Sliding Modes for Anomaly Observation in TCP Networks: From Theory to Practice

Sandy Rahme, Yann Labit, Frédéric Gouaisbaut, Thierry Floquet

Sliding modes for anomaly observation in TCP networks: from theory to practice.

Sandy Rahmé, Yann Labit, Frédéric Gouaisbaut and Thierry Floquet

Abstract

Anomaly detection has been an active open problem in the networks community since several years. In this article we aim at detecting such abnormal signals by control theory techniques. Several classes of sliding mode observers are proposed for a fluid flow model of TCP/IP network. Comparative simulations via Network Simulator NS-2 show the enhancement brought by higher order sliding mode observer. The efficiency of this latter observer opens the way towards observing traffics with real TCP flows characteristics. To achieve this end, trace replay techniques for TCP traffic traces are presented. Finally, experiments lead to successful anomaly estimation under real traffic conditions.

I. INTRODUCTION

Communication networks have greatly grown in complexity that is demanding a guaranteed Quality of Service (QoS) more than ever. Networks QoS is highly sensitive to a wide variety of disruptions, often designated as anomalies. Anomalies are often related to physical or technical problems such as power or file server failures, abrupt changes caused by legitimate traffic such as network overload or flash crowds, and risky illegitimate behavior such as *Denial of Service* attacks [1]. These attacks can be accomplished by the exploitation of TCP/IP flaws at one target, flooding it with packets, and also can take a distributed configuration called Distributed Denial of Service or DDoS attacks, hardening the identification of the attacking sources.

Anomaly detection has been the topic of a number of surveys and articles (see for example [2] and references therein). Roughly speaking, anomaly detection can be classified into two

S. Rahmé, Y. Labit, and F. Gouaisbaut are with both CNRS; LAAS; 7 avenue du colonel Roche, F-31077 Toulouse Cedex 4, France and University of Toulouse; UPS, INSA, INP, ISAE, UT1, UTM, LAAS; F-31077 Toulouse Cedex 4, France. {srahme, ylabit, fgouaisb@laas.fr}

T. Floquet is with both LAGIS, FRE CNRS 3303, École Centrale de Lille, BP48, 59651 Villeneuve d'Ascq Cedex, France and INRIA Lille - Nord Europe, Équipe - Projet Non-A, France. thierry.floquet@ec-lille.fr

different ways. Intrusion Detection Systems (IDS) are probably the most common ways for detecting anomalies. An IDS monitors packets flowing in the network and compares them with preconfigured and predetermined attack patterns known as signatures. Another type of detecting systems is the Anomaly Detection Systems (ADS) which are concerned with general activities that differ from normal network behavior. The main advantage of an ADS is that it does not require prior knowledge of specific intrusion signatures [3]. Thus, instead of defining a large number of known intrusions, it is enough to define a profile for a normal activity.

Contrary to previous work, we address the problem of anomaly detection by designing an observer to estimate the anomaly that represents the unmeasurable disturbances in the TCP network. Sliding mode techniques are often used to design robust nonlinear observers or control laws because of their robustness against various kinds of uncertainties such as parameter perturbations, external disturbances and measurement errors. Moreover, they can be used unknown input reconstruction that has found useful applications in fault detection and isolation [4], [5]. Based on the TCP fluid flow model conceived in [6], we aim at developing sliding mode observers for a TCP network. To the best of our knowledge, for observation/detection purpose, this framework has been barely adopted. In [7], a classical Luenberger observer coupled with an extended state is designed for detecting Constant Bit Rate (CBR) anomalies. In this paper, first order sliding mode observers were first studied for the detection problem. However, the high frequency oscillations induced have to be smoothed by filtering techniques. Another relevant method is the design of higher order sliding mode observer [8] whose performances show significant improvements in terms of good tracking of the real anomaly shape and the instantaneous detection of the anomaly variations. Successful simulations tested on the adopted model for TCP dynamics [6], lead us to focus on observing anomalies under real traffic conditions. One practical means consists of replaying real TCP traffic in a simulator so that all traffic characteristics might be taken into account via the Network Simulator NS-2 [9].

The article is organized as follows. Section II presents the TCP network topology and the problem statement. In Section III, first and second order sliding mode observers are designed for estimating anomalies in TCP networks. The performances of the conceived observers are evaluated via Matlab/Simulink and NS-2 in Section IV. In Section V, a procedure for replaying

TCP flows in NS-2 while preserving their real characteristics is introduced.

