Network intrusion detection system for drone fleet using both spectral analysis and robust controller / observer

Ruohao Zhang, Jean-Philippe Condomines, Riad Chemali, Nicolas Larrieu

RAPPORT DE RECHERCHE

aout 2018

RR-ENAC-2018-01

Network intrusion detection system for drone fleet using both spectral analysis and robust controller / observer

N°2018-01

ENAC

La référence aéronautique

www.enac.fr

Ruohao Zhang, Jean-Philippe Condomines, Nicolas Larrieu, Riad Chemali
SINA Department, ENAC, Université de Toulouse, BP 54005, Toulouse Cedex 4, 31055, France Email: firstname.surname at enac.fr

Resume
This paper proposes an hybrid method based on both a spectral traffic analysis and a robust controller / observer for anomaly estimation inside UAV networks. This method is based on both Lyapunov Krasovskii functional and dynamic behavior of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). The proposed hybrid method considers, as a preliminary step, a statistical signature of the traffic exchanged in the network. By looking up this signature in a bank of signatures, it is possible to characterize the different anomalies that can be observed in UAV networks. Consequently, the different signatures that we can process, based on the different types of intrusion we generate in the network, are used to select the accurate model for robust control estimation. This selection is conducted by choosing a specific controller / observer among a dedicatedbankofmodels.Thefirststatisticalsignatureextraction of the analyzed tr

Network intrusion detection system for drone fleet using both spectral analysis and robust controller / observer

Ruohao Zhang, Jean-Philippe Condomines, Nicolas Larrieu, Riad Chemali
SINA Department, ENAC, University of Toulouse, BP 54005, Toulouse Cedex 4, 31055, France
Email: firstname.surname at enac.fr

***Abstract*—This paper proposes an hybrid method based on both a spectral traffic analysis and a robust controller / observer for anomaly estimation inside UAV networks. This method is based on both Lyapunov Krasovskii functional and dynamic behavior of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). The proposed hybrid method considers, as a preliminary step, a statistical signature of the traffic exchanged in the network. By looking up this signature in a bank of signatures, it is possible to characterize the different anomalies that can be observed in UAV networks. Consequently, the different signatures that we can process, based on the different types of intrusion we generate in the network, are used to select the accurate model for robust control estimation. This selection is conducted by choosing a specific controller / observer among a dedicated bank of models. The first statistical signature extraction of the analyzed traffic is done with a multi-fractal analysis. This solution based on wavelet analysis has been selected because it offers a wide spectral characterization of the entire traffic process. The wavelet-based analysis methodology has been widely used for the last decade for Internet traffic characterization but this is the first time that this tool has been used on a UAV ad hoc network traffic. Moreover, several research studies on network anomaly estimation have been carried out using automatic control techniques. These studies provide methods for designing both observer and command laws dedicated to time delay problems while estimating the anomaly or intrusion in the system. As a first result, the spectral analysis tool has provided clearly distinguishable signatures between the traffics with and without anomalies. Then, the designed controller / observer system has been successfully applied to some relevant practical problems such as ad hoc networks for aerial vehicles and its effectiveness is illustrated by using real traffic traces including Distributed Denial of Service (DDoS) attacks. Our first results show promising perspectives for Intrusion Detection System (IDS) in a fleet of UAVs. Indeed, different types of anomaly have been considered and they are all accurately detected by the intrusion detection process we propose in this paper.**

***Index Terms*—UAV, Intrusion Detection System, Robust Estimator, Spectral Analysis, Drone Ad Hoc Network**

I. Introduction

The number and diversity of applications involving Unmanned Aerial Vehicles (UAVs) are growing every year. The need to use a fleet of versatile UAVs has led to an increased interest from the network community to design algorithms for Anomaly Detection Systems (ADS) or Intrusion Detection Systems (IDS) based on TCP network. Among abnormal patterns in TCP networks [1]–[3] such as overload, flash crowds, worms, port scans, flash crowds have the worst impact on the fleet of UAVs because they create congestion and reduce significantly the Quality of Service (QoS) of the entire network. This is the worst-case scenario for UAV certification and integration into civil airspace. Consequently, malicious anomaly detection is an important issue nowadays. In [3] an overview is provided reviewing multiple research areas and application domains.

Network anomalies and security-related problems (such as Distributed Denial of Service (DDoS) attacks) are important issues for the detection of active security threats. A variety of tools for anomaly detection are principally based on data packet signature. This behavior is known to be very effective against well-known DDoS attacks. However, this mechanism is inefficient when a new type of attack is performed. For this reason, we outline in this paper a new type of IDS able to detect different types of DDoS. The proposed IDS is a two-step process (see Figure 1 for details). The first step is dedicated to traffic characterization. Its objective is to get a specific signature of the traffic we want to analyze. These different signatures are used to automatically select the different controller / observer models used in the second step of the intrusion detection process. This approach has the major advantage that it is not associated with a specific type of attack. Any attacks which do not follow the initial model can be analyzed, detected and managed. Consequently, the security and performances of the entire network can be improved.

This traffic estimation is performed thanks to a statistical signature of the traffic exchanged in the network. This signature provides us an unique identification of the current traffic. By looking up this signature in a bank of signatures, it is possible to characterize the different anomalies that can be observed in UAV networks. Consequently, the different signatures that we can process, based on the different types of intrusion we generate in the network, are used to select the accurate model for robust control estimation. This selection is performed by choosing a specific controller / observer among a dedicated bank of models. The first statistical signature extraction of the analyzed traffic is done with a multi-fractal analysis. This solution, based on wavelet analysis, has been selected because it offers a wide spectral characterization of the entire traffic process. Moreover, this analysis methodology has been widely used for the last decade for Internet traffic characterization but this is the first time that this tool has been

used on a UAV ad hoc network traffic.

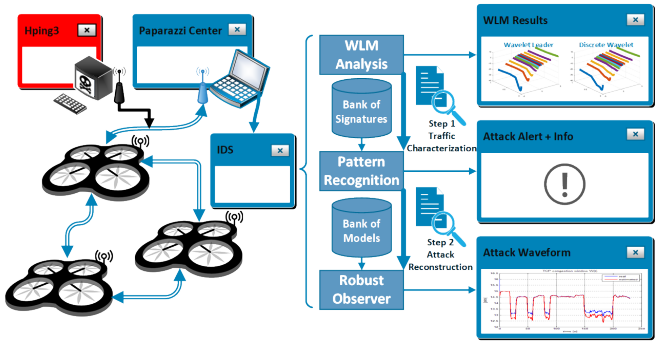

Fig. 1. General framework of the proposed IDS system

The contribution of this paper is to propose a new hybrid method which is able to detect traffic anomalies (i.e. DDoS). This algorithm has been designed and tested in real traffic conditions. Indeed, the Simulink design of our new IDS process and its theoretical evaluation have been faced with real traffic traces. These traces have been generated using a hybrid UAV network simulator. Consequently, the validation of the theoretical estimator is improved by testing its performances faced with real DDoS attacks, real UAV trajectories, real UAV background traffic, and real UAV fleet topology. Guided by the Lyapunov theory, we propose a new design to define all correction terms associated with time delay linear state-space representation of TCP model. Initial results for Intrusion Detection System (IDS) in a fleet of UAVs are promising. Indeed, different types of anomaly have been considered and they are all accurately detected by the intrusion detection process we propose in this paper.

