Robust control tools for traffic monitoring in TCP networks

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

***Abstract*— Several studies have considered control theory tools for traffic control in communication networks, as for example the congestion control issue in IP (Internet Protocol) routers. In this paper, we propose to design a linear observer for time-delay systems to address the traffic monitoring issue in TCP/AQM (Transmission Control Protocol/Active Queue Management) networks. Due to several propagation delays and the queueing delay, the set TCP/AQM is modeled as a multiple delayed system of a particular form. Hence, appropriate robust control tools as quadratic separation are adopted to construct a delay dependent observer for TCP flows estimation. Note that, the developed mechanism enables also the anomaly detection issue for a class of DoS (Denial of Service) attacks. At last, simulations via the network simulator NS-2 and an emulation experiment validate the proposed methodology.**

I. Motivations and Contributions

Internet is becoming the major communication network. It allows an increasing number of activities, ranging from web browsing, file exchanges to on-line games or IP telephony. Because of its increasing popularity, traffic monitoring tools have to be embedded into the network to supervise communications to ensure QoS (Quality of Service) or even to avoid security breaches. Two techniques can be used:

Active monitoring [1] consists of generating probes into the network, and then to observe 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 such traffic (it inevitably affects the current traffic). Intrusiveness of probe traffic is thus one of the key features which active monitoring tools have to care about.

Secondly, passive monitoring [2] refers to network measurements with appropriate devices located at some relevant point in the network. Passive monitoring is performed on the capture of traffic and off-line estimate networks features. It provides a non intrusive method but not enough reactive.

In this paper, we propose to address the traffic monitoring issue in networks with the design of an observer. First, a dynamical model which describes the TCP flow rates behavior as well as a class of anomalies is introduced. Then, robust control tools, especially quadratic separation, are used to derive a convergence condition for the time delay observer. Basically, the observer, embedded at a router, uses the queue length measurement of the buffer to reconstruct the whole state composed of 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) is thus required. Next, the model is extended in order to detect a class of anomalies from the second category (attacks). Note that the proposed methodology allows on-line and non-intrusive monitoring (as active monitoring but without injecting 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.

II. Network Dynamics

A. 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 times (see Figure 1).

Since the bottleneck is shared by N flows, TCP applies the congestion avoidance algorithm to avoid the network saturation [3]. Following the AIMD (*Additive-Increase Multiplicative-Decrease*) 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 [4], [5] and [6] 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 [5], we use a more accurate one, introduced in [4] and described by (1) which takes into account the forward and backward delays. The model and

[1] CNRS; LAAS; 7, avenue du Colonel Roche, F-31077 Toulouse, France.
[2] Université de Toulouse; UPS, INSA, INP, ISAE; LAAS; F-31062 Toulouse, France. yariba@laas.fr

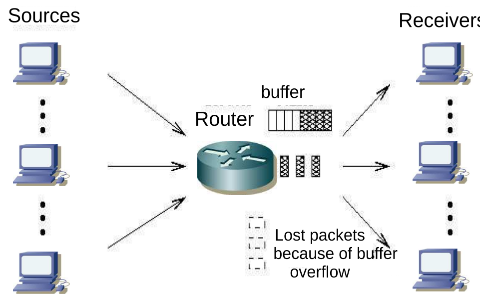

Fig. 1. Network topology

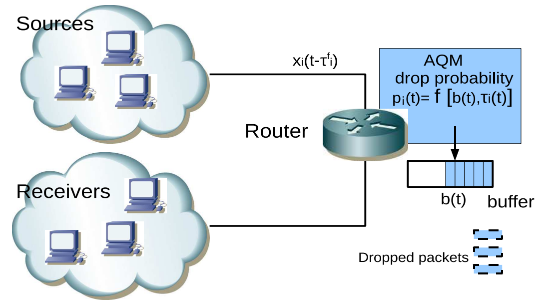

Fig. 2. Implementation of an AQM

notations are as follow:

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

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). 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 signal $p_i(t)$ corresponds to the dropping probability of a packet at the router buffer. Note that the network variables mentionned above in model (1) are considered as mean values [4] (for instance, $W_i(t)$ represents actually the average congestion window size).