II. TCP MECHANISM AND MODELING

A. TCP fluid flow model

In this article, a congested router is considered where packets sent from N homogeneous sources flow through to reach their destinations (c.f. Figure 1). Mathematical modeling of TCP

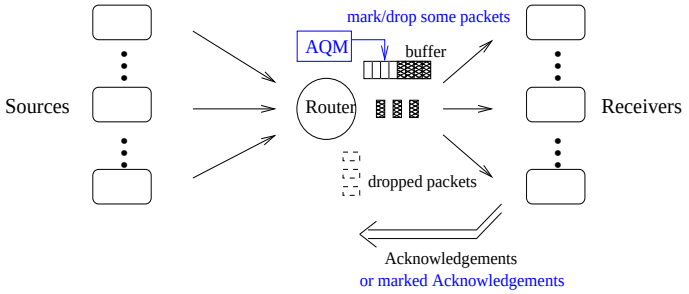


Fig. 1: TCP network topology.

networks has been widely studied in the literature [6], [10]. In [6], a fluid-flow model for the TCP traffic is considered using specifically a stochastic differential equation analysis. Simulation results on such a model demonstrated the accuracy in capturing the TCP dynamics. Our work will be focused on a simplified version where the packets lost caused by timeout mechanism (TO) is ignored. Therefore it is assumed that the losses occur in the network because of unavoidable congestion conditions when the router cannot buffer the number of arriving packets. The average dynamics of the TCP congestion window size $W(t)$ and the queue length $q(t)$ of the router buffer are described by the following coupled equations:

$$\begin{cases} \dot{W}(t) &= \frac{1}{R(t)} - \frac{W(t)W(t-R(t))}{2R(t-R(t))}p(t-R(t)), \\ \dot{q}(t) &= \frac{W(t)}{R(t)}N - C + d(t), \\ R(t) &= \frac{q(t)}{C} + T_p. \end{cases} \tag{1}$$

The differential equations expressed at packet level in the previous model depend on the number of TCP connections N, on the packets round trip time $R(t)$ [s], on the link capacity C [packets/s], the propagation delay T_p [s] and the dropping probability $p(t)$ of a packet entering the buffer queue. The anomaly flowing through the router is represented by $d(t)$. This extra signal is added to the queue length dynamics in order to represent any additional unknown traffic perturbing the

normal TCP network behavior.

An observer will be designed to first estimate the average TCP congestion window size $W(t)$, and then reconstruct the anomaly based on the known queue length $q(t)$ of the router. For the observer design described afterwards, the anomaly $d(t)$ and its first time derivative are supposed to be bounded by upper bound d_{max} and $\dot{d}_{max}$ respectively.

Because of the complexity of the nonlinear system (1), a linearized fluid-flow system around the equilibrium point is required as the following:

$$\begin{cases} \delta\dot{W}(t) = & -\frac{N}{R_0^2 C}(\delta W(t) + \delta W(t - h(t))) - \frac{1}{R_0^2 C}(\delta q(t) - \delta q(t - h(t))) - \frac{R_0^2 C^2}{2N^2}\delta p(t - h(t)), \\ \delta\dot{q}(t) = & \frac{N}{R_0}\delta W(t) - \frac{1}{R_0}\delta q(t) + d(t). \end{cases} \tag{2}$$

The equilibrium point is obtained from the system of equations:

$$\begin{cases} W_0^2 p_0 &= 2, \\ W_0 &= \frac{R_0 C}{N}, \\ R_0 &= \frac{q_0}{C} + T_p, \\ d_0 &= 0. \end{cases} \tag{3}$$

To maintain the stability of the whole TCP network, Active Queue Management (AQM) has been proposed, to detect incipient congestion. While monitoring the instantaneous or average queue size, dropping or marking packets mechanisms are determined. Many AQM mechanisms have been developed after the Random Early Detection (RED) algorithm, such as stabilized-RED (SRED), BLUE, REM, adaptive virtual queue (AVQ) and many others evaluated in [11]. PI, PID [12], and static state feedback controllers [7], based on control theory, are developed for TCP models (like in [6]) to achieve satisfactory control performance in terms of the queue length dynamics, the packet loss rates or the link utilization.

III. Sliding mode observers for monitoring TCP traffic

A. Principle of sliding modes

The sliding mode approach is a way to force the system to evolve after a finite time on a suitable sliding manifold by the use of a discontinuous output injection signal. For the observation prupose, the sliding manifold is usually given by the difference between the observer and the system output. Unknown inputs, if any, can be explicitly reconstructed by analyzing the so-called equivalent information (or output) injection [4], [13]. However, the main drawback is

the undesirable high-frequency oscillations, typically referred to as the chattering phenomenon, caused by fast switching in the discontinuous control signal. Sliding modes were generalized under the concept of higher order sliding modes conceived in order to reduce the chattering phenomenon while preserving the robustness properties. The sliding surface is thus defined by the vanishing of a corresponding sliding surface s and its successive time derivatives up to a certain order, defining the r^{th} order sliding set:

$$\mathcal{S}_r = \left\{ x \in \mathbb{R}^n : s = \dot{s} = \ldots = s^{(r-1)} = 0 \right\}.$$

A control law leading to such a behavior is called a r^{th} order ideal sliding mode algorithm with respect to s. Designs for either observation or control, with applications in mechanics, robotics or electric machines, can be found in the literature [14], [15].

