Network anomaly estimation for TCP/AQM networks using an observer

Yassine Ariba, Yann Labit, Frederic Gouaisbaut

University of Toulouse, LAAS-CNRS
7 avenue du Colonel Roche, 31077 Toulouse cedex 4 FRANCE
Email: {ylabit, fgouaisb, yariba}@laas.fr

***Abstract*— Network anomaly detection is an active research area in network community. Researchers have approached this problem using various techniques such as artificial intelligence, machine learning, state machine modeling, statistical approaches. The purpose of this preliminary work is to design an observer for network anomaly estimation for TCP/AQM (Transmission Control Protocol/Active Queue Management) networks using time delay system approach. Collaborating an observer with an AQM, constant anomalies considered as perturbations for the network can be detected. We illustrate the effectiveness of results via SIMULINK and the NS-2 simulator.**

Keywords: Network anomaly detection, Observer, AQM, Time delay system.

I. Motivations

Network anomalies typically refer to circumstances when network operations deviate from normal network behavior. Detecting anomalies such as malfunctioning network devices, network overload, flash crowds, worms, port scans, risky internal user behavior, malicious denial of service attacks (DoS), network intrusions that disrupt the normal delivery of network services has become an important key issue for the network community. Such anomalies can be found at any time in the traffic and degrade Quality of Service (QoS) of the network: congestion at first, then non-responsive routers and even worse. Network anomalies (in sense that there is a deviation from the normal network condition) can be roughly classified into two categories. The first category is related to network failures and performance problems (like file server failures, broadcast storms, etc...). The second major category of network anomalies is security-related problems (like DoS or DDoS detections) in detecting active security threats. A variety of tools and techniques exists to detect anomalies mainly based on information theory called IDS (Intrusion Detection Systems) and ADS (Anomaly Detection Systems). They both look for "bad things" on a system or network, things that may be potential security incidents. An IDS uses a defined set of rules or filters that have been crafted to catch a specific, malicious event. IDS are based on two principal techniques to detect the anomalies/intrusions of the traffic: First, the use of signatures i.e. of specific formats of packages or particular successions of packages giving place to the attack. This technique is not well adapted to the detection of the variations of the traffic which has not a particular signature (like flash crowd or of DDoS without signature). Secondly, the use of statistical profiles of the traffic can be used. But nowadays, approaches which used the statistics are mainly limited to first order (average and standard deviation). The very strong natural variability of the traffic [1] produced a strong fluctuation of these measurements, thus inducing very high level of false positives (false alarms) and false negatives (missed detections). Recent studies take into account a richer form of the statistical structure of the traffic (correlation, spectral density ...) [2], [3], [4], [5], [6]. An ADS, on the other hand, operates only from a baseline of normal activity. As described above, behavior that varies from this standard is noted. While an IDS looks mainly for a misuse signature, the ADS looks for a strange event which leads to unapproved network changes.

In this paper, we propose to design an observer in the time delay systems framework for the anomalies detection. The main advantage of this technique is that we avoid the problem of false positives/negatives appeared in statistical approaches. The observer synthesis is based on a linearized fluid flow model of the TCP/AQM behaviour. Consequently, an AQM regulating the queue size of the router buffer is required to ensure the relevance of the observer. Hence, the observer must be associated to an AQM to perform its diagnosis. Note that taking into account the drop probability fixed by the AQM, the detecting mechanism is independent of the former (as long as the AQM is able to regulate the queue size at a prescribed level).

The paper is organized as follows. The second part presents the problem statement introducing the model of a network supporting TCP and AQM for congestion control. Then, section III is dedicated to the observer design for the detection and the estimation of anomalies. Section IV presents application of the exposed theory and simulation results using SIMULINK and NS-2 (see [7]). Finally, Section V concludes the paper.

Notations: For two symmetric matrices, A and B, $A > (\geq)$ B means that $A-B$ is (semi-) positive definite. A^T denotes the transpose of A. 1_n and $0_{m\times n}$ 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.

