the first router. So, to control the queue length of the buffer (avoiding then overflows), an AQM is embedded in the router. If an efficient regulation is maintained, the proposed linear observer (9) can be added in the router for flow monitoring. In our example, the observer have been tested over AQM gain-K [16]. This latter is adjusted such that it regulates the queue length of the router to a desired level $b_0 = 100$ packets while the maximal buffer size is set to 400 packets.

Given the topology in Figure 5, the previous specifications and the equilibrium point (3), the observer is then written as

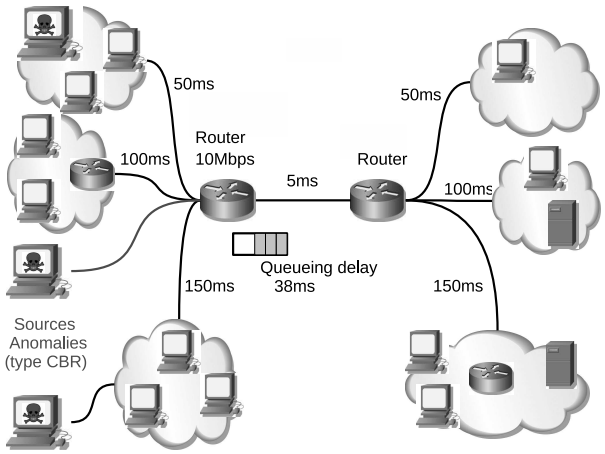


Figure 5: Example of a bottleneck link

$$\begin{bmatrix} \delta\dot{\hat{x}}_1(t) \\ \delta\dot{\hat{x}}_2(t) \\ \delta\dot{\hat{x}}_3(t) \\ \dot{\hat{b}}(t) \\ \dot{\hat{d}}(t) \end{bmatrix} = \begin{bmatrix} -0.73 & 0 & 0 & -0.049 & 0 \\ 0 & -0.22 & 0 & -0.008 & 0 \\ 0 & 0 & -0.10 & -0.002 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \delta\hat{x}_1(t) \\ \delta\hat{x}_2(t) \\ \delta\hat{x}_3(t) \\ \delta\hat{b}(t) \\ \hat{d}(t) \end{bmatrix} + \begin{bmatrix} -1.34 & -1.34 & -1.34 & 0 & 0 \\ -0.74 & -0.74 & -0.74 & 0 & 0 \\ -0.51 & -0.51 & -0.51 & 0 & 0 \\ 20 & 20 & 20 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \delta\hat{x}_1(t-0.025) \\ \delta\hat{x}_2(t-0.05) \\ \delta\hat{x}_3(t-0.075) \\ \delta\hat{b}(t) \\ \hat{d}(t) \end{bmatrix}$$
$$+ \begin{bmatrix} -970 & 0 & 0 \\ 0 & -959 & 0 \\ 0 & 0 & -956 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \delta p_1(t-0.198) \\ \delta p_2(t-0.348) \\ \delta p_3(t-0.498) \end{bmatrix} + L \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \end{bmatrix} (\tilde{x}(t) - \hat{x}(t)) \tag{22}$$

where the observer gain L ensures the convergence of $\hat{x}(t)$ to the real state $\tilde{x}$. Applying Theorem 2, the matrix gain can be found as $L = [0.28\ 0.46\ 0.45\ 1.76\ 0.54]^T$. Prior theoritical simulations with the nonlinear model (2) under Matlab/Simulink show that the mechanism works well (see Figure 6). It can be observed that the observer recovers the network variables in spite of a disturbance generated in between $100s$ and $200s$. Then, we have performed a simulation of $400s$ on NS-2 where the 20 ftp connections of each three TCP sources send data to their respective receivers. An additional non-responsive traffic generated by 3 UDP (user datagram protocol) flows (at $1Mbps$ each one) is injected into the bottleneck as illustrated in Figure 5. This latter simulates a CBR anomaly and is introduced at the intervals: $150-170$s, $250-270$s and $300-320$s.