In the sequel, Section 2 presents the theoretical background of our proposed controller / observer system and the state of the art of characterization tools described in the literature to extract network traffic signatures. Section 3 presents the basics of the characterization and the modeling adopted to tackle the time delay linear estimation problem of determining the state vector components of a fluid-flow model fitted out with a TCP model. Section 3 also introduces the principles of our IDS methodology which combines spectral analysis and traffic reconstruction. Finally, Section 4 gathers all the results from the validation tests performed on both steps.

II. Related Work

The intrusion detection methodology proposed in this paper is the result of a collaboration between two scientific areas. The first one is related to traffic characterization. It uses spectral analysis in order to generate a specific traffic signature depending on the type of attacks we want to detect. The second is related to automatic control methods applied for traffic reconstruction. It uses robust controller / observer methods to analyze the traffic and rebuild its characteristics and behavior.

In the next subsections, we will summarize the latest research for these two specific scientific fields.

A. Spectral analysis for traffic characterization

Several research studies have been conducted for traffic characterization using spectral analysis. One of the most consistent is [4]. The authors have demonstrated how Long Range Dependence (LRD) can be an efficient parameter to quantify the level of variability of Internet traffic. They have developed a specific method (including a Matlab toolbox) to process data traffic. This process uses wavelet analysis (see [5] for details) which is an efficient tool to obtain the variability level of any data series for different time scales and different moments of analysis. In this paper, we will use an enhanced version of the method introduced in [5] developed by H. Wendt more recently called Wavelet Leader Multi-fractal (WLM) analysis (see [6]–[9] for details).

B. Robust controller / observer for traffic reconstruction

Exploiting the capabilities of observers or estimators allows us, by generating consolidated signals, to extend the way malicious intrusion can be controlled while enhancing the intrinsic flight handling qualities of a fleet of UAVs. Among the non-linear methods [10] described in the literature, the Super-Twisting Algorithm (STA) [11]–[13] is the most widely used for chattering avoidance while detecting anomalies. Its principles rely firstly on the non-linear fluid model applied on TCP dynamics and secondly on sliding modes [14] which are often used to design robust non-linear observers or control laws. Unfortunately, building upon this peculiar observer provides for bounded input-bounded state (BIBS), finite-time stability only [15]. Consequently, this statement restricts the application of this observer to the class of the systems for which the upper bound of the initial condition might be estimated in advance. Such an approach can be very non-systematic for complex dynamic systems such as the TCP model for a fleet of UAVs.

Another relevant method proposed in the literature is based on time delay linear state estimation. Such an approach [16] draws on both Lyapunov Krasovskii functional and dynamic behavior of TCP/AQM (Transmission Control protocol/ Active Queue Management) to use a Luenberger observer to cope with anomaly detection. An Active Queue Management consists of adjusting data flow rates sent by the UAV through the network. The principle consists of dropping (or marking when the ECN (Explicit Congestion Notification) [17] option is enabled) some packets before the buffer saturates. Consequently, the estimator must be associated with a robust AQM in order to perform its diagnosis. The study of congestion control in a time delay system framework is not new and has been successfully demonstrated in [18]–[21]. A relevant constructive algorithm [22] has been proposed.

III. Intrusion Detection Methodology

Our methodology introduced in this section is a two-step process (as shown in Figure 1). The first step is dedicated to traffic characterization. Its objective is to get a specific signature of the traffic we want to analyze. We will see in Section IV that we are able to obtain two completely

different attack signatures according to Wavelet Leader Multifractal analysis (WLM). These different signatures are used to automatically select the different controller / observer models used in the second step of the intrusion detection process.

A. Step 1: spectral analysis-based traffic characterization

The WLM analysis is used to quantify the variability of any time series (in this paper we focus on network traffic) we want to characterize. This method has the advantage of capturing the complexity of traffic for different time scales and different moments of analysis. This process produces a graphical result (called a spectral signature) which is used to find the difference between legitimate traffic and traffic which contains an attack.

Based on the WLM methodology we can quantify the variability of any time series according to two complementary parameters: the time scale and the moment of analysis. *Time scale* allows us to see any repetition in the process over time. *Moment of analysis* allows us to analyze traffic data in different spectral representations. This second metric quantifies the variation of the traffic according to, for instance, $q = 1$ (average), $q = 2$ (variance) and so on.

An example of spectral signature for regular traffic (i.e. not containing any attacks) is shown in Figure 2. This figure represents the spectral characteristics of the data according to the time scale of analysis (i.e. the *granularity* parameter) and the moment of observation. We will illustrate in section IV how this signature can be different according to the type of attack we wish to analyze and detect. There is an initial theoretical assumption to verify each time you want to use the WLM method on any specific time series. Indeed, any data series needs to verify scale invariance in order to justify the self-similarity feature. Computer network traffic naturally exhibits scale invariance property throughout different time scales as demonstrated in [23].

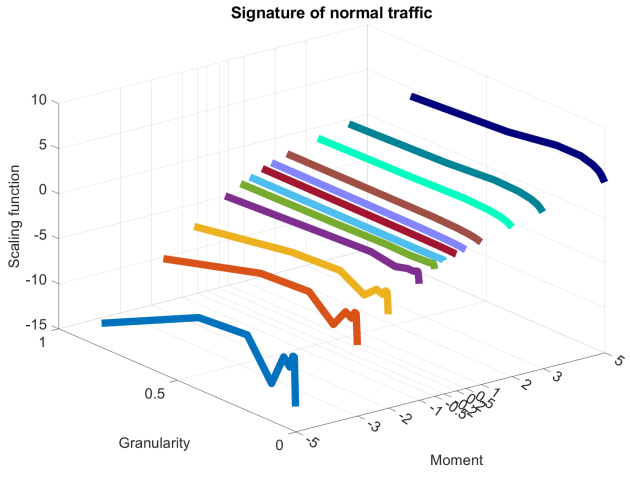

Fig. 2. Example of spectral signature using WLM method

These differences can be easily quantified and analyzed with analytic methods such as curve similarity score (an example of edge matching algorithm is given in Section IV). Furthermore, by comparing the observed signature with a bank of signatures of known traffics, we will then be able to automatically select the different controller / observer models used in the second step of the intrusion detection process. This is the topic of the next subsection where we will describe the automatic control modeling we have performed based on an controller / observer robust estimation.

B. Step 2: controller / observer-based robust estimation

In order to tackle a wide range of applications, various implementations of TCP models in terms of assumptions and numerical techniques [24]–[26] exist. TCP network is commonly represented using a linearized fluid-flow model [24] associated with our network topology. In this paper, the topology consists of N TCP sources, with the same propagation delay connected to a destination node through a router.

This simple topology is due to :

1) The high complexity behavior of a fleet of UAVs in which each UAV can be sender, receiver and router;
2) The difficulty for such systems to derive a reliable and representative network modeling from scratch.

The bottleneck link is shared by N flows and TCP applies the congestion avoidance algorithm described in [27]. To implement an Intrusion Detection System (IDS) according to the network topology presented previously, it is necessary to use, if possible, additional instruments (e.g. probability of packet, queue of the router buffer) and linear / non-linear estimation algorithms. The estimation algorithm makes use of the queue at the router buffer which delivers a scalar q. Assuming a continuous flow, the behavior of our topology network can be represented mathematically as follows:

$$\mathscr{M}_s \begin{cases} \dot{W}(t) = \frac{1}{\tau(t)} - \frac{W(t)W(t-\tau(t))}{2\tau(t-\tau(t))} p(t-\tau(t)) & \\ \dot{q}(t) = \frac{W(t)}{\tau(t)} N - C + d(t) & (process) \\ y(t) = q(t) & (measurement) \end{cases} \quad (1)$$

In the first differential equation, $W(t)$ represents the TCP window size, $\tau(t)$ the round trip time (RTT) which can be modeled using parameters associated to the network configuration C, T_p as $\tau = q/C + T_p$. The latter quantity C represents the transmission capacity of the router, T_p the propagation delay and N the number of TCP sessions. The variable $p(t)$ is the marking / dropping probability of a packet and can be seen as known measured input. This quantity relies on the explicit congestion notification to regulate the queue size of the router buffer. In the second differential equation, $q(t)$ is the queue length of the router. The malicious anomalies are modeled by an additional signal $d(t)$ mixed with the regular traffic passing through the router and filling the buffer.

The non-linear state space representation corresponding to $\mathscr{M}_s$ can be described in a compact form such as: $\dot{\underline{x}} = f(\underline{x}, u, d)$ and $y = h(\underline{x}, u)$ where: $\underline{x} = [W^T, q^T]^T, u = p$ and $y = q$ are the state, input and output vectors respectively. Moreover, a linearization of $\mathscr{M}_s$ was carried out in [29] to allow the use

of traditional control theory approaches. The fluid-flow model of TCP now becomes :

$$\delta\mathscr{M}_s \begin{cases} \delta\dot{W}(t) &= -\frac{N}{\tau_0^2 C}(\delta W(t)+\delta W(t-\tau(t))) \\ &\quad -\frac{1}{\tau_0^2 C}(\delta q(t)-\delta q(t-\tau(t))) \\ &\quad -\frac{\tau_0 C^2}{2N^2}\delta p(t-\tau(t)) \\ \delta\dot{q}(t) &= \frac{N}{\tau_0}\delta W(t)-\frac{1}{\tau_0}\delta q(t)+d(t) \end{cases} \tag{2}$$

where $\delta W = W - W_0$, $\delta q = q - q_0$, $\delta p = p - p_0$ are the perturbed variables around the operating point defined by:

$$\begin{cases} d(t) = 0 \\ \dot{W}(t) = 0 \Rightarrow W_0^2 p_0 = 2 \\ \dot{q}(t) = 0 \Rightarrow \begin{cases} W_0 = \frac{\tau_0 C}{N} \\ \tau_0 = \frac{q_0}{C} + T_p \end{cases} \end{cases} \tag{3}$$

Inspired by the theory of time delay systems [16], the dynamics of the queue and the congestion window are modeled to address delay issues. Indeed time delay is an intrinsic phenomenon in networks whose control should improve the precision of $\delta\mathscr{M}_s$. The idea is to exploit the linearized TCP fluid-model within a time delay framework as follows where $\delta\underline{x}(t) = [\delta W(t)\ \delta q(t)]^T$ is the state vector and $\delta u(t) = \delta p(t)$ the input:

$$\delta\mathscr{M}_s \begin{cases} \delta\dot{\underline{x}}(t) &= \mathbf{A}\delta\underline{x}(t)+\mathbf{A}_d\delta\underline{x}(t-\tau(t)) \\ &\quad +\mathbf{B}\delta u(t-\tau(t))+\mathbf{B}_d d(t) \\ y(t) &= \begin{bmatrix} 0 & 1 \end{bmatrix}\delta\underline{x}(t) \end{cases} \tag{4}$$

with

$$\begin{cases} \mathbf{A} = \begin{bmatrix} -\frac{N}{\tau_0^2 C} & \frac{1}{\tau_0^2 C} \\ \frac{N}{\tau_0} & -\frac{1}{\tau_0} \end{bmatrix} \\ \mathbf{A}_d = \begin{bmatrix} -\frac{N}{\tau_0^2 C} & -\frac{1}{\tau_0^2 C} \\ 0 & 0 \end{bmatrix} \end{cases} \tag{5}$$

and

$$\begin{cases} \mathbf{B} = \begin{bmatrix} -\frac{C^2\tau_0}{2N^2} \\ 0 \end{bmatrix} \\ \mathbf{B}_d = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{cases} \tag{6}$$

Based on such a linearized model, formulated in the general form of a time delay system, it is possible to design both AQM and estimator by using the Lyapunov Krasovskii method [28] which is an extension of the traditional Lyapunov theory.

Various AQM mechanisms exist in the literature such as Random Early Detection [30] (RED), Random Early Marking [31] (REM) and more recently using control theory (proportional and proportional integral controller [32] or state feedback controller [33]). As shown in Figure 3 the control law stabilizes the TCP network (queue lengths and rates) to a desired equilibrium (W_0, τ_0, q_0) in spite of the presence of some non-responsive traffics, ensuring then a certain level of quality of service (QoS). A major issue in the certifying of a fleet of UAVs is to estimate the malicious intrusion while taking into account a level of QoS (i.e., the drop probability $p(t)$). This is why the non-modeled malicious traffic $d(t)$ needs to be estimated. The estimator has to be designed in addition to an efficient AQM. Thus, in [36] we proposed a robust controller / observer for IDS by solving an LMI criteria.

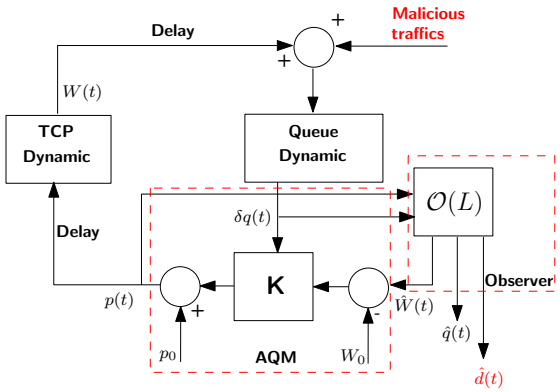

Fig. 3. IDS design

IV. Intrusion Detection System Validation

A. UAV ad hoc network hybrid platform

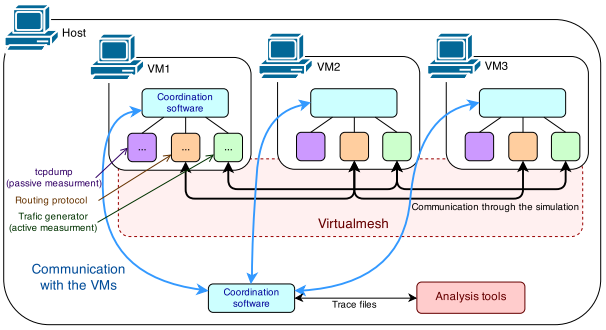

Fig. 4. Testbed implementation

In order to validate our new traffic estimator in real traffic conditions, we use a hybrid experimental system to take advantage of the low cost of a simulation while still obtaining the accuracy of a real protocol stack. We have been using virtual machine implementations to deal with the entire complexity of the Linux operating system. The traces used to generate UAV mobility patterns were extracted from real traces so that physical related factors could be as realistic as possible. The system we have been using to evaluate protocols is divided into several parts. It includes a set of tools that can deal with several scenarios: a hypervisor to run the virtual machines, measurement tools and a framework to allow virtual machines to communicate through a virtual wireless medium. We chose to use VirtualBox as a virtualisation tool because it is an easy-to-use and efficient hypervisor. The virtualized system is a 12.04 version Ubuntu, working with the 2.6.38 version of the Linux kernel. Our testbed architecture uses a Virtualmesh framework. It is a framework that interfaces a Linux-based system with an OMNeT++ simulation. OMNeT++ is a powerful network simulator which simulates several systems and normalized protocols. An illustration of this system is shown

in Figure 4. In [34], more details about this hybrid tool can be found.