II. Problem statement

In this section, we describe first the considered network topology and the linearized fluid-flow model of TCP. Then,

we recall the AQM mechanism which must be associated with the proposed observer.

A. Network topology

In this paper, we consider the network topology consisting of N TCP sources, with the same propagation delay connected to a destination node through a router (see figure 1). The

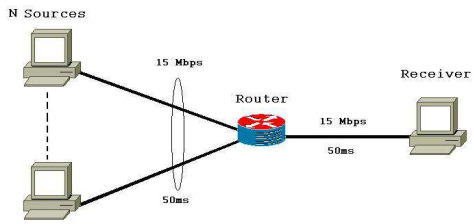

Fig. 1. A network topology

bottleneck link is shared by N flows and TCP applies the well known congestion avoidance algorithm to cope with the phenomenon of congestion collapse [8]. Many studies have been dedicated to the modeling of TCP and its AIMD (additive-increase multiplicative-deacrease) behavior [9], [10], [11] and references therein.

B. The linearized fluid-flow model of TCP

We consider in this work the model (1) developed by [12]. This latter describes the mean dynamic behaviours of the sources congestion window W and the queue at the router buffer q. This model may not capture with high accuracy the dynamic behaviour of TCP but its simplicity allows us to apply our methodology. Let consider the following model

$$\left\{\begin{array}{rcl} \dot{W}(t) & = & \frac{1}{R(t)} - \frac{W(t)W(t-R(t))}{2R(t-R(t))}p(t-R(t)) \\ \dot{q}(t) & = & \frac{W(t)}{R(t)}N - C + d(t) \end{array}\right. \quad (1)$$

where W is the TCP window size, q is the queue length of the router buffer, R is the round trip time (RTT) and can be expressed as $R = q/C + T_p$. C, T_p and N are parameters related to the network configuration and represent the transmission capacity of the router, the propagation delay and the number of TCP sessions respectively. The variable p is the marking/dropping probability of a packet (that depends whether the ECN option, explicit congestion notification, is enabled, see [13]). In the mathematical model (1), we have introduced an additional signal $d(t)$ which models crossing traffics passing through the router and filling the buffer. These traffics are not TCP based flows (not modeled in TCP dynamic) and can be viewed as perturbations since they are not reactive to packets dropping (for example, UDP based traffic). A linearization and some simplifications of (1) was carried out in [14] to allow the use of traditional control theory approach. The linearized fluid-flow model of TCP is as follow,

$$\left\{\begin{array}{l} \delta\dot{W}(t) = -\frac{N}{R_0^2C}\Big(\delta W(t) + \delta W(t-h(t))\Big) \\ \qquad -\frac{1}{R_0^2C}\Big(\delta q(t) - \delta q(t-h(t))\Big) - \frac{R_0C^2}{2N^2}\delta p(t-h(t)) \\ \delta\dot{q}(t) = \frac{N}{R_0}\delta W(t) - \frac{1}{R_0}\delta q(t) + d(t) \end{array}\right. \quad (2)$$

where $\delta W \doteq W - W_0$, $\delta q \doteq q - q_0$ and $\delta p \doteq p - p_0$ are the perturbated variables about the operating point. The operating point (W_0, q_0, p_0) is defined by

$$\left\{\begin{array}{l} \dot{W} = 0 \;\Rightarrow\; W_0^2 p_0 = 2 \\ \dot{q} = 0 \;\Rightarrow\; W_0 = \frac{R_0C}{N},\; R_0 = \frac{q_0}{C} + T_p \end{array}\right. \quad (3)$$

The input of the model (2) corresponds to the drop probability of a packet fixed by an AQM. This latter has for objective to regulate the queue size of the router buffer.