B. First order sliding observer

Before going through the design of the observer, the linearized system (2) must be reformulated to ensure the efficiency of sliding modes. Once a subset of the system dynamics is known, thus defined as output, the discontinuous injection signal is added to the latter so that the ability of the system to attain and maintain sliding motion will be more efficient than taking into account the complete system [16]. Therefore, the state $x(t)$ and the output $y(t)$ in the reformulated system (4) will refer respectively to the unknown congestion window size and the router queue length.

$$\begin{cases} \dot{x}(t) = & Mx(t) + M_d x(t-h) + Dy(t) + D_d y(t-h) + E_d u(t-h), \\ \dot{y}(t) = & Gx(t) + Hy(t) + d(t), \end{cases} \tag{4}$$

where $u(t) = \delta p(t)$ the input, and

$$M = M_d = -\frac{N}{R_0^2 C},\ D = -\frac{1}{R_0^2 C},\ D_d = \frac{1}{R_0^2 C}, E_d = -\frac{R_0 C^2}{2N^2},\ G = \frac{N}{R_0}\ \text{, and } H = -\frac{1}{R_0}.$$

A sliding mode observer can be designed as follows:

$$\begin{cases} \dot{\hat{x}}(t) = & M\hat{x}(t) + M_d \hat{x}(t-h) + Dy(t) + D_d y(t-h) + E_d u(t-h), \\ \dot{\hat{y}}(t) = & G\hat{x}(t) + Hy(t) + L(\hat{y}(t) - y(t)) + \nu(t), \end{cases} \tag{5}$$

where L is the linear gain of the observer and $\nu(t)$ the discontinuous function of the form:

$$\nu = \begin{cases} -k\text{sign}(\hat{y}(t) - y(t)), & \text{if } \hat{y}(t) \neq y(t), \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

Given the estimation errors $e_x(t) = \hat{x}(t) - x(t)$ and $e_y(t) = \hat{y}(t) - y(t)$, their dynamics with respect to (4) are then governed by the equations:

$$\begin{cases} \dot{e}_x(t) &= Me_x(t) + M_d e_x(t-h), \\ \dot{e}_y(t) &= Ge_x(t) + Le_y(t) + \nu(t) - d(t). \end{cases} \tag{7}$$

In order to prove the stability of the sliding observer and the convergence of $\hat{x}$ towards x, we propose the following theorem:

Theorem 1 *Given scalars $L < 0$, $p_y > 0$ and an appropriate discontinuous function ν* (6) *such that $k > G|e_x|_{max} + d_{max}$, the system* (7) *is asymptotically stable for all delay $h > 0$.*

Proof: The asymptotic stability of the observer errors (7) is proved by studying each equation separately. First, it is shown in [17] that since $M = M_d < 0$, the stability of the origin of e_x is guaranteed independently of the delay h. This implies that the quantity $G(Me_x(t)+M_d e_x(t-h))$ is ultimately bounded. For the output error e_y, finite time stability conditions are established involving a Lyapunov function $V(t) = e_y(t)^T p_y e_y(t)$. Stability conditions in the theorem ensure that $\dot{V}(t) < -\beta\sqrt{V(t)}$ with $\beta > 0$ leading to the convergence of e_y in finite time. ■

When the convergence of the observation errors (7) is established, the anomaly $d(t)$ can be estimated from the output error. To bypass the chattering phenomenon problem, smoothing techniques (like filters) based on the principle of equivalent control [18] can be used to reconstruct the anomaly traffic. In other words, when sliding motion occurs on $e_y = 0$, one has $d(t) = Ge_x(t) + \nu_{eq}(t)$, where $\nu_{eq}(t)$ is the equivalent value on the sliding manifold of the discontinuous action $\nu(t)$, that can be obtained applying low pass filtering. A first order low pass filter combined with the first order sliding mode observer has been applied in simulation (see [19]) but is not efficient enough for chattering reduction. A third order for the low-pass filter was the lowest order able to reduce the chattering phenomenon without losing the real shapes of the anomalous traffics. However, filtering techniques lead to drawbacks like the intuitive regulation of the filter parameters as well as the delay in the anomaly reconstruction.

C. Super-twisting observer for detection purpose

For the detection purpose, a specific second order sliding mode algorithm called the super-twisting algorithm is considered. This algorithm is developed to avoid the chattering phenomenon

[20]. The continuous control law ϑ consists of two terms:

$$\begin{cases} \vartheta(s) &= \vartheta_1 - \lambda|s|^{\rho}\text{sign}(s), \\ \dot{\vartheta}_1 &= -\alpha\text{sign}(s), \end{cases} \tag{8}$$

where $\alpha > 0, \lambda > 0$, $0 < \rho \leq \frac{1}{2}$ and s is the sliding variable. Contrary to other second order sliding mode algorithms, the main advantage of the super-twisting algorithm is that it does not need the knowledge of the time derivative of the sliding variable. In this work, we fix $\rho = \frac{1}{2}$ which gives the faster convergence towards $s = \dot{s} = 0$ as shown in [20]. In order to apply this algorithm on the TCP model (2), the following observer is designed:

$$\begin{cases} \dot{\hat{x}}(t) &= M\hat{x}(t) + M_d\hat{x}(t-h) + Dy(t) + D_dy(t-h) + E_du(t-h), \\ \dot{\hat{y}}(t) &= G\hat{x}(t) + Hy(t) + z(t) - \lambda|\hat{y}(t) - y(t)|^{\frac{1}{2}}\text{sign}(\hat{y}(t) - y(t)), \\ \dot{z}(t) &= -\alpha\text{sign}(\hat{y}(t) - y(t)). \end{cases} \tag{9}$$

Define the observation errors as: $e_x(t) = \hat{x} - x(t)$, $e_y(t) = \hat{y} - y(t)$ and $e_z(t) = z + Ge_x - d(t)$, then using (4) and (9), the observation errors dynamics are given by:

$$\begin{cases} \dot{e}_x(t) &= Me_x(t) + M_de_x(t-h), \\ \dot{e}_y(t) &= Ge_x(t) + z(t) - \lambda|e_y(t)|^{\frac{1}{2}}\text{sign}(e_y(t)) - d(t) = e_z(t) - \lambda|e_y(t)|^{\frac{1}{2}}\text{sign}(e_y(t)), \\ \dot{e}_z(t) &= G(Me_x(t) + M_de_x(t-h)) - \dot{d}(t) - \alpha\text{sign}(e_y(t)). \end{cases} \tag{10}$$

The stability conditions for the sliding mode observer (9) are shown in the following theorem.

Theorem 2 *The origin of the system* (10) *is asymptotically stable if there exist a positive definite matrix* $P = \begin{pmatrix} p_1 & p_3 \\ p_3 & p_2 \end{pmatrix}$ *and* $W \in \mathbb{R}^{2\times 1}$ *such that the following two Linear Matrices Inequalities (LMIs) are verified:*

$$\frac{1}{2}E_{12}^TP + \frac{1}{2}PE_{12} - C^TW^T - WC \pm 2\Pi \begin{pmatrix} p_3 & \frac{1}{2}p_2 \\ \frac{1}{2}p_2 & 0 \end{pmatrix} < 0 \tag{11}$$

where $\Pi = sup_t\left(|G(Me_x(t) + M_de_x(t-h))|\right) + \dot{d}_{max}$, $C = [1 \quad 0]$, *and* $E_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. *The observer gain is obtained from* $L = \begin{bmatrix} \frac{\lambda}{2} & \alpha \end{bmatrix}^T = P^{-1}W$.

Proof: Similar to the case of the first sliding mode observer, asymptotic stability of e_x is guaranteed independently of the delay h. For the study of stability of e_y and e_z, let $\phi =$

$\left[|e_y|^{\frac{1}{2}}\text{sign}(e_y)\ e_z\right]^T$ be the new state vector. Finite time convergence of ϕ towards is verified using candidate Lyapunov function $V = \phi^T P \phi$, for a positive definite matrix P. Stability condition (11) leads to a positive definite matrix Q such that $\dot{V} = -|\phi_1|^{-1}\phi^T Q \phi$. This implies the convergence of e_y and e_z towards zero in finite time. Since $\lim_{t \longrightarrow \infty} e_x = 0$, an estimate of the anomaly $d(t)$ is obtained from $e_z = z + Ge_x - d(t) = 0$ without any filtering action. ■

IV. Simulations

The proposed observer (9) is tested via Simulink and the Network Simulator NS-2 [9]. In the network topology, 60 TCP sources are sending data to the destination through a router with a link capacity $C = 3750$ packets/s which is equivalent to 15 Mbits/s with a mean packet size of 500 bytes, and $T_p = 0.2$s the propagation delay.

The observer (OBS) is implemented on the router level as well as the AQM as shown in Figure 2.

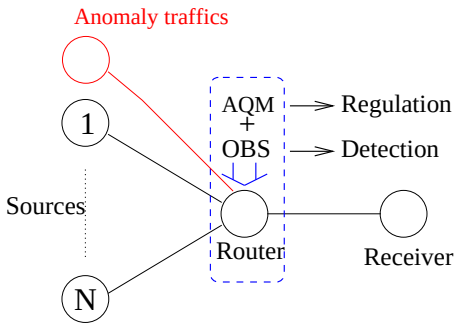
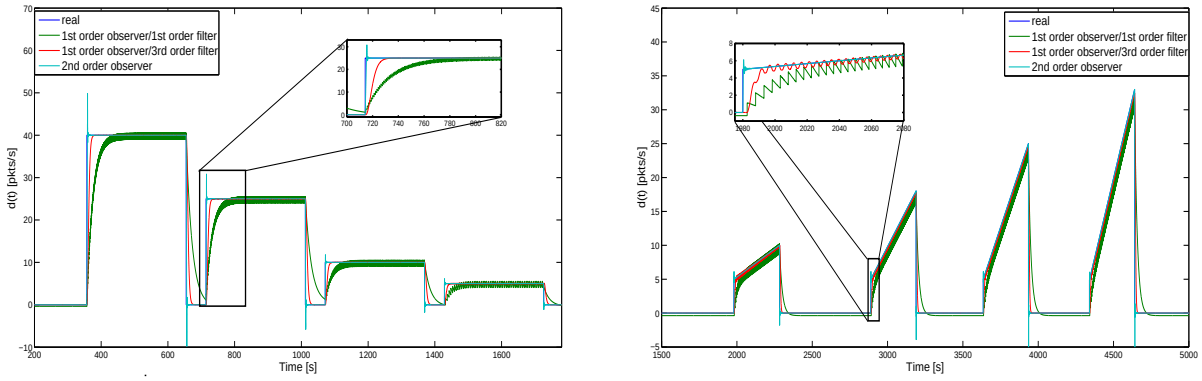


Fig. 2: Network configuration.