The main advantage of using such a hybrid simulator is to extract any characteristics from the simulation and to inject them into the Simulink design directly. The theoretical model is then used under real traffic conditions and not only theoretical stimulus. The advantage of such an evaluation is to take into account the huge variability and complexity of real traffic. Consequently, we have been able to generate DDoS between the different virtual machines by taking into account the exact UAV environment of the drone mission we have considered in this research. First, we captured the network traffic generated (both regular traffic and the DDoS traffic) and then, we injected this traffic into the Simulink design.

B. Traffic characterization results for intrusion detection system calibration

The objective of this analysis is to create a bank of signature, in order to extract a specific pattern for each type of intrusion and to analyze the differences between normal traffic without anomaly and traffic with anomaly. In order to obtain traffic signature in three dimensions (3D), we measured the scaling function with respect to the statistic moments (q), which can take positive or negative values, and also with respect to the granularity of the traffic. We now illustrate the results obtained by our multi-fractal analysis (WLM) method on the basis of the hybrid UAV network simulator. As we stated previously, the normal TCP traffic is generated by 5 TCP sources generating long-life TCP flows to a receiver through a router with a link capacity $C = 1250$ packets/s (which is equivalent to 3 Mbit/s), and $T_p = 30ms$ the propagation delay. We will analyze the traffic in the face of different DDoS (Distributed Denial of Service) attacks. Two types of DDoS attacks are considered: a Constant Flash-Crowd (CFC) and a Progressive Flash-Crowd (PFC) attack. These anomalies have been generated using the HPing3 tool. This software is run on the hacker node (see Figure 5 for details about the network topology which has been considered) and can run different types of attack but mainly flooding attacks for our experiments. Indeed, in our scenario, HPing3 exchanges thousands of small TCP flows in order to generate a SYN flood attack on the receiver node. The resulting malicious traffic is much more significant than the regular traffic. Figure 6 shows the features of the traffic which has been generated through the hybrid network simulation tool. This traffic includes 4 different CFCs of the same magnitude but with different durations and, consequently, different impacts for the UAV network.

1) Attack signature for traffic with Constant Flash-Crowd CFC: We consider in this section, the CFC attacks which have been generated. The objective is to obtain a dedicated spectral analysis for this specific type of DDoS attack. This spectral analysis (based on scaling function characterization) provides a specific attack signature for each type of network traffic. Consequently, in Figures 7 and 8, a comparison of the signatures of the regular traffic and traffic including CFC attacks is illustrated. The obtained results show a large

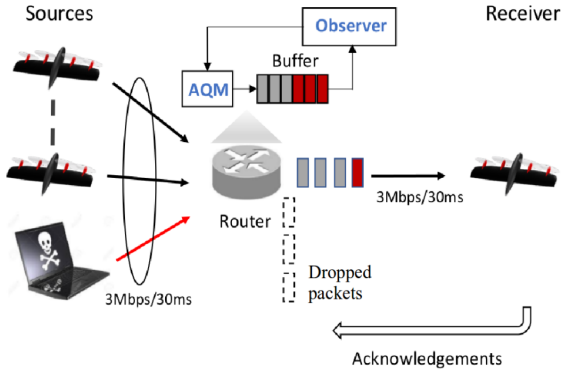

Fig. 5. Considered topology

variation in the scaling function $\zeta(q)$, especially in the case of negative moments for traffic including attacks. We observe that the scaling function (for the negative moment $q = -5$) reaches values $\zeta(q) \leq -19$ for traffic including DDoS attacks while it does not exceed the value of $\zeta(q) \leq -13$ for normal traffic.

2) Attack signature for traffic with Progressive Flash-Crowd PFC: In a second time, the network is exposed to PFC attacks (see Figure 9 for details about the traffic profile of this DDoS). The comparison between traffic with and without attack shows that the variation of the scaling function $\zeta(q)$ is always visually noteworthy in negative statistic moments (here $q = -5$). Indeed, we can see in Figure 10 the value of the scale function is between $\zeta(q) \geq -17$ and $\zeta(q) \leq 6$ for regular traffic. On the contrary, in the case of traffic including PFC attack, the values $\zeta(q)$ are between $-19 \leq \zeta(q) \leq 5$ (see Figure 11 for details).

3) Discussion on traffic signature characterization: These characterization results show that it is possible to extract dedicated signature for traffic with and without anomalies. Moreover, the spectral analysis provides different signatures for each type of DDoS. Indeed, the scaling function is not the same for DDoS CFC and PFC. Consequently, we can build a selector according to each specific spectral signature which will be able to select automatically a specific controller / observer for the IDS tool. However, this automation process is not completely performed at this time by our intrusion detection system algorithm. Indeed, these two steps (characterization and anomaly reconstruction) are performed separately. It is worth noting that the whole process is considered as a work-in-progress task. However, in the next section, we present some preliminary results for WLM signature comparison. We used a edge matching algorithm to be able to quantitatively find a difference between two different signatures generated with and without DDoS attacks.

C. WLM signature comparison results

Before the acquisition of the aforementioned bank of signatures, it is important to tune the WLM method's variables including moments and time scale to obtain the optimum sensitivity. One way to quantify the sensitivity is to measure

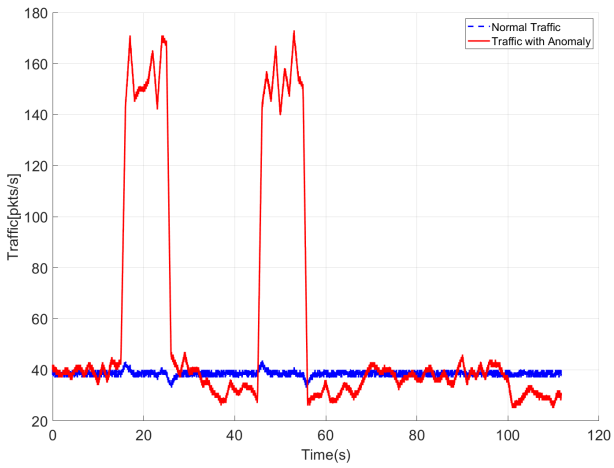

Fig. 6. Real UAV traffic profile with DDoS attacks (CFC)

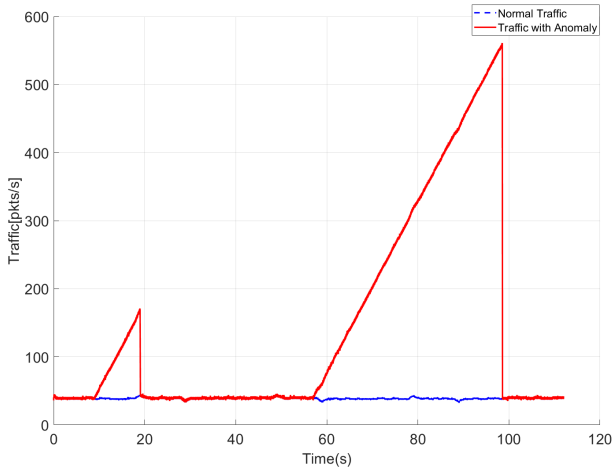

Fig. 9. Real UAV traffic profile with DDoS attacks (PFC)

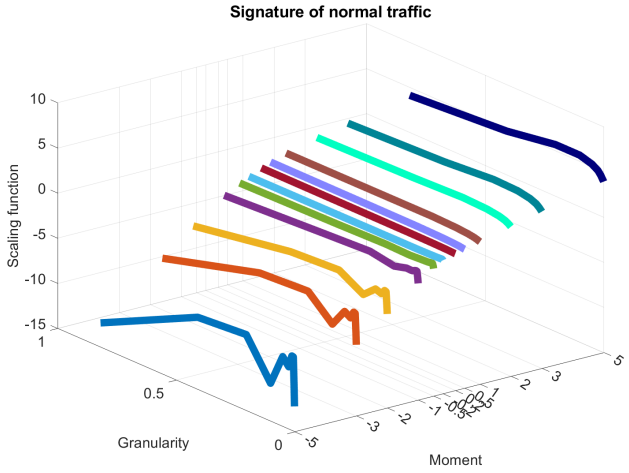

Fig. 7. Scaling function for regular traffic

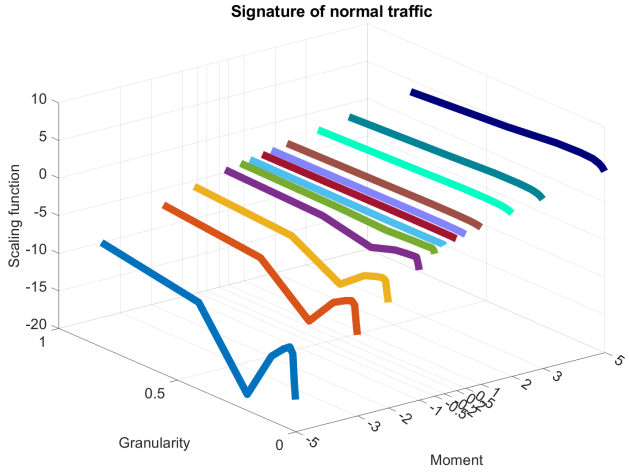

Fig. 10. Scaling function for regular traffic

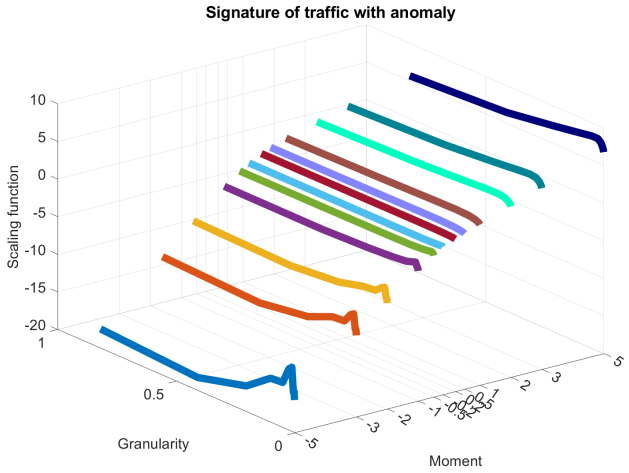

Fig. 8. Scaling function for traffic with CFC anomaly

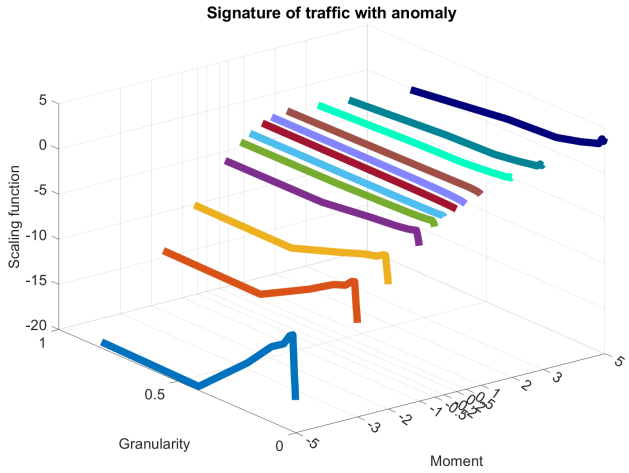

Fig. 11. Scaling function for traffic with PFC anomaly

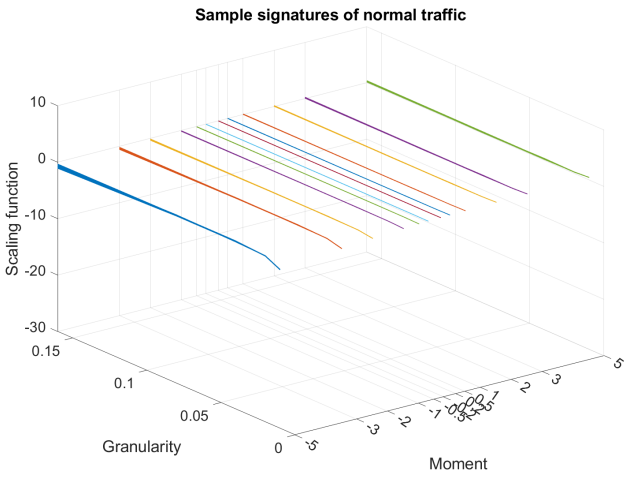

Fig. 12. Scaling function for regular traffic

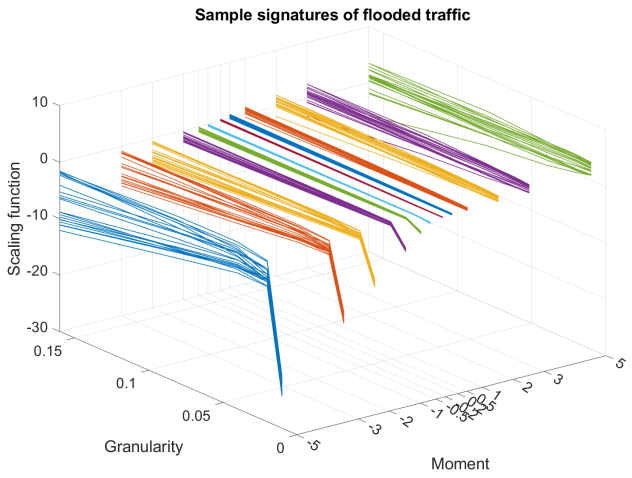

Fig. 13. Scaling function for traffic with CFC anomaly

how much difference there is between signatures with and without different attacks. In order to compare signatures one by one, we need to use a reliable and performant algorithm for solving equivalence problems. Among fundamental methods, three-dimensional edge matching method introduced in [35] appears to be the most suitable signal processing methodology for classifying 3D curves.

This method, which was designed to help solving 3D Jigsaw Puzzle problems, allows to compare two curves in a three dimensional space and returns a value normalized between 0 and 1 called "similarity score". Let $\mathscr{C}$ and $\bar{\mathscr{C}}$ two discretized curves. A "similarity score" is defined as $p(\mathscr{C},\bar{\mathscr{C}}) \in [0,1]$, such that if $\mathscr{C}$ and $\bar{\mathscr{C}}$ are congruent then $p = 0$, and the closer p gets to 1 the more $\mathscr{C}$ and $\bar{\mathscr{C}}$ are different. In our case of having multiple signature curves at different moments of analysis, we simply connect the curves end-to-end and consider it as one three-dimensional curve and perform the similarity score calculation. This method has been tested and validated with signatures acquired from our UAV ad hoc network hybrid platform generating communications from one drone to one host PC acting as Ground Control Station (GCS). This experimental scenario was a two-step process. In the first step, we generated only regular drone-to-GCS traffic, and in the second step, we generated regular drone-to-GCS traffic plus CFC flooding attack to GCS.

We took some samples of the resulted signatures during the test and plot them all together as shown in Figure 12 and 13. As noticed in the previous section, it can be observed that the signatures are visually very different when the GCS is attacked by CFC flooding attacks. With this specific CFC flooding attack only on the GCS the shape of the signature is also modified compared to the original CFC flooding attack (see Figure 9 for details). As shown in Figure 14, the curve similarity score has clearly distinguished the differences in the signatures when each of the 6 attacks happened during our test.

Although it can be observed in Figure 14, that during the 3rd, 4th and 5th attack, the similarity score experienced two peaks and form a valley shape waveform during the attack as if there are two attacks. This is caused by prolonged attacks which saturated the reception buffer of this experimental IDS design. In this case, because the buffer is saturated, the IDS does not see any difference in the incoming traffic and therefore resulted in signature which resembles a normal traffic with only small variations that are not significant in terms similarity score analysis.

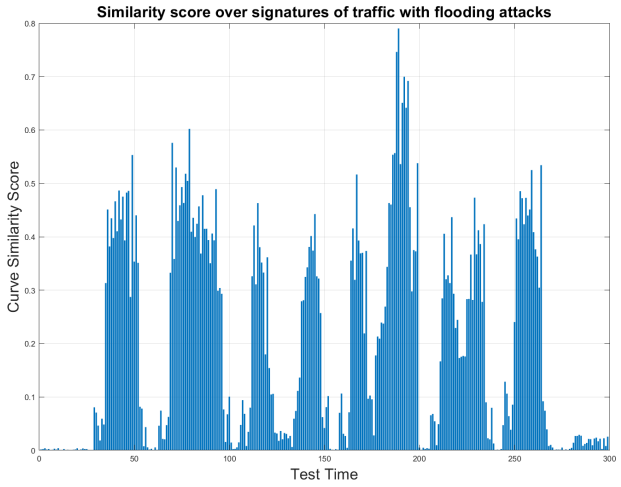

Fig. 14. Similarity score over signatures of drone to GCS traffic with 6 CFC attacks (attack No.3 4 5 saturate the reception buffer)

Therefore we have successfully demonstrated that how the first step of our newly purposed IDS can distinguish network traffic with and without CFC flooding, and how the variation of some parameters such as the test duration, which translates into the size of reception buffer, will influence the performance of this implementation. With an addition of an analytical method such as the curve similarity score method mention

W_0	15 packets
q_0	37.5 packets/s
p_0	0.0089
R_0	0.06 s

TABLE I
EQUILIBRIUM POINT

in this section, it is possible to achieve an automatic detection of anomalies. But the curve similarity score method has work exceptionally well in our test case, which has led us to think we can actually implement a similar mechanism in our IDS. Because an actual pattern recognition algorithm is expensive in terms of computation power, it is less efficient to perform such calculation on all signatures we obtained in a drone network. Consequently, a simple and algorithmic efficient curve matching method can be implemented on individual nodes in a distributed drone network, and it can act as an alarm and a trigger to the command center/ground station to notify the operators about the anomalies. Then, decisions can be made on, whether or not, to further investigate the anomalies with more powerful tools such as pattern recognition and anomaly reconstruction.

In the next section, we are going to present additional results related to the second step of this process: anomaly reconstruction and detection using robust controller / observer.

D. Anomaly reconstruction results

We now illustrate the performances reached by the developed controller / observer on the basis of our hybrid UAV network simulator. To conduct such a task, we define in Table I the values of the congestion window size and the router queue length at the equilibrium point of the system: W_0 and q_0. They have been selected by considering the mean value for N sessions around which $W(t)$ and $q(t)$ oscillate respectively. The proposed observer has been tested with the state feedback AQM in [16] and observer gains are $L = [1.2338538, 5.2445906, 2.24 * e + 3, 1.94 * e + 2]$. This observer is synthesized to construct the state of CFC and PFC attacks.

1) Attack reconstruction for traffic with constant flash-crowd (CFC): Figures 15, 16 and 17 illustrate a typical realization of traffic including CFC attack which can be detected by our time-delay linear observer. This CFC attack generated by our hybrid UAV network simulator has been injected into Simulink to compare our IDS model to the real traffic traces. This is depicted in Figure 17 where regular traffic is around 30 pkt/s when, for the malicious traffic, the throughput is increased to 150 pkt/s. Moreover, the real traffic (blue) and estimated intrusion (red) are plotted on the same figure for comparison purposes. Figure 16 shows the time response of the estimation queue $q(t)$ calculated by the time-delay linear observer method. As expected, the queue is stabilized above the desired level and the intrusion does not affect the different steady states of the system. Figure 15 shows the time response of the TCP congestion windows $W(t)$. As expected, the TCP congestion window evolution is reconstructed with great accuracy.