In this paper, the dynamics of the queue and the congestion window are modeled as a time delay system. Indeed, the delay is an intrinsic phenomenon in networks and taking into account its characteristic should improve the precision of our model with respect to the TCP behavior. The linearized TCP fluid model (2) can be rewritten as the following time delay system:

$$\left\{\begin{array}{l} \dot{x}(t) = Ax(t) + A_dx(t-h) + Bu(t-h) + B_dd(t) \\ x_0(\theta) = \phi(\theta), \text{ with } \theta \in [-h, 0] \end{array}\right. \quad (4)$$

with

$$A = \left[\begin{array}{cc} -\frac{N}{R_0^2C} & -\frac{1}{CR_0^2} \\ \frac{N}{R_0} & -\frac{1}{R_0} \end{array}\right],\; A_d = \left[\begin{array}{cc} -\frac{N}{R_0^2C} & \frac{1}{R_0^2C} \\ 0 & 0 \end{array}\right],\; B = \left[\begin{array}{c} -\frac{C^2R_0}{2N^2} \\ 0 \end{array}\right] \quad (5)$$

$B_d = [0 \;\; 1]^T$, $x(t) = [\delta W(t) \;\; \delta q(t)]^T$ is the state vector and $u(t) = \delta p(t)$ the input. $\phi(\theta)$ is the initial condition.

C. AQM for congestion control

To achieve high efficiency and high reliability of communications in computer networks without considering anomaly, there are many investigations of congestion control systems like AQM (Active Queue Management, see figure 2). This latter mechanism regulates the queue length of a router by actively dropping packets. This strategy allow the TCP flows regulation with an implicit control (or explicit if the ECN mechanism is enabled). Various mechanisms have been proposed in the literature such as Random Early Detection (RED) [15], Random Early Marking (REM) [16], Adaptive Virtual Queue (AVQ) [17] and many others [18]. Their performances have been evaluated in [18] and empirical studies have shown their effectiveness (see [19]). Recently, significant studies proposed by [14] 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 [12], many research have been devoted to deal with congestion problem in a control theory framework (for examples see [20], [21], [11] and references therein).

In the next section, the observer is designed taking into account the drop probability generated by the AQM. Hence, measuring this latter quantity the observer can be associated to any AQM and provides estimations independently from the congestion control strategy. Note that although dealing with a different problem, the observation principle has yet been used

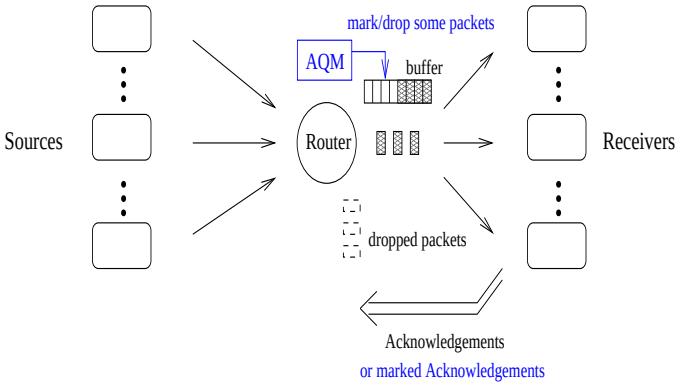

Fig. 2. AQM for congestion control

at an AQM router to make inferences about the traffic passing through it [22].

III. Observer design for an ADS

A. Augmented model

As it has been previously stated, the disturbance detection can be performed with the use of an observer. To this end, an augmented system that takes into account the disturbance is considered. Assuming a constant or piecewise-constant function $d(t)$, the following new model is derived

$$\dot{\tilde{x}} = \underbrace{\begin{bmatrix} A & 0 \\ 0\ 0 & 1 \\ 0\ 0 & 0 \end{bmatrix}}_{\bar{A}} \tilde{x}(t) + \underbrace{\begin{bmatrix} A_d & 0 \\ 0\ 0 & 0 \\ 0\ 0 & 0 \end{bmatrix}}_{\bar{A}_d} \tilde{x}(t-h) + \underbrace{\begin{bmatrix} B \\ 0 \end{bmatrix}}_{\bar{B}} \delta p(t-h) \tag{6}$$

where $\tilde{x}^T = [\delta W \quad \delta q \quad d]^T$ represents the augmented state. Notice that a constant or piecewise-constant function $d(t)$ is suitable to model CBR (*constant bit rate*) type traffics. Then, an observer has to be designed to reconstruct the whole state of (6), in particular non-TCP flows modeled by d. Remarks that the observer is thus developed for the traffic diagnosis and the detection of CBR type application. The methodology to derive this latter is proposed in the next subsection and depend on measured signals. The static equation that express the output of system (6): $y(t) = \bar{C}\tilde{x}(t) = [0 \quad 1 \quad 0]\tilde{x}(t)$, measures the queue size of the router buffer.