Estimation of the state and instantaneous measures are compared (the queue length and sending rates) as well as the anomaly detection "sensor" is illustrated in Figure 7. Results show that while reconstructing the state of model (4), the time-delay observer (9) is able to provide an estimation of the TCP flow rates based only on the queue length measurement. Furthermore, the augmented model (8) allows the observer to detect non-modeled piecewise constant traffic. Hence, as it can be seen in Figure

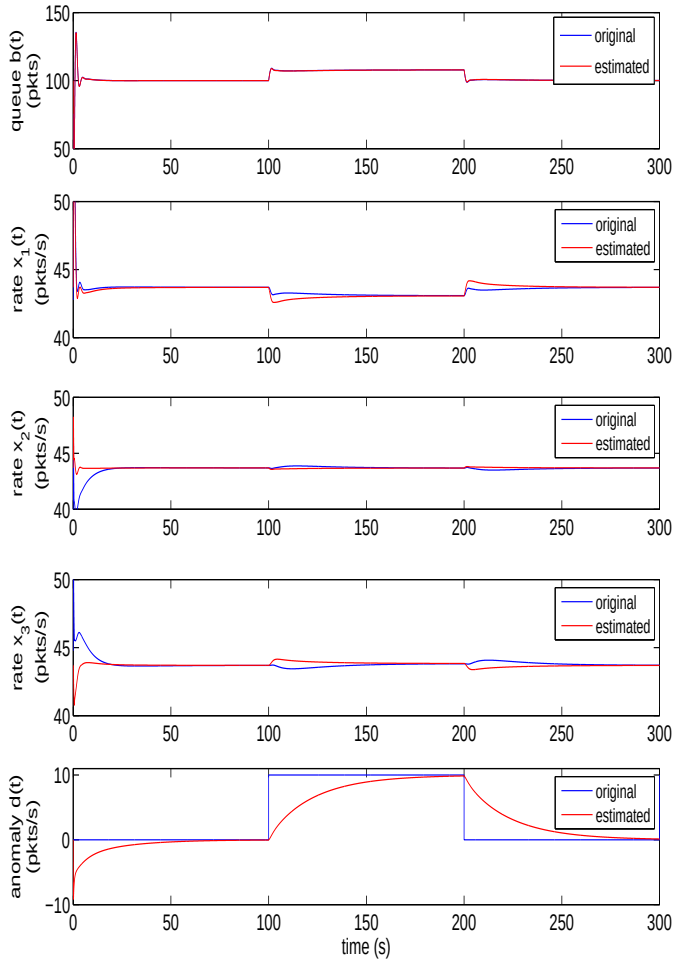


Figure 6: Observer over gain-K: original/estimated states and anomaly detection (nonlinear simulation on Matlab)

7, although the anomaly does not affect the queue (this attack is invisible from the buffer measurement), the mechanism can clearly detect the three UDP anomalies.

Remark 1 *In Figure 7, the estimated state follows the linearized model (2) which considers the network mean variables whereas the original state measured in NS gives instantaneous values. That is why such large oscillations around estimated signals are obtained in the measurements.*

Table 4.1 shows that the observer state matches average flow rates.

4.2 Emulation

Going further than simulations, another example is now proposed considering an emulation experiment. Emulation refers to experiments that introduce the simulator into a live network. Indeed, the NS environment provides special objects that allow the simulator to interact (catch and inject) with real traffics