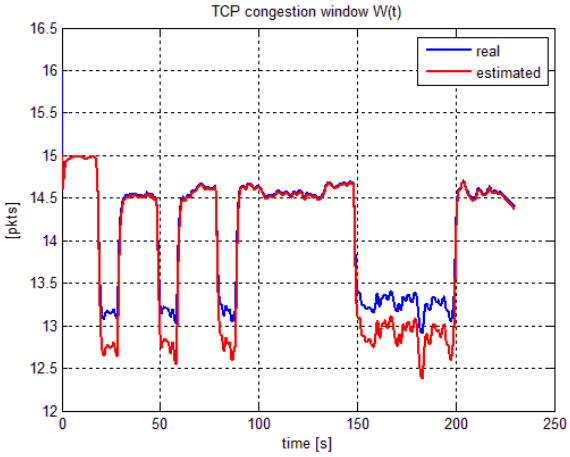

Fig. 15. TCP congestion window W(t) - CFC attack

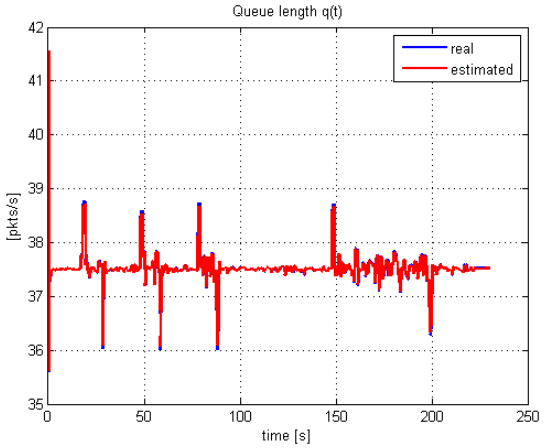

Fig. 16. Queue length q(t) - CFC attack

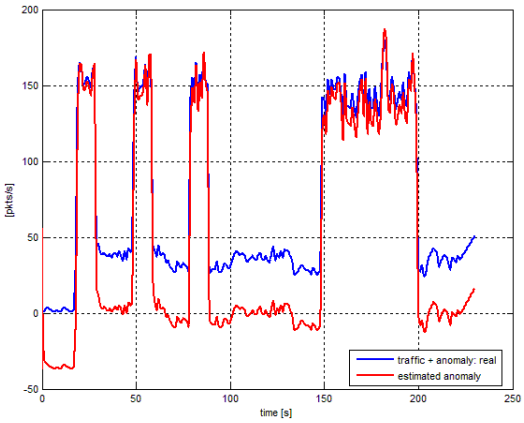

Fig. 17. Estimation with real traffic replay - CFC attack

2) Attack reconstruction for traffic with progressive flash-crowd (PFC): In this section, we consider the PFC attack generated by our hybrid UAV network simulator. As previously

mentioned, these attacks have been injected into Simulink to compare our IDS model with the real traffic traces. This is depicted in Figure 20 where regular traffic is around 40 pkt/s; while for the malicious traffic, the throughput is increased slowly to reach values close to 140 pkt/s. We can observe that the estimator is able to reproduce the shape of the anomaly quickly and make an accurate distinction between the normal traffic and the intrusion traffic (see Figure 20 for details). In addition to this, our controller / observer is able to estimate the states of system $W(t)$ and $q(t)$ with accuracy (see Figures 18 and 19 for details).

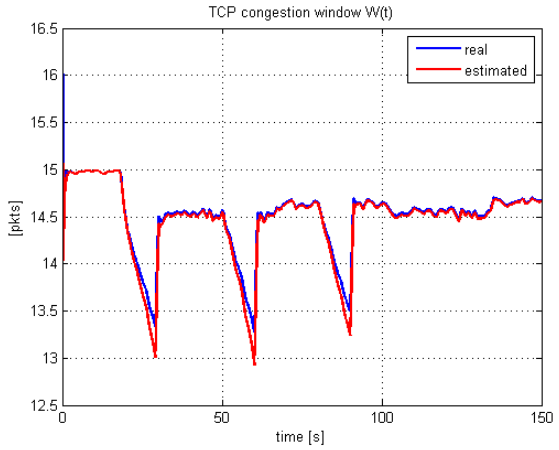

Fig. 18. TCP congestion window W(t) - PFC attack

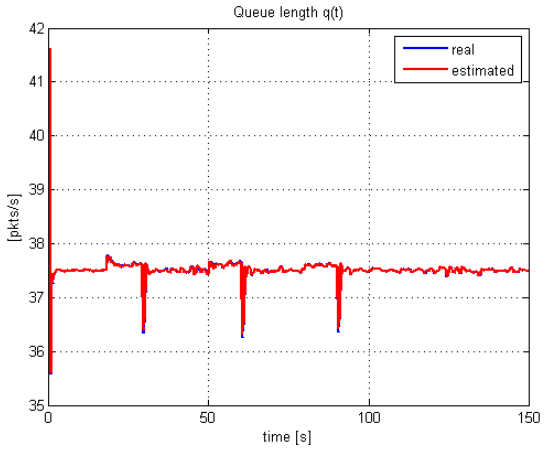

Fig. 19. Queue length q(t) - PFC attack

3) Discussion on traffic reconstruction performances: These results look promising given that the estimator simulated with Matlab Simulink is able to detect the different intrusions rapidly and with an accurate threshold. The delay in the detection is negligible and the estimator can make an accurate distinction between legitimate traffic and traffic with intrusions. Consequently, this is a first promising result for intrusion detection system design applied to drone fleet network.

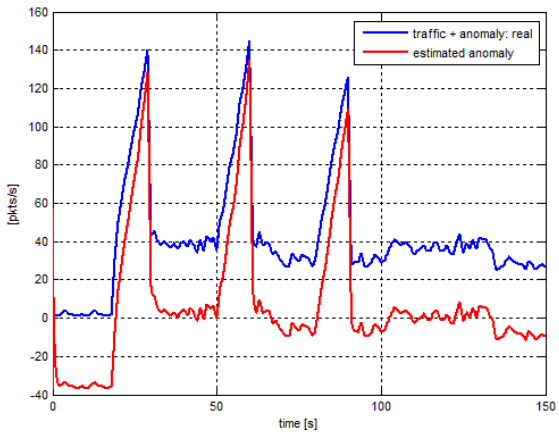

Fig. 20. Estimation with real traffic replay - PFC attack

V. Conclusion and Future Work

In this paper, we have explained how a new hybrid method can improve intrusion detection systems in the specific context of drone fleet. We have combined the use of a linear controller / observer and spectral analysis of the traffic. Based on a wavelet analysis, this traffic characterization process provides a preliminary level of knowledge about which type of intrusion is performed in the network. Based on this information, our linear controller / observer can be tuned and can perform traffic reconstruction in order to estimate accurately the level of attack observed in the network. Consequently, our design methodology provides a simple way to construct and instantiate our gain matrices for both the AQM controller and the observer. This approach has given us promising results with a simple topology within a time-delay framework. Indeed, two different types of anomaly have been considered in this paper (constant and progressive flash-crowds) and they are both accurately detected by the intrusion detection process proposed in Section 3 and validated in Section 4.

In our future work, we intend to identify several research perspectives. First of all, we plan to propose an evolution of the modeling in the drone fleet network. This should include different types of traffic (UDP and TCP for instance) and also take into account network mobility. Moreover, we plan to analyze different types of attack: not only DDoS but also intrusion where the traffic generated in the network is significantly lower and therefore, more difficult to detect. A proposed solution would be to consider one bank of models in order to detect, with different signatures, DDoS and other types of attack. Finally, we plan to investigate a way to implement and test this new generation intrusion detection system operating in a real environment. To address this last objective, we would like to consider real experiments with real UAVs. Each UAV could embed this specific bank of models. By conducting a collaborative mission, in the context of one UAV fleet, we will be able to test and validate the theoretical estimators which, until now, have only been studied in simulation. We plan to perform this part of the research in the near future in the recently constructed UAV flight arena in ENAC, Toulouse, France.

REFERENCES

[1] A. Lakhina and al., Diagnosing network-wide traffic anomalies, in ACM SIGCOMM, Portland, 2004, pp. 219230.