B. Observer design

Let construct an observer for the augmented system defined by the following differential equation:

$$\frac{d\hat{x}(t)}{dt} = (\bar{A} - G\bar{C})\hat{x}(t) + \bar{A}_d\hat{x}(t-h) + \bar{B}\delta p(t-h) + Gy(t),$$

where $\hat{x}(t)$ is the observer state, G, called the observer gain is a matrix to be designed. 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) which allows the reconstruction of the states of system (6). Let define the error between the state of the system $\tilde{x}(t)$ et the state of the observer $\hat{x}(t)$:

$$\epsilon(t) = \hat{x}(t) - \tilde{x}(t) \tag{7}$$

As we aim at reconstructing the states variables and especially the unknown disturbance, we have to prove the asymptotic convergence of the error towards zero. The error dynamic is driven by the following time delay differential equation:

$$\dot{\epsilon}(t) = (\bar{A} - G\bar{C})\epsilon(t) + \bar{A}_d\epsilon(t-h) \tag{8}$$

The following theorem gives a simple way to construct the unknown matrix G in order to stabilize (8).

Theorem 1 *For given h, α, if there exists two definite positive matrices P, Q of appropriate dimension, a matrix W such that the following LMI holds*

$$\Xi = \begin{bmatrix} \Xi_{11} & \Xi_{12} & \Xi_{13} \\ \Xi_{12}^T & \Xi_{22} & 0 \\ \Xi_{13}^T & 0 & -P \end{bmatrix}$$

where

$$\begin{aligned} \Xi_{11} &= \bar{A}P - C^TW^T + P\bar{A} - W\bar{C} + Q - \tfrac{\alpha}{h}P \\ \Xi_{12} &= \tfrac{\alpha}{h}P + h\alpha(P\bar{A} - W\bar{C})^T\bar{A}d \\ \Xi_{13} &= h\alpha(P\bar{A} - W\bar{C})^T \\ \Xi_{22} &= -Q + h\alpha\bar{A}_d^TP\bar{A}_d - \tfrac{\alpha}{h}P \end{aligned}$$

then the system defined by (7) and (8) is asymptotically stable and the observer gain is given by $G = P^{-1}W$.

Proof: In order to prove the asymptotic convergence of $\epsilon(t)$ towards zero, let us introduce an appropriate Lyapunov Krasovskii functional:

$$V(t) = \epsilon(t)^TP\epsilon(t) + \int_{t-h}^{t} \epsilon(s)Q\epsilon(s)ds + \int_{t-h}^{t}\int_{s}^{t} \dot{\epsilon}(v)R\dot{\epsilon}(v)dvds$$

The derivative of V along the trajectories of (8) leads to:

$$\begin{aligned} \dot{V}(t) \quad &= 2\dot{\epsilon}(t)^TP\epsilon(t) \\ &+h\dot{\epsilon}(t)^TR\dot{\epsilon}(t) - \int_{t-h}^{t} \epsilon(s)^TR\epsilon(s)ds \\ &+\epsilon(t)^TQ\epsilon(t) - \epsilon(t-h)^TQ\epsilon(t-h) \end{aligned}$$