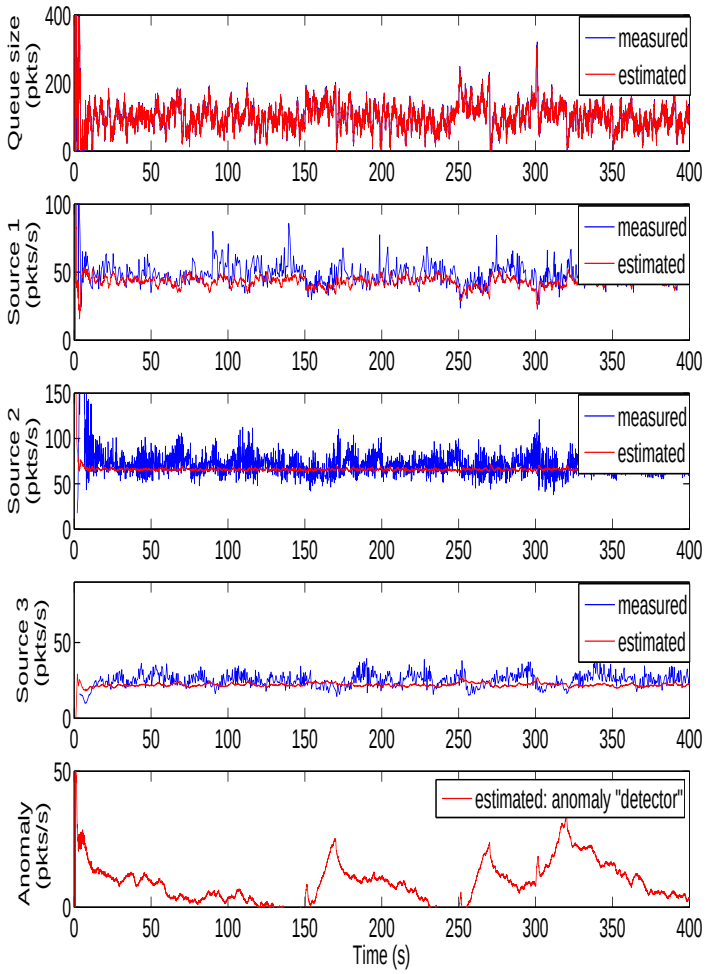


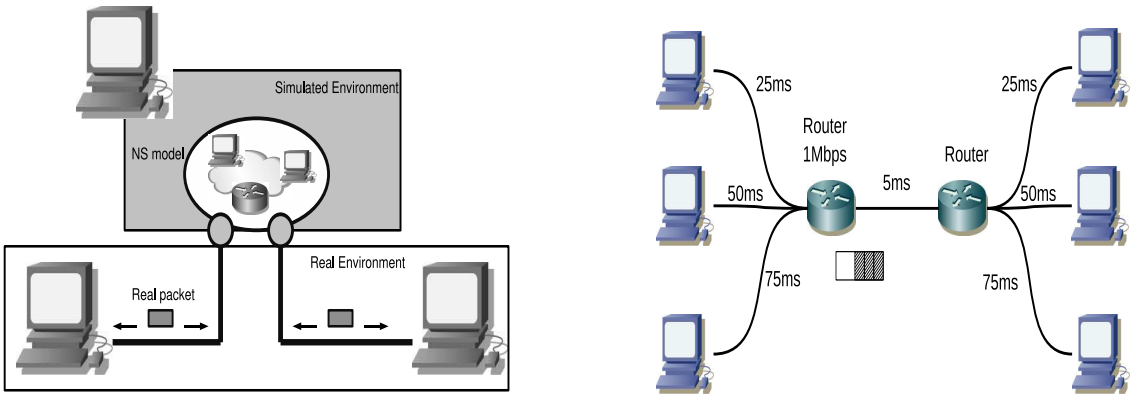
Figure 7: Observer over gain-K: original/estimated states and anomaly detection (simulation on NS)

Table 1: Average of measure/estimated of flow rates

	Simulation		Emulation	
	measured	estimated	measured	estimated
$x_1(t)$ (pkt/s)	51	43	92	99
$x_2(t)$ (pkt/s)	49	43	93	100
$x_3(t)$ (pkt/s)	53	45	113	110

using a real-time scheduler (see [6] and Figure 8a).

Regarding our study, the NS environment will be embedded in the computer that plays the role of the routers and other computers will generate and receive the traffic. Hence, the bottleneck and the observer are emulated while a real TCP traffic is handled and monitored.