A. Simulink

Using Simulink, the linearized time-delay model of the TCP network (2) is considered. As the AQM, we have chosen the state feedback control Gain-K developed in [7] to regulate the queue length to 175 packets. Compared with the others AQM, Gain-K improves the performances of the router by reducing the oscillations around the equilibrium point q_{ref}, thus reducing the amount of dropped packets and improving the buffer utilization [7].

Periodic anomalies with rectangular and triangular shape series of different amplitudes are considered. The triangular shape of these anomalies is justified in [21] where experimentations were held on softwares generating anomalous traffic like the ”Tribal Flood Network version



(a) with rectangular shape.

(b) with triangular shape.

Fig. 3: First and second order sliding mode observers for anomaly reconstruction.

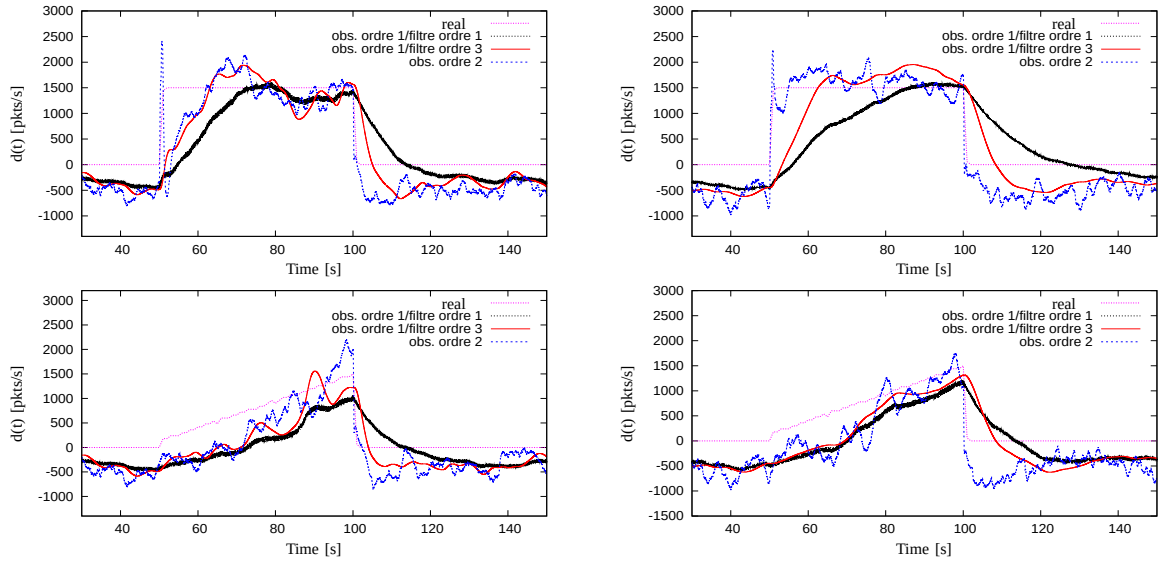
2000" (TFN2k) [22].

The first order sliding mode observer (5) exhibits undesirable chattering phenomenon that is not well reduced with first order low-pass filter as seen in Figure 3. The third order for the low-pass filter was the lowest order able to reduce the chattering phenomenon while detecting anomalies without losing their real shapes. From the comparative graphs presented in Figure 3, we can see that the third order filter reveals higher detection speed and smoother oscillations than the first order filter for the proposed anomaly shapes, thus inducing lower amount of false positives and false negatives. Whereas, the second order sliding mode observer detects instantaneously the anomaly with an ideal tracking of the real shape as seen in Figure 3. Therefore, the second order sliding observer improves the reactivity of the detectors in network security systems face to the anomaly.

B. Network Simulator NS-2

For the validation of the proposed methodology in NS-2, 60 TCP sources are generating long lived TCP flows (FTP connections) to a receiver through a congested router whereas anomalous traffic is generated by 3 sources attacking the router. Two anomaly shapes are introduced using the User Datagram Protocol (UDP) in NS-2 within the interval $50 - 100$s: a Constant Bit Rate (CBR) and a Triangular Bit Rate (TBR). The CBR generator is already implemented in NS-2, but for TBR, we have added a traffic generator in NS-2 code.

On the router level, the buffer size is set to 800 packets while different AQMs are implemented



(a) RED (b) Gain-K

Fig. 4: Anomaly estimation with different AQM: RED and state feedback Gain-K.

to regulate the queue length to the desired level $q_{ref} = 175$ packets. RED [23] is a well-known AQM used to randomize the packet drop by setting a marking probability with respect to the average queue length of the router buffer. We chose also the state feedback Gain-K [7] based on control theory.

The performances of each conveived observer are shown in Figure 4. In the following, a comparative study is conducted on two phases: the reconstruction phase, then the detection phase of the presence/absence of anomalies. During the reconstruction phase, the observation characteristics of CBR and TBR anomalies are determined: the convergence time, then the average errors between the estimated and the original, finally the standard deviations around these errors. For the anomaly detection, the duration of persistence of false positives and negatives are studied for the different observers associated with the AQM. We recall that after the appearance of the real anomaly, false negatives are emitted during the time interval where the estimated anomaly does not reach positive values. Respectively, after the disappearance of the anomaly, false positives persist as long as the estimated anomaly is positive.