Using Jensen inequality, which states that $-\int_{t-h}^{t} \epsilon(s)^TR\epsilon(s)ds \leq \frac{1}{h}(\epsilon(t)-\epsilon(t-h))^TR(\epsilon(t)-\epsilon(t-h))$, an upper bound of the derivative of V is given by :

$$\dot{V}(t) < \zeta(t)^T \begin{bmatrix} \Gamma_{11} & \Gamma_{12} \\ \Gamma_{11}^T & \Gamma_{22} \end{bmatrix} \zeta(t)$$

where

$$\begin{aligned} \Gamma_{11} &= (\bar{A} - G\bar{C})^TP + P(\bar{A} - G\bar{C}) + Q - \tfrac{1}{h}R \\ &\quad + h(\bar{A} - G\bar{C})^TR(\bar{A} - G\bar{C}) \\ \Gamma_{12} &= \tfrac{1}{h}R + h(\bar{A} - G\bar{C})^TR\bar{A}d \\ \Gamma_{22} &= -Q + hA_d^TRA_d - \tfrac{1}{h}R \end{aligned}$$

and

$$\zeta(t) = \begin{bmatrix} \epsilon(t) \\ \epsilon(t-h) \end{bmatrix}$$

In order to obtain a simple design criterion, let choose $R = \alpha P$, with α a given constant, and by noting $W = PG$, the following matrix $\begin{bmatrix} \Gamma_{11} & \Gamma_{12} \\ \Gamma_{11}^T & \Gamma_{22} \end{bmatrix}$ is reduced to

$$\begin{aligned}\Gamma_{11} &= (\bar{A} - G\bar{C})^T P + P(\bar{A} - G\bar{C}) + Q - \tfrac{\alpha}{h} R \\ &\quad + h\alpha(P\bar{A} - W\bar{C})^T P^{-1}(P\bar{A} - W\bar{C}) \\ \Gamma_{12} &= \tfrac{\alpha}{h} P + h(P\bar{A} - W\bar{C})^T \bar{A}d \\ \Gamma_{22} &= -Q + h\alpha A_d^T P A_d - \tfrac{\alpha}{h} P\end{aligned}$$

The system defined by equations (7) and (8) is then asymptotically stable if

$$\begin{bmatrix} \Gamma_{11} & \Gamma_{12} \\ \Gamma_{11}^T & \Gamma_{22} \end{bmatrix} < 0$$

Using schur complement, this last inequality is equivalent to $\Xi < 0$, which concludes the proof.

■

Remark 1 *It can be easily proved that if system (8) is stable for a given h, then it is also stable for all delays less that this prescribed upperbound.*

IV. Simulink and NS-2 simulations

A. Simulink

This subsection is dedicated to the Simulink simulations of the nonlinear time-delay model of the network (1). The observer mechanism has to detect the anomalous traffic CBR coming from different sources (see figure 3). In this simulation, the network is under an anomaly from $t = 20s$ and repeated each 10s with a pulse width of 50 per cent. The amplitude of this anomaly is 10 packets, a small level to show that the observer can estimate states and pertubation even if "small" anomalies are present. The nonlinear model of the network is reactive and the observer shows that it could be easy to detect anomalous traffic as it is described on the figure 6. Note that the AQM employed in this simulation is the state feedback developed in [20].

As it is shown on figures 4 and 5, the states of the model are well estimated and the perturbation is detected correctly (figure 6).

B. NS-2

Simulink experiments show that our observer manages to estimate states but also manages to estimate an anomalous traffic. We aim at proving the effectiveness of our method using NS-2 [7], a network simulator. As a widely adopted numerical illustration extracted from [14] (see figure 1 for the network topology), let consider the case where $q_{ref} = 175$ packets, $T_p = 0.2$ second and $C = 3750$ packets/s (corresponds to a 15 Mb/s link with average packet size 500 bytes). Then, for a load of $N = 60$ TCP sessions, we have $W_0 = 15$ packets, $p_0 = 0.008$, $R_0 = 0.246$ seconds. According to the state feedback AQM presented in [20], $K = 10^{-3} \begin{bmatrix} -0.2372 \\ 0.0429 \end{bmatrix}$. Taking values from the previous numerical example, we apply the new AQM based on a state feedback associated to the proposed observer, see figure 9: original states, estimated states and estimated anomalous traffic are illustrated on it. The target queue length q_0 is 175 packets while buffer size is 800. The proposed observer has also been tested with RED AQM and PI AQM from [14], see figures 7 and 8. The anomalous traffic is constant beginning at $t = 100s$ and ending at $t = 140s$. In the both cases the whole state is correctly well estimated and the observer can detect the anomaly phenomenon. However, the perturbation is much more estimated using the set (state-space AQM [20], the proposed observer) rather than the two others cases. This comes from the quality and the high efficiency of the states estimation.