In this paper, the objective is to develop a method which computes, at the router and during congestion, 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

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

B. 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, timeout. This strategy allows the regulation of TCP flows with an implicit control (or explicit if the ECN, *Explicit Congestion Notification*, protocol is enabled). And the AQM plays the role of a controller that feedbacks to sources the congestion information. The reader may refer, for example, to the survey [7] to have more details on such mechanisms.

So, AQM supports TCP for congestion control and regulates the queue length of the buffer as well as flow rates around an equilibrium point [8], [9], [10]. 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 [4], [10], [9] 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 is valid 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

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

model (2) can be linearized to obtain:

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

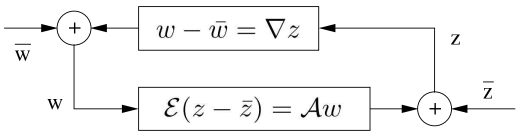

Fig. 3. An interconnected system

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

$$A = \begin{bmatrix} a_1 & 0 & 0 & h_1 \\ 0 & \ddots & 0 & \vdots \\ 0 & 0 & a_N & h_N \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} e_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & e_N \\ 0 & 0 & 0 \end{bmatrix}$$

$$A_d = \begin{bmatrix} f_1\eta_1 & \dots & f_1\eta_N & 0 \\ \vdots & \vdots & \vdots & 0 \\ f_N\eta_1 & \dots & f_N\eta_N & 0 \\ \eta_1 & \dots & \eta_N & 0 \end{bmatrix},$$

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 delays 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.

III. OBSERVER FOR TRAFFIC MONITORING

A. Preliminaries

First, and before designing the oberver, it is necessary to introduce the following theorem [11] 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 exists a matrix $\Theta = \Theta^*$ satisfying conditions*

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

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

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 [12]. 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.

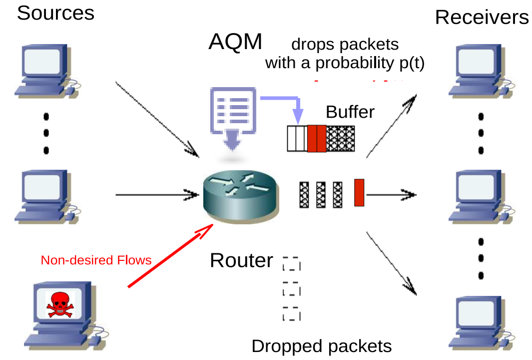

Fig. 4. Introduction of an additional non-TCP traffic as anomaly

B. Design of the observer

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

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

where

$$x(t) = \begin{bmatrix} \delta x_1(t) \\ \vdots \\ \delta x_N(t) \\ \delta b(t) \end{bmatrix}, \quad x_d(t) = \begin{bmatrix} \delta x_1(t-\tau_1^f) \\ \vdots \\ \delta x_N(t-\tau_N^f) \\ \delta b(t) \end{bmatrix},$$

$$u(t) = \begin{bmatrix} \delta b(t-\tau_1^b) \\ \vdots \\ \delta b(t-\tau_N^b) \end{bmatrix}, \quad C = \begin{bmatrix} 0 & \dots & 0 & 1 \end{bmatrix}.$$

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*, [13]). 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 [14] as traditional *flooding-based DoS* (for example $Shrew$) or *PDoS* (see [14] 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:

$$\begin{cases} \dot{\tilde{x}}(t) = \bar{A}\tilde{x}(t) + \bar{A}_d\tilde{x}_d(t) + \bar{B}u(t) \\ \tilde{y}(t) = \bar{C}\tilde{x}(t) \end{cases} \quad (8)$$