1) Anomaly reconstruction: In Table I, the second order observer shows a faster convergence than the first order observers in the presence of CBR anomalies. However, the first order with

the first order filter shows the best tracking of the anomaly in terms of more reduced observation errors and standard deviations especially with the Gain-K. Indeed, in the presence of high frequency oscillations, first order filtering is slow but precise.

For TBR anomalies, we can see from Table II that the second order sliding mode observer allows

	convergence time [s]			average error [packets/s]			standard deviation [packets/s]		
	order 1 filter 1	order 1 filter 3	order 2	order 1 filter 1	order 1 filter 3	order 2	order 1 filter 1	order 1 filter 3	order 2
RED	33.9	32.1	23.3	-193	-250.4	-146.7	62.5	213.7	179.8
Gain-K	36.2	18.1	6.02	46.82	254.5	118.9	24.1	129.2	189.1

TABLE I: Observation characteristics for CBR anomalies.

a faster convergence as well as a better observation of the varying anomaly's rate than the first order sliding mode observer with the AQM studied. Otherwise, the lowest standard deviations are obtained with the first order observer with the first order low-pass filter. In conclusion, second order observers are able to identify more precisely the original amplitudes of the anomaly studied.

	convergence time [s]			average error [packets/s]			standard deviation [packets/s]		
	order 1 filter 1	order 1 filter 3	order 2	order 1 filter 1	order 1 filter 3	order 2	order 1 filter 1	order 1 filter 3	order 2
RED	12.2	14.1	11.3	-634.4	-414.4	-236.3	108.4	263.1	356.7
Gain-K	6.1	3.8	4.1	-482.9	-371.6	-346.3	131.2	179.8	324.8

TABLE II: Observation characteristics for TBR anomalies.

2) Anomaly detection: In Figure 4, we can see that during the absence of anomalie, the observers detect negative values. We considered -450 packets/s for the second order sliding mode and -350 packets/s for the first order as thresholds from which the durations of false negatives and positives are determined. In Table I and Table II, the second order observer allows reducing false negative and positive alarms more than the first order with the presence of filters. It should be noted that in the presence of the AQM RED, the persistence of the false negatives induced by the second order observer reaches 2.4s. This fact is due to the presence of oscillations

that delay the observation of an anomaly above the threshold.

	order 1 filter 1	order 1 filter 3	order 2
RED	0.39	0.83	2.4
Gain-K	1.5	1.3	0.05

(a) False negatives.

	order 1 filter 1	order 1 filter 3	order 2
RED	50.01	8.07	2.57
Gain-K	61.6	12.02	5.9

(b) False positives.

TABLE III: Persistence of false negative and positive alarms for CBR anomalies (in seconds).

	order 1 filter 1	order 1 filter 3	order 2
RED	3.21	1.6	0.36
Gain-K	5.84	4.88	1.12

(a) False negatives.

	order 1 filter 1	order 1 filter 3	order 2
RED	32.08	6.5	3.8
Gain-K	22.3	15.4	1.08

(b) False positives.

TABLE IV: Persistence of false negative and positive alarms for TBR anomalies (in seconds).

The efficacy of the second order sliding mode observer motivates towards testing its performance on a real TCP traffic. The best means consists of replaying a traffic trace captured from a real network by specific softwares. The advantage of this approach is to guarantee that all real traffic properties will be represented while testing the observer. The following section details the procedure required for flow replaying tools in NS-2.

V. REAL TCP TRAFFIC REPLAY

For experimental purposes, traffic traces are collected on the RENATER[1] network. In LAAS-CNRS[2], a generic polymorphic platform for network emulation and experiments called ”Laas-NetExp” [24] is set. From a specific machine, chosen to be the router in our network topology as in Figure 2, flowing packets are captured via the network analyser ”Wireshark” [25]. While capturing, anomalous packets have been sent from a machine in Mont-de-Marsan Institute of Technology (about 200 kilometers away from Toulouse). The software used for generating real attacks is TFN2k [22].

[1]RENATER is the French National Network for Education and Research.

[2]The Laboratory of Analysis and Architecture of Systems is a research unit associated with the University of Toulouse, France.

The Network Simulator NS-2 contains the necessary features to replay traces. In [26], an off-line analysis is defined to be applied on measured traces. These techniques allow extracting then categorizing flows into TCP, UDP and others, as well as determining non-trivial properties of every transmitted flow present in our adopted model (1): the packets sizes, average packets round trip time, packets loss rate and link capacities between the sources and the router.