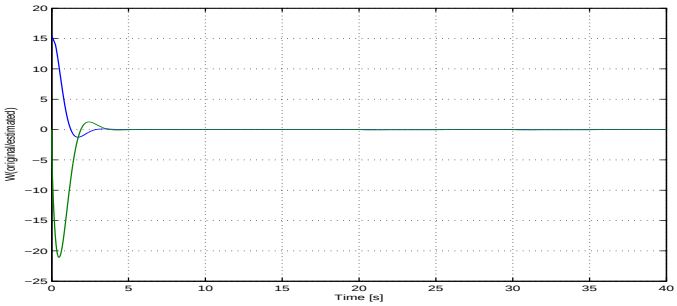

Fig. 4. W window (estimated (blue line) / original (green line))

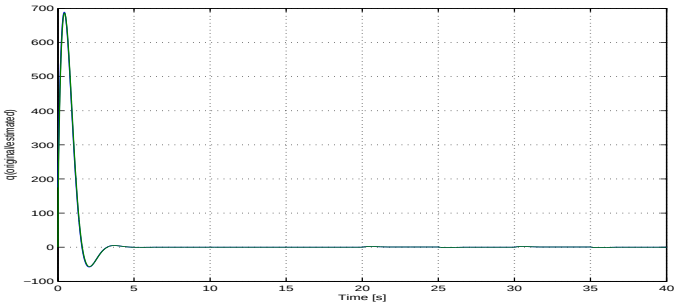

Fig. 5. Queue length q (estimated (blue line) / original (green line))

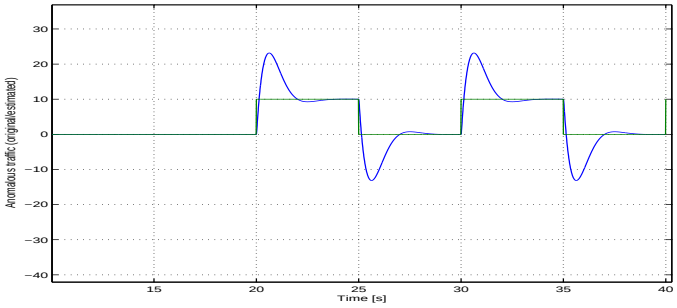

Fig. 6. Anomalous traffic (estimated (blue line) / original (green line))

V. Future works

Anomaly Detection will play a key role in advancing the capabilities of security technology. As the number of threats grows and diversifies, an ADS becomes a required element of system security. To protect ourselves against unknown threats, we designed an observer for the estimation of anomalous traffics without having the problem of false positives/negatives.