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

$$\bar{A} = \left[\begin{array}{c|c} A & \begin{matrix} 0 \\ \vdots \\ 0 \\ 1 \end{matrix} \\ \hline 0 \ \dots \ 0 & 0 \end{array}\right], \ \tilde{x}_d(t) = \left[\frac{x_d(t)}{d(t)}\right],$$

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

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

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

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 $X \in \mathrm{R}^{(N+2)\times 1}$ such that the following inequality holds*

$$\begin{bmatrix} \Xi_1 + \Xi_3 & Y & \dots & Y \\ Y^T & \frac{1}{\tau_1^{f2}} S_1 & & 0 \\ \vdots & & \ddots & \\ Y^T & 0 & & \frac{1}{\tau_N^{f2}} S_N \end{bmatrix} > 0 \quad (10)$$

with

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

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

$$Y = \left[\begin{array}{cccc} (P\bar{A} - X\bar{C}) & P\bar{A}_{d_1} & \dots & P\bar{A}_{d_N} \end{array}\right]^T \quad (13)$$

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

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

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: Due to the space limitation, we just give a sketch of the proof but a detailed version can be found in [15]. 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 to make sure that the error $e(t)$ converges toward zero. Hence, the first problem can be recast as the stability issue of system

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

where $e_d(t) = \tilde{x}_d(t) - \hat{x}_d(t)$. System (16) is then rewritten as $\dot{e}(t) = \mathbb{A}e(t) + \sum_{i=1}^{N} \bar{A}_{d_i} e(t - \tau_i^f)$ with $\mathbb{A} = \left(\bar{A} - L\bar{C}\right)$,

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

Next, transforming the previous system as an interconnected system of the form of Figure 3, Theorem 1 may be applied to derive the stability condition. System (16) is thus expressed as the interconnection of

$$w(t) = \underbrace{\begin{bmatrix} s^{-1}1_{N+2} & 0 & 0 \\ 0 & \mathcal{D}\otimes 1_{N+2} & 0 \\ 0 & 0 & (1-\mathcal{D})s^{-1}\otimes 1_{N+2} \end{bmatrix}}_{\nabla} z(t) \quad (17)$$

and equation (18) where $\mathcal{D} = diag\left(e^{-\tau_1^f s}, ..., e^{-\tau_N^f s}\right)$. Then, it remains to find an appropriate separator Θ and to apply Theorem 1 (see [15]). ■

IV. SIMULATION AND EMULATION

A. 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 [16] (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 [8]. 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 gain is L computed applying Theorem 2: $L = [0.28\ 0.46\ 0.45\ 1.76\ 0.54]^T$. Prior theoritical simulations

$$\underbrace{\left[\begin{array}{c|c} \multicolumn{2}{c}{1_{(N+2)(N+1)} \quad 0_{(N+2)(N+1)\times(N+2)N}} \\ \hline -1_{(N+2)} & \\ \vdots & 0_{(N+2)N} \quad 1_{(N+2)N} \\ -1_{(N+2)} & \\ \hline \multicolumn{2}{c}{0_{(N+2)N\times(N+2)(2N+1)}} \end{array}\right]}_{\mathcal{E}} \underbrace{\left[\begin{array}{c} \dot{e}(t) \\ e(t) \\ \vdots \\ e(t) \\ \dot{e}(t) \\ \vdots \\ \dot{e}(t) \end{array}\right]}_{z(t)} = \underbrace{\left[\begin{array}{c|c} \multicolumn{2}{c}{\mathbb{A} \quad \bar{A}_{d_1} \quad \dots \quad \bar{A}_{d_N} \quad 0} \\ \hline 1_{(N+2)} & \\ \vdots & 0_{N(N+2)\times 2N(N+2)} \\ 1_{(N+2)} & \\ \hline \multicolumn{2}{c}{0_{(N+2)N\times(N+2)(2N+1)}} \\ \hline 1_{(N+2)} & \\ \vdots & -1_{(N+2)N} \quad -1_{(N+2)N} \\ 1_{(N+2)} & \end{array}\right]}_{\mathcal{A}} \underbrace{\left[\begin{array}{c} e(t) \\ e(t-\tau_1^f) \\ \vdots \\ e(t-\tau_N^f) \\ e(t)-e(t-\tau_1^f) \\ \vdots \\ e(t)-e(t-\tau_N^f) \end{array}\right]}_{w(t)} \tag{18}$$

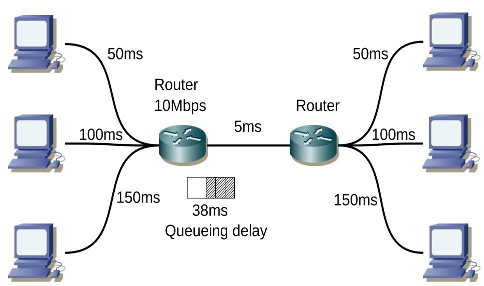

Fig. 5. Example of a bottleneck link

with the non linear model (2) under Matlab/Simulink show that the mechanism works well. 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) traffic (at $1Mbps$ each one) is injected into the bottleneck as illustrated in Figure 4. This latter simulates a CBR anomaly and is introduced at 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 6. Results show that reconstructing the state of model (4), the time-delay observer (9) is able to provide an estimation of TCP flow rates only based on the queue length measurement. Furthermore, the augmented model (8) allows the observer to detect also non-modeled piecewise constant traffic. Hence, as it can be seen in Figure 6, 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 *Regarding to NS-2 simulations, Figure 6, 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 for the measurements.*

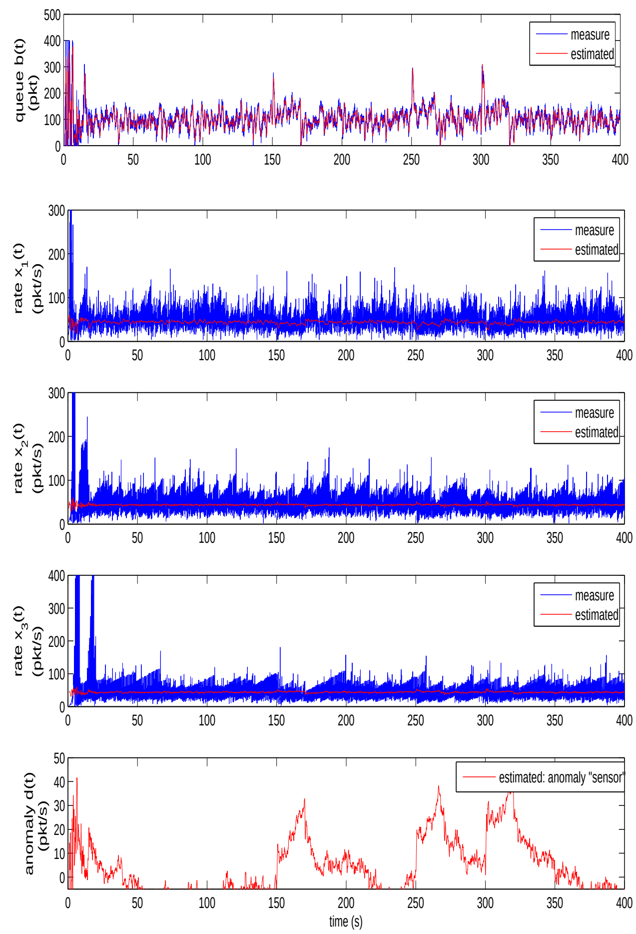

Fig. 6. Observer over gain-K: original/estimated states and anomaly detection (simulation on NS)

Table IV-A shows that the observer state matches average flow rates.