The capture is analyzed and the properties of the data transmitted during the capture are determined. For the TCP trafic, 6 homogeneous flows were sent to their destinations through a chosen router. The methodology in [26] is adopted for extracting the average characteristics of the real TCP flows. The average TCP packet size is found to be equal to 1 KByte, and the average values for the link capacities and the RTT are determined for each flow. The anomalous traffic sent from Mont-de-Marsan consists of several short then long sequences with a constant bit rate equal to 100Kbits/s. Each of the short attacks lasts 7 seconds with 5 seconds between two consecutive ones and the long attacks last 4 minutes with intervals varying between 1 to 3 minutes between each couple of attacks.
The characteristics of the sources and of the router incoming links are defined for the simulation topology presented in Figure 2. During the capture, the router is configured to regulate the queue length using the mechanism of the Token Bucket Filter (TBF). TBF is a simple queueing discipline that only passes packets arriving at a rate which is not exceeding some administratively set rate [27]. Its implementation consists of a buffer (bucket), constantly filled by some virtual tokens, at a specific rate. Each arriving token collects one incoming data packet from the data queue and is then deleted from the bucket. The router capacity is set to be $C = 0.15$ Mbits/s.
To validate the proposed observer (9) on real traffic characteristics, the equilibrium point of the average network states is required. The values of the congestion window size and the queue length at the equilibrium are specified by the mean value around which $W(t)$ and $q(t)$ oscillate respectively before the beginning of the attacks ($W_0 = 5.8$ packets and $q_0 = 17.08$ packets).

The graphs in Figure 5 show the traffic captured on the router which includes TCP traffic. The anomaly is also present in the total traffic in such a way that a simple observation of the traffic flow cannot identify it. After extracting TCP flows from the total traffic with their average characteristics, the observer implemented on the router level can estimate the anomaly flowing

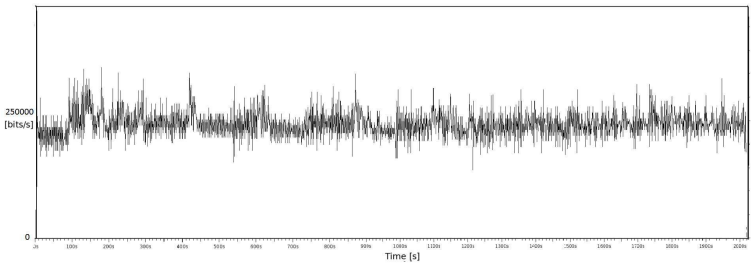
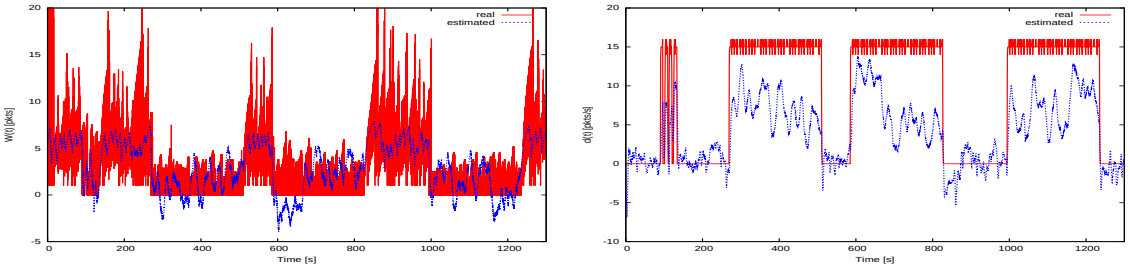


Fig. 5: Total traffic captured on the router level.



(a) TCP congestion window W(t)

(b) anomaly d(t)

Fig. 6: Estimation of traffic replay.

through its buffer. The second order sliding mode observer proposed is able to track the anomaly seen in Figure 6.On the other hand, in Figure 6a, before the beginning of the attacks, the window of congestion average $W(t)$ is correctly estimated, but in some time intervals during the long attacks the estimation does not follow the real evolution. We can explain these perturbations by experimental aspects coming up against the hypothesis of the TCP model (1).

- Because of the use of the Token Bucket Filter (TBF) based on the AQM ”Drop Tail” to regulate the router queue length, the sources are frequently forced to reduce their congestion windows towards zero. This phenomenon reflects the real performance of TBF but contradicts the fundamental hypothesis of the adopted TCP model which is the persistence of packets emission during the congestion avoidance phase.
- The average TCP packet size sent during the long attacks is different from the average size considered for the design of the observer. This real experimental fact perturbs the equilibrium value of the congestion window, thus defecting the anomaly reconstruction.

On the other hand, the instantaneous detection of the anomaly with good tracking of its real

profil represents the main advantage of the sliding mode control theory. This result reflects the relevance of the sliding mode observer (9) on real traffic conditions with respect to the hypothesis considered in the theoretical model.

VI. Conclusions and future work

In this article we have studied the performances of sliding mode observers for anomalies detection and reconstruction in TCP/IP networks. Based on Simulink and NS-2 simulation results, the second order sliding mode observer reveals better performances compared to the first order one, in terms of the instantaneous detection of the presence/vanishing of the anomaly and the fast tracking of the real anomaly profile. Furthermore, the advantages of the second order sliding mode observer are shown and validated on real experiments while estimating the congestion window size, then reconstructing the shape of the anomalous flows.

Our work has been focused on a new approach of monitoring TCP network. Future work is concerned with proposing a new architecture for helping TCP with guaranteeing the QoS of the router and the whole network topology subject to an anomaly.

References

[1] A. Lakhina, M. Crovella, and C. Diot, "Diagnosing network-wide traffic anomalies," in *Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communications*, ser. SIGCOMM '04, Portland, Oregon, USA, 2004, pp. 219–230.