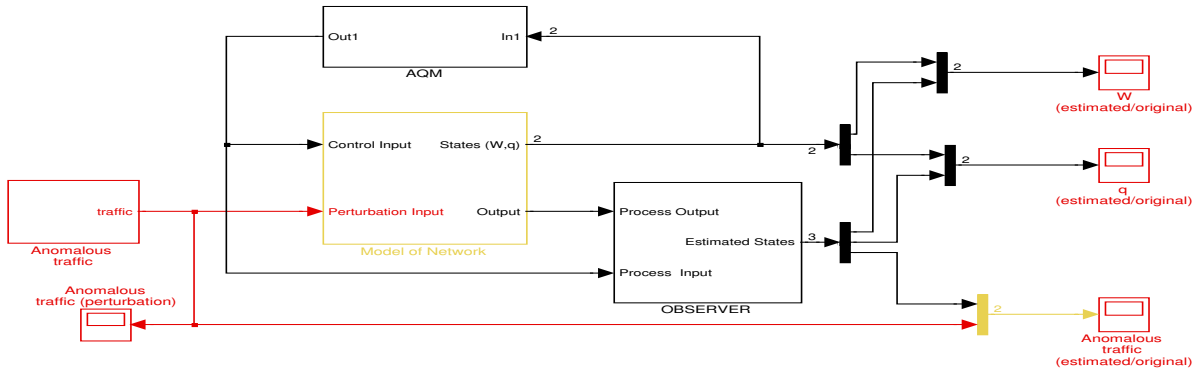

Fig. 3. Simulink of the closed-loop system under anomalous traffic

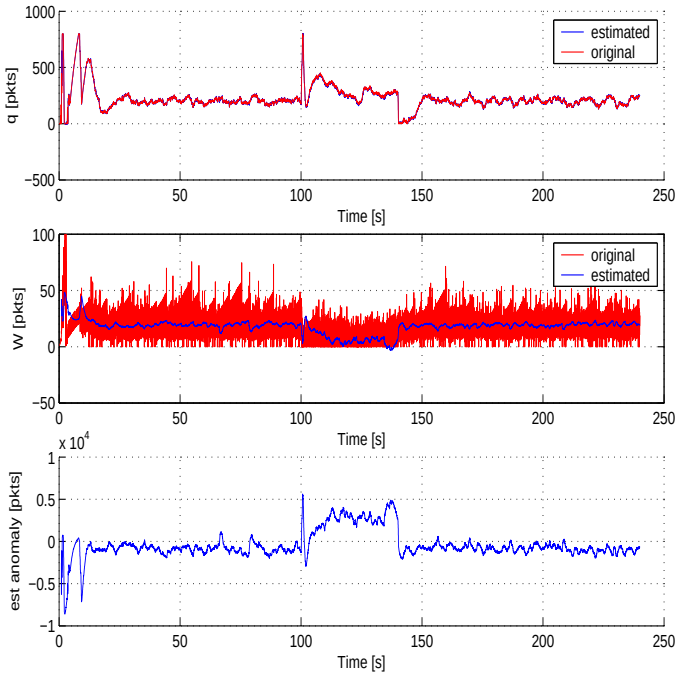

Fig. 7. RED configuration: estimated/original states and estimated anomaly

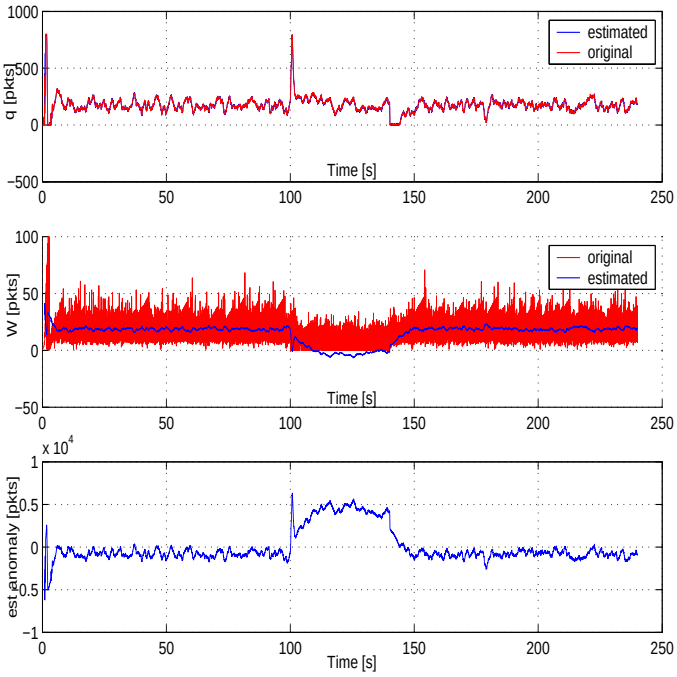

Fig. 8. PI configuration: estimated/original states and estimated anomaly

Using this technique, one can estimate different network anomalies (such as downloads, flash crowds...). This latter is independent from the congestion control policy and can then be implemented on different AQM mechanisms. Finally, the proposed methodology has been validated using Simulink and NS simulator. Based on this preliminary work, we have to improve the classification of estimated anomalies.