B. Emulation

Going further than simulations, another example is proposed considering now 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) real traffics using a real-time scheduler (see [17] and Figure 7).

TABLE I

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

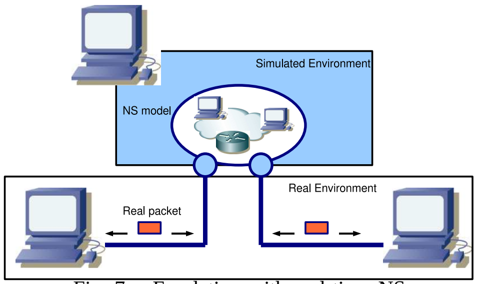

Fig. 7. Emulation with real-time NS

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.

However, since the emulator requires a high computational cost, numerical values of the example must be scaled down. The considered example takes the same topology as in Figure 5 but the router bandwidth is reduced to $1Mbps$ and propagation delays are divided by 2. Source traffics are generated with the network tool Iperf. Applying a congestion control mechanism, the queue size of the buffer is regulated and a linear observer can thus be developed according to the appropriate equilibrium point. Results of the emulation are shown in Figure 8.

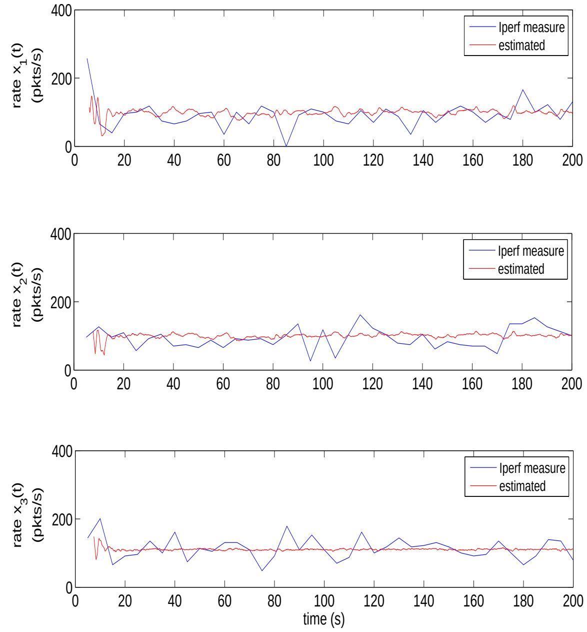

Fig. 8. Observer over gain-K: original/estimated of rates

V. CONCLUSIONS

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.

REFERENCES

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

[2] 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*, 2000, pp. 1–7.

[3] V. Jacobson, "Congestion avoidance and control," in *ACM SIGCOMM*, Stanford, CA, Aug. 1988, pp. 314–329.

[4] H. S. Low, F. Paganini, and J. Doyle, *Internet Congestion Control*. IEEE Control Systems Magazine, Feb 2002, vol. 22, pp. 28–43.

[5] 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*, Aug. 2000, pp. 151–160.

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

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

[8] 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*, New Orleans, USA, Dec. 2007, pp. 3818–3823.

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

[10] 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*, vol. 47, pp. 945–959, June 2002.

[11] D. Peaucelle, D. Arzelier, D. Henrion, and F. Gouaisbaut, "Quadratic separation for feedback connection of an uncertain matrix and an implicit linear transformation," *Automatica*, vol. 43, no. 5, pp. 795–804, 2007.

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

[13] S. E. I. CERT, "Denial of service attacks," http://www.cert.org/tech_tips/denial_of_service.html.

[14] 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*, 2005, pp. 97–104.

[15] Y. Ariba, F. Gouaisbaut, S. Rahme, and Y. Labit, "Robust control tools for traffic monitoring in tcp/aqm networks," LAAS-CNRS, Paul Sabatier University, Toulouse, France, Tech. Rep. 09042, Jan. 2009, available on-line http://hal.archives-ouvertes.fr/hal-00357761/fr/.

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

[17] 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.