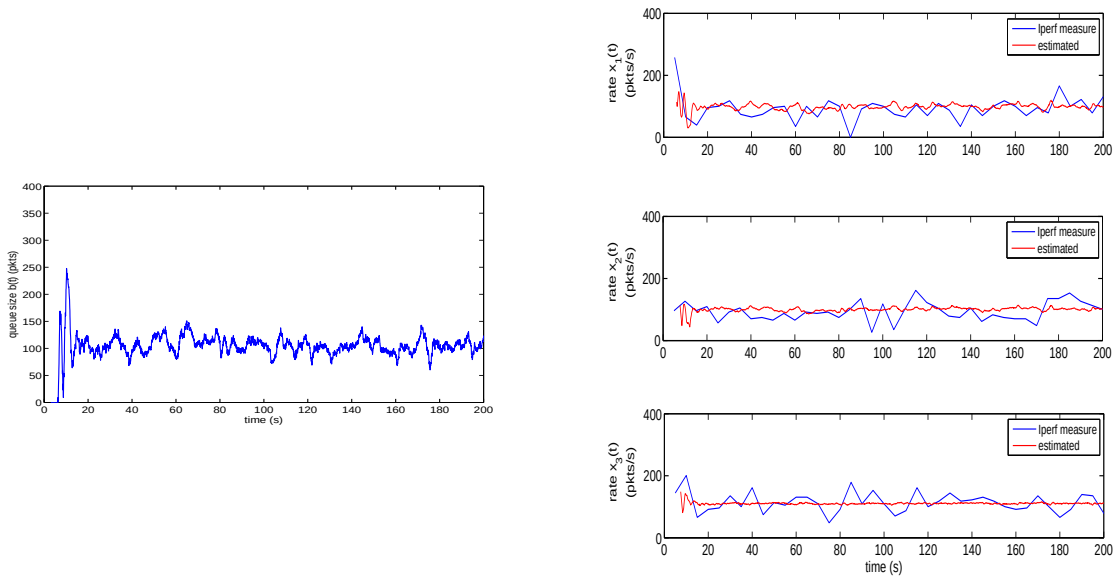
(a) (b)

Figure 8: (a) Emulation with real-time NS, (b) Second example of a bottleneck link

However, since the emulator requires a high computational cost, numerical values of the example must be scaled down (reducing the bandwidth). The considered example is illustrated in Figure 8b. Source traffics are generated with the network tool Iperf [21]. Applying a congestion control mechanism, the queue size of the buffer is regulated (see Figure 9a) and a linear observer can thus be developed according to the appropriate equilibrium point. Results of the emulation are shown in Figure 9b.

As it has been noticed in Remark 1, the state of the observer corresponds to average rates (see Table 4.1). Because of the network load (3 heavy data streams by source which cause congestion phenomenon), Iperf gives measures of the rate at a sampling period of $5s$. That is why, in Figure 9b, measures appear dispersed around the estimation.

A network emulator may be considered as an hybrid between a network simulator and a protocol implementation. Future works concern the real implementation of the AQM/observer into the Linux kernel to enable whole real experiments and real traffic monitoring in high speed networks.



(a) (b)

Figure 9: (a) AQM gain-K [1]: regulation of the queue length, (b) Observer over gain-K: original/estimated of rates

5 CONCLUSIONS AND FUTURE WORKS

In this paper, robust control theory tools have been used to design an observer for traffic monitoring purpose. This latter is embedded in a router and provides TCP flows estimations which pass through it. However, since the proposed observer is linear, an AQM that regulates the traffic around an equilibrium point is required. Besides, an augmented model is developed and the associated observer allows the detection of a class of anomalies in order to prevent potential malicious traffic as DoS attacks.

Future works concerns modeling studies of other existing DoS or DDoS attacks to endow the observer (by model augmentation) of a larger versatile anomaly detection system. Another point is the development of a non linear observer able to reconstruct the state, thus the traffic, without the AQM requirement.

References

[1] Y. Ariba, F. Gouaisbaut, and Y. Labit. Multiple time-delays system modeling and control for router management. In *European Control Conference*, Budapest, Hungary, August 2009.

[2] Y. Ariba, Y. Labit, and F. Gouaisbaut. Network anomaly estimation for tcp/aqm networks using an observer. pages 45–50, Annapolis, USA, June 2008.

[3] S. Athuraliya, D. Lapsley, and S. Low. An enhanced random early marking algorithm for internet flow control. In *IEEE INFOCOM*, pages 1425–1434, December 2000.