REFERENCES

[1] 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*, Oct 1996, p. 171.

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

[3] N. Ye, "A markov chain model of temporal behavior for anomaly detection," in *Proceedings of the 2000 IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop*, 2000, pp. 171–174.

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

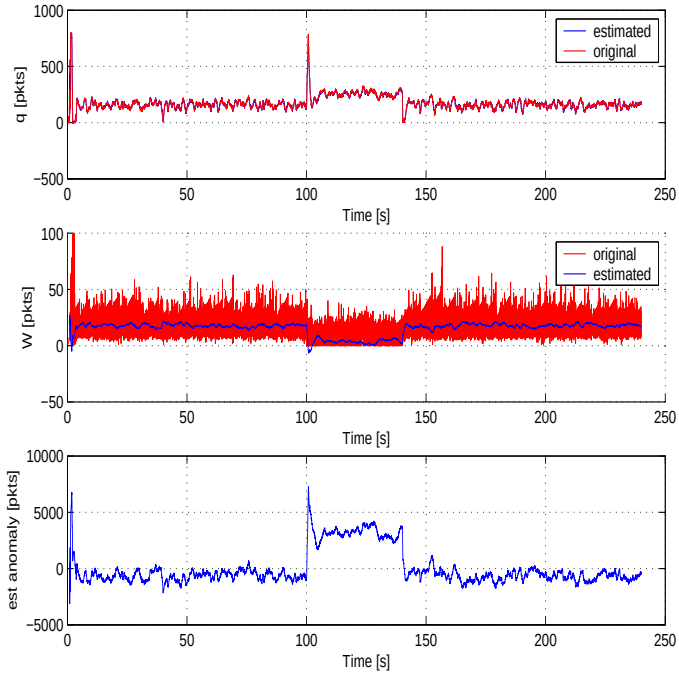

Fig. 9. K configuration: estimated/original states and estimated anomaly

[5] P. Barford, J. Kline, D. Plonka, and A. Ron, "A signal analysis of network traffic anomalies," in *Internet Measurement Workshop 2002*, 2002.

[6] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for cdns and web sites," in *In Proceedings of the International World Wide Web Conference*, 2002, pp. 252–262.

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

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

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

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

[12] 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 *SIGCOMM*, Aug. 2000, pp. 151–160.

[13] K. K. Ramakrishnan and S. Floyd, "A proposal to add explicit congestion notification (ecn) to ip," RFC 2481, Jan. 1999.

[14] 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.

[15] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," *IEEE/ACM Transactions on Networking*, vol. 1, pp. 397–413, Aug. 1993.

[16] S. Athuraliya, D. Lapsley, and S. Low, "An enhanced random early marking algorithm for internet flow control," in *IEEE INFOCOM*, Dec. 2000, pp. 1425–1434.

[17] S. Kunniyur and R. Srikant, "Analysis and design of an adaptive virtual queue (avq) algorithm for active queue management," in *SIGCOMM'01*, San Diego, CA, USA, aug 2001, pp. 123–134.

[18] 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.

[19] L. Le, J. Aikat, K. Jeffay, and F. Donelson Smith, "The effects of active queue management on web performance," in *SIGCOMM*, Aug. 2003, pp. 265–276.

[20] Y. Labit, Y. Ariba, and F. Gouaisbaut, "Design of lyapunov based controllers as tcp aqm," in *2nd IEEE Workshop on Feedback control implementation and design in computing systems and networks (FeBID'07)*, Munich, Germany, May 2007, pp. 45–50.

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

[22] H. Zhang, C. V. Hollot, D. Towsley, and V. Misra, "A self-tuning structure for adaptation in tcp/aqm networks," in *Globecom*, vol. 7, 2003, pp. 3641–3646.