[2] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys (CSUR)*, vol. 41, pp. 1–58, July 2009.

[3] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash crowds and denial of service attacks: characterization and implications for CDNs and web sites," in *Proceedings of the 11th international conference on World Wide Web*, ser. WWW '02, Honolulu, Hawaii, USA, 2002, pp. 293–304.

[4] C. Edwards, S. Spurgeon, and R. Patton, "Sliding mode observers for fault detection and isolation," *Automatica*, vol. 36, pp. 541–553, 2000.

[5] T. Floquet, J.-P. Barbot, W. Perruquetti, and M. Djemaï, "On the robust fault detection via a sliding mode disturbance observer," *International Journal of Control*, vol. 77, no. 7, pp. 622–629, 2004.

[6] 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 *Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, ser. SIGCOMM '00, Stockholm, Sweden, 2000, pp. 151–160.

[7] Y. Ariba, F. Gouaisbaut, and Y. Labit, "Feedback control for router management and TCP/IP network stability," *IEEE Transactions on Network and Service Management*, vol. 6, no. 4, pp. 255–266, December 2009.

[8] S. V. Emel'yanov, S. K. Korovin, and A. Levant, "High-order sliding modes in control systems," *Computational Mathematics and Modeling*, vol. 7, pp. 294–318, 2005.

[9] E. Altman and T. Jiménez, “Ns simulator for beginners,” Lecture notes, Dec. 2003, uRL: http://www-sop.inria.fr/maestro/personnel/Eitan.Altman/COURS-NS.

[10] R. Srikant, *The mathematics of internet congestion control*. Boston: Birkhäuser, 2004.

[11] S. Ryu, C. Rump, and C. Qiao, “Advances in active queue management (AQM) based TCP congestion control,” *Telecommunication Systems*, vol. 25, pp. 317–351, March 2004.

[12] C. Hollot, V. Misra, D. Towsley, and W. Gong, “Analysis and design of controllers for AQM routers supporting TCP flows,” *IEEE Transactions on Automatic Control*, vol. 47, pp. 945–959, June 2002.

[13] T. Floquet, C. Edwards, and S. Spurgeon, “On sliding mode observers for systems with unknown inputs,” *International Journal of Adaptive Control and Signal Processing*, vol. 21, no. 8-9, pp. 638–656, 2007.

[14] M. Defoort, F. Nollet, T. Floquet, and W. Perruquetti, “A third-order sliding-mode controller for a stepper motor,” *IEEE Transactions on Industrial Electronics*, vol. 56, no. 9, pp. 3337–3346, September 2009.

[15] S. Riachy, Y. Orlov, T. Floquet, R. Santiesteban, and J.-P. Richard, “Second order sliding mode control of underactuated Mechanical systems I: Local stabilization with application to an inverted pendulum,” *International Journal of Robust and Nonlinear Control*, vol. 18, no. 4-5, pp. 529–543, 2008.

[16] J.-J. Slotine, J. Hedrick, and E. Misawa, “On sliding observers for nonlinear systems,” in *American Control Conference (ACC)*, Seattle, WA, USA, June 1986, pp. 1794–1800.

[17] K. Gu, V. L. Kharitonov, and J. Chen, *Stability of Time-Delay Systems*. Birkhäuser Boston, 2003.

[18] V. Utkin, *Sliding Modes in Control and Optimization*. Berlin, Germany: Springer-Verlag, 1992.

[19] S. Rahmé, Y. Labit, and F. Gouaisbaut, “Sliding mode observer for anomaly detection in TCP/AQM networks,” in *Proceedings of the Second International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ)*. Colmar, France: IEEE Computer Society, 2009, pp. 113–118.

[20] A. Levant, “Sliding order and sliding accuracy in sliding mode control,” *International Journal of Control*, vol. 58, no. 6, pp. 1247–1263, 1993.

[21] Y. Labit and J. Mazel, “Hidden: Hausdorff distance based intrusion detection approach dedicated to networks,” in *Proceedings of the 2008 the third International Conference on Internet Monitoring and Protection (ICIMP)*, Bucharest, Romania, July 2008, pp. 11–16.

[22] J. Barlow and W. Thrower, “TFN2K - An analysis,” AXENT Security Team, March 2000, uRL:http://www.packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt.

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

[24] P. Owezarski, P. Berthou, Y. Labit, and D. Gauchard, “LaasNetExp: a generic polymorphic platform for network emulation and experiments,” in *Proceedings of the 4th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities (TRIDENTCOM)*, Innsbruck, Austria, 2008, pp. 1–9.

[25] A. Orebaugh, G. Ramirez, J. Burke, L. Pesce, J. Wright, and G. Morris, *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Rockland, MA, USA: Syngress Publishing, 2007.

[26] P. Owezarski and N. Larrieu, “A trace based method for realistic simulation,” in *IEEE International Conference on Communications*, vol. 4, Paris, France, June 2004, pp. 2236–2239.

[27] D. Clark, S. Shenker, and L. Zhang, “Supporting real-time applications in an integrated services packet network: architecture and mechanism,” in *Proceedings of the conference on Communications architectures & protocols*, ser. SIGCOMM ’92, Baltimore, Maryland, USA, 1992, pp. 14–26.