[4] Software Engineering Institute CERT. Denial of service attacks. http://www.cert.org/tech_tips/denial_of_service.html.

[5] J. Cleary, S. Donnely, I. Graham, A. McGregor, and M. Pearson. Design principles for accurate passive measurement. In *PAM (Passive and Active Measurements) Workshop, Hamilton, New Zealand*, pages 1–7, 2000.

[6] K. Fall. Network emulation in the vint/ns simulator. In *ISCC '99: Proceedings of the The Fourth IEEE Symposium on Computers and Communications*, July 1999.

[7] K. Fall and K. Varadhan. The ns manual. notes and documentation on the software ns2-simulator, 2002. URL: www.isi.edu/nsnam/ns/.

[8] M. Fliess, C. Join, and H. Mounier. *An introduction to nonlinear fault diagnosis with an application to a congested internet router*, chapter 16, pages 327–343. Advances in communication control networks. Springer, 2005. edited by S. Tarbouriech, C. T. Abdallah and J. Chiasson.

[9] S. Floyd and V. Jacobson. Random early detection gateways for congestion avoidance. *IEEE/ACM Transactions on Networking*, 1:397–413, August 1993.

[10] F. Gouaisbaut and D. Peaucelle. A note on stability of time delay systems. In 5^{th} *IFAC Symposium on Robust Control Design (ROCOND'06)*, Toulouse, France, July 2006.

[11] C. V. Hollot, V. Misra, D Towsley, and W. Gong. Analysis and design of controllers for aqm routers supporting tcp flows. *IEEE Trans. on Automat. Control*, 47:945–959, June 2002.

[12] A. Hussain, J. Heidemann, and C. Papadopoulos. A framework for classifying denial of service attacks, in karlsruhe, germany, august 2003. In *SIGCOMM*, Aug 2003.

[13] T. Iwasaki and S. Hara. Well-posedness of feedback systems: insights into exact robustnessanalysis and approximate computations. *IEEE Trans. on Automat. Control*, 43:619–630, May 1998.

[14] V. Jacobson. Congestion avoidance and control. In *ACM SIGCOMM*, pages 314–329, Stanford, CA, August 1988.

[15] K. B. Kim. Design of feedback controls supporting tcp based on the state space approach. In *IEEE Trans. on Automat. Control*, volume 51 (7), July 2006.

[16] Y. Labit, Y Ariba, and F. Gouaisbaut. On designing lyapunov-krasovskii based controllers for aqm routers supporting tcp flows. In *46th IEEE Conference on Decision and Control*, pages 3818–3823, New Orleans, USA, December 2007.

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

[18] H. S. Low, F. Paganini, and J.C. Doyle. *Internet Congestion Control*, volume 22, pages 28–43. IEEE Control Systems Magazine, Feb 2002.

[19] X. Luo, R. Chang, and E. Chan. Performance analysis of tcp/aqm under denial-of-service attacks. In *The 13th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems*, pages 97–104, 2005.

[20] V. Misra, W. Gong, and D Towsley. Fluid-based analysis of a network of aqm routers supporting tcp flows with an application to red. In *ACM SIGCOMM*, pages 151–160, August 2000.

[21] NLANR/DAST. Iperf. URL: http://iperf.sourceforge.net/.

[22] 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, Oct 1996.

[23] D. Peaucelle, D. Arzelier, D. Henrion, and F. Gouaisbaut. Quadratic separation for feedback connection of an uncertain matrix and an implicit linear transformation. *Automatica*, 43(5):795–804, 2007.

[24] R.S. Prasad, M. Murray, C. Dovrolis, and K. Claffy. Bandwidth estimation:metrics, measurement techniques, and tools. In *IEEE Network Magazine*, 2003.

[25] S. Ryu, C. Rump, and C. Qiao. Advances in active queue management (aqm) based tcp congestion control. *Telecommunication Systems*, 4:317–351, 2004.

[26] R. Srikant. *The Mathematics of Internet Congestion Control*. Birkhauser, 2004.

[27] S. Tarbouriech, C. T. Abdallah, and J. Chiasson. *Advances in communication Control Networks*. Springer, 2005.