[2] A. Hussain ans al. A framework for classifying denial of service attacks, in SIGCOMM, Karlsruhe, Germany, Aug 2003, pp. 99110.

[3] V. Chandola and al., Anomaly detection: A survey, ACM Comput. Surv., vol. 41, no. 3, pp. 158, 2009.

[4] P. Borgnat, G. Dewaele, K. Fukuda, P. Abry, and K. Cho, "Seven Years and One Day: Sketching the Evolution of Internet Traffic," in IEEE INFOCOM 2009, 2009, pp. 711-719.

[5] Abry, P., Veitch, D. and Flandrin, P. (1998), "Long-range Dependence: Revisiting Aggregation with Wavelets". Journal of Time Series Analysis, 19: 253266. doi:10.1111/1467-9892.00090

[6] H. Wendt, "Contributions of Wavelet Leaders and Bootstrap to Multifractal Analysis: Images, Estimation Performance, Dependence Structure and Vanishing Moments. Confidence Intervals and Hypothesis Tests.", Signal and Image processing, Ecole normale suprieure de lyon - ENS LYON, 2008.

[7] H. Wendt, Patrice Abry, and Stephine Jaffard. "Bootstrap for empirical multifractal analysis." IEEE signal processing magazine 24.4 (2007): 38-48.

[8] H. Wendt, and Patrice Abry. "Multifractality tests using bootstrapped wavelet leaders." IEEE Transactions on Signal Processing 55.10 (2007): 4811-4820.

[9] H. Wendt, et al. "Wavelet leaders and bootstrap for multifractal analysis of images." Signal Processing 89.6 (2009): 1100-1114.

[10] M. Fliess and al., Advances in Communication Control Networks, ser. Lecture notes in Control and Information Sciences. Springer, 2005, ch. An Introduction to Nonlinear Fault Diagnosis with an Application to a Congested Internet Router, pp. 393395.

[11] S. Rahme and al., Sliding mode observer for anomaly detection in TCP/AQM networks, in Communication Theory, Reliability, and Quality of Service, 2009. CTRQ 09. Second International Conference on, 20-25 2009, pp. 113 118.

[12] S. Rahme , and al., Second order sliding mode observer for anomaly detection in TCP networks: from theory to practice., IEEE Conference on Decision and Control 2010, pp 5120-5125.

[13] S. Rahme and al., Sliding Modes for Anomaly Observation in TCP Networks: From Theory to Practice., inIEEE Transactions on Control Systems Technology, 2013, 21(3):1031-1038

[14] T. Floquet and al., On sliding mode observers for systems with unknown inputs, International Journal of Adaptive Control and Signal Processing, vol. 21, no. 8-9, pp. 638656, 2007.

[15] C. Edwards, and al., "Advances in Variable Structure and Sliding Mode Control", Lecture Notes in Control and Information Science, Springer-Verlag, Berlin (2006), pp. 271292

[16] Y. Ariba and al., "Traffic monitoring in transmission control protocol/active queue management networks through a time-delay observer," in IET Control Theory and Applications, vol. 6, no. 4, pp. 506-517, March 1 2012.

[17] K. K. Ramakrishnan and S. Floyd., "A proposal to add explicit congestion notifi- cation (ecn) to ip". RFC 2481, January 1999.

[18] C. Chen and al., Design of robust active queue management controllers for a class of TCP communication networks, Information Sciences., vol. 177, no. 19, pp. 40594071, 2007.

[19] S. Manfredi and al., Robust output feedback active queue management control in TCP networks, in IEEE Conference on Decision and Control, Dec. 2004, pp. 1004 1009.

[20] D. Wang and C. V. Hollot, Robust analysis and design of con- trollers for a single TCP flow, in IEEE International Conference on Communication Technology (ICCT), vol. 1, Apr. 2003, pp. 276280.

[21] K. B. Kim, Design of feedback controls supporting TCP based on the state space approach, in IEEE Trans. on Automat. Control, vol. 51 (7), Jul. 2006.

[22] Y. Ariba and al., Design and performance evaluation of a state-space based AQM, in IARIA International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ 2008), Jul. 2008, pp. 8994.

[23] R. Fontugne, P. Abry, K. Fukuda, D. Veitch, K. Cho, P. Borgnat and H. Wendt, "Scaling in Internet Traffic: A 14 Year and 3 Day Longitudinal Study, With Multiscale Analyses and Random Projections," IEEE/ACM Transactions on Networking, vol. 25, pp. 2152-2165, Aug..

[24] H. S. Low, F. Paganini, and J. Doyle, "Internet Congestion Control". IEEE Control Systems Magazine, Feb 2002, vol. 22, pp. 2843.

[25] R. Srikant, "The Mathematics of Internet Congestion Control". Birkhauser, 2004.

[26] S. Tarbouriech and al., "Advances in communication Control Networks". Springer, 2005.

[27] V. Jacobson, Congestion avoidance and control, in ACM SIG- COMM, Stanford, CA, Aug. 1988, pp. 314329.

[28] K. Gu, V. L. Kharitonov, and J. Chen, "Stability of Time-Delay Systems". Birkha user Boston, 2003, control engineering.

[29] V. Misra and al., Fluid-based analysis of a network of AQM routers supporting TCP flows with an application to red, in ACM SIGCOMM, Aug. 2000, pp. 151160.

[30] S. Floyd and V. Jacobson, Random early detection gateways for congestion avoidance, IEEE/ACM Transactions on Networking, vol. 1, pp. 397413, Aug. 1993.

[31] S. Athuraliya and al., An enhanced random early marking algorithm for internet flow control, in IEEE INFOCOM, Dec. 2000, pp. 14251434.

[32] C. V. Hollot and al., Analysis and design of controllers for AQM routers supporting TCP flows, IEEE Trans. on Automat. Control, vol. 47, pp. 945959, Jun. 2002.

[33] Y. Ariba and Y. Labit,"Congestion control of a single router with an active queue management", International Journal on Advances in Internet Technology,2009.

[34] J.-A. Maxa and al. "Emulation-Based Performance Evaluation of Routing Protocols for Uaanets". Nets4Aircraft 2015, May 2015, Sousse, Tunisia. Springer, LNCS (9066), pp.227-240, Nets4Cars/Nets4Trains/Nets4Aircraft 2015.

[35] A. Grim, T. OConnor, P. Olver, C. Shakiban, R. Slechta and R. Thompson, "Automatic Reassembly of Three-Dimensional Jigsaw Puzzles", International Journal of Image and Graphics, vol. 16, no. 02, p. 1650009, 2016.

[36] T. Miquel, J.-P. Condomines, R. Chemali, N. Larrieu. "Design of a robust Controller/Observer for TCP/AQM network: First application to intrusion detection systems for drone fleet". IROS 2017, EEE/RSJ International Conference on Intelligent Robots and Systems, Sep 2017, Vancouver, Canada. hal-01545617

École Nationale de l'Aviation
7, avenue Édouard Belin
BP 54005
31055 Toulouse cedex 4
Tèl. +33 (0)5 62 17 40 00
Fax +33 (0)5 62 17 40 23

N° éditeur ISSN.....

ENAC

La référence aéronautique

www.enac.fr