Network Intrusion Detection System for UAV Ad-hoc Communication From methodology design to real test validation

Jean-Philippe Condomines, Ruohao Zhang, Nicolas Larrieu

Version of Record: https://www.sciencedirect.com/science/article/pii/S1570870518306541
Manuscript_529b38631eb1f979c27cb4b35bbb5718

Network Intrusion Detection System for UAV Ad-hoc Communication

From methodology design to real test validation

Jean-Philippe Condomines, Ruohao Zhang and Nicolas Larrieu

Université de Toulouse, ENAC, BP 54005, Toulouse Cedex 4, 31055, France
firstname.surname at enac.fr

Abstract

The use of a swarm of low-cost, mission-specific drones to form a Flying Ad-hoc Network (FANET) has literally become a 'hotspot' in the drone community. A number of studies have been conducted on how to achieve a FANET, but few have considered the security perspectives of this subject. FANET's unique features have made it difficult to strengthen its defense against ever-changing security threats. Today, more and more FANET applications are implemented into civil airspace, but the development of FANET security has remained unsatisfactory. In this paper, we try to address this issue by proposing a new Intrusion Detection System (IDS), an hybrid method based on both spectral traffic analysis and a robust controller / observer for anomaly estimation inside UAV networks. The proposed hybrid method considers, as a preliminary step, a statistical signature of the traffic exchanged in the network. By examining the resulted signatures, the differences are used to select the accurate model for accurate estimation of that abnormal traffic. The proposed IDS design has been successfully applied to some relevant practical problems such as ad hoc networks for aerial vehicles, and the 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 UAV communication networks. Indeed, different types of anomaly have been considered and they are all accurately detected by the intrusion detection process we propose in this paper. Finally, both simulation-based validation and real-time real-world based implementation of our IDS are described in this article.

Keywords: UAV, FANET, Intrusion Detection System, Spectral Analysis, Robust Estimator, Drone Ad Hoc Network

1. Introduction

During the past years, Unmanned Aerial Vehicles (UAVs) are attracting more and more attention. The use of UAVs has many apparent advantages over conventional maned aircrafts especially in terms of operational expense, operator's safety, operability in difficult/hazardous environments and accessibility for civil applications. Recent technical advancements have made it easier than ever to setup an Unmanned Aerial System with complex topology to achieve sophisticated missions which were previously impossible without actual human involvements. The rapid advancements and heavy involvement of Information Technology have huge impacts on the path which drone communities take to develop future UAV systems. Today's decentralized technology promotes distribution of mission and corresponding resources [1]. This approach allows redundancy in terms of critical components and improve the overall robustness of the system. However, most of today's advancements in the domain of network-attached UAV fleet are focusing on the path to achieve a drone network as described in [2, 3, 4]. Little has been considered for the cyber security of the drone network approaches leaving even the most state-of-art drone network systems vulnerable against various security threats [5]. Several researches [6, 7, 8, 9] have been conducted describing in detail the possible security threats a UAV fleet can be facing during its normal operation. Here we address one type of FANET security issues which is network intrusion in a wireless ad-hoc network. As described in [10, 11] there are multiple threat models related to network intrusion such as overload, flash crowds, worms, port scans and jamming attacks. Among these abnormal patterns, 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 a major adversity for UAV certification and integration into civil airspace. Consequently, malicious anomaly detection is an important issue nowadays. In [12] 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 for dealing with 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. Our proposed intrusion detection model is a two-step mechanism which first characterize the traffic by using a statistical signature and then select a precise estimator model to reconstruct the attack traffic.

All types of attack which do not follow the initial characteristics trigger an alarm and, consequently, the malicious traffic can be analyzed in depth. 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 detected, analyzed and managed. Consequently, the security and performance of the entire network can be improved. This traffic characterization is performed thanks to a statistical signature of the traffic exchanged in the network. Note that, statistical signatures, based on wavelet analysis, have been selected because they offer a wide spectral characterization of the entire traffic process. Each 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 and make a model of the anomaly in the UAV network. Subsequently, attack will be analyzed by using a robust control estimation to reconstruct the attack traffic. This is the first time that both spectral analysis and robust control estimation have been coupled and used on a UAV ad hoc network traffic.

The main contribution of this paper is to propose a new hybrid method which is able to detect traffic anomalies (i.e. DDoS). Tests with real network conditions have been performed to evaluate the characteristics of this method and to explore the possibilities of future integration. The preliminary design of our new IDS process and its theoretical assessment have been faced with real traffic traces. These traces have been generated using a hybrid UAV network simulator. Consequently, the validation of the new IDS system is improved by testing its performances faced with real DDoS attacks, real UAV trajectories, real UAV background traffic, and real UAV fleet topology in real-time. Finally, different types of anomaly have been considered and they are all accurately detected by the intrusion detection process we propose in this paper. First results for the proposed Intrusion Detection System (IDS) in a fleet of UAVs are promising.

In the sequel, Section 2 addresses the state of the art of FANET and the new challenges risen with this new topic, Then we present the characterization tools described in the literature to extract network traffic signatures and the theoretical background of our proposed controller / observer system. 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. Section 4 gathers all the results obtained after solving the time-delay linear estimation problem in real conditions. Finally, Section 5 describes the details about the proposed hybrid IDS implementation in real-time real-world environ-

ments, and introduces different test methods that we have examined and results we have obtained before we draw the conclusion.

2. Related Work

The intrusion detection methodology proposed in this paper is the result of a collaboration between two scientific fields. The first one is related to traffic characterization. It uses spectral analysis in order to generate a specific traffic signature. 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 on the related fields.

2.1. UAV ad-hoc network and challenges

The use of a fleet of UAV is advantageous and just as challenging. A number of researches have been conducted to identify different threats. In [2], the authors have addressed the unique characteristics related to Flying Ad-hoc Network or FANET which need to be specifically taken care of during the design of the network system. In [5, 9] the authors have discussed in detail the possible security threats within the drone communication system including cyberattacks such as Jamming, Spoofing or Intruding the wireless network system. One of the most significant challenge while securing a FANET comes from the mobility of the network structure. FANET is essentially a subset of Mobile Ad-hoc Network (MANET) [3]. In contrast to a stationary ad-hoc network, a FANET is subject to constant changes of network topology due to the continuous variation of number and roles of the participants in the network. Moreover, a drone system is built upon complex wireless sensory sub-systems [7], and an UAV is designed to operate with as less human intervention as possible. Those natures have potentially make the UAV network defense a Whac-a-Mole game. Furthermore, a secured communication alone is not enough to ensure the safety of the overall FANET communication system as demonstrated in [13]. For example, in [5, 14] the authors discussed a scenario where attacks can happen on a illegally 'captured' drone. Indeed, for a FANET, the risk of losing a drone to the wrong hands remains to be practical. In such case, hackers can get access to the network regardless the wireless encryption and launch different attacks to the network from within. But most importantly, FANET is undoubtedly making its way into civil airspace. As a consequent, the safety perspective rather than the security perspective will have the uttermost importance - a secured FANET can help improve the

safety of UAV fleets, but it is more important to ensure the safety of the overall system even if the network is compromised. Hence, existing network security strategies for fixed-topology is deemed no longer effective. The new network security strategies must be implemented to ensure the safety of the system by also taking into account the mobility of the network, various possible attacks and the risk of attacks from within the network.

2.2. Network Intrusion detection systems for FANET

The civil applications of UAVs have experienced a very rapid advancement in the last decade. Alongside their recent achievements and promising future, its issues are just surfacing. Various researches have been conducted to address aforementioned challenges such as GPS spoofing, eavesdropping and signal jamming, [9] but only until recent years, the network intrusion detection for FANET has finally caught the attention from the drone community. [15] has proposed an IDS design based on belief approach to identify the prime suspect of intruder inside a FANET. This approach has an improved false positive rate against misbehaviors of a member of the network. However, this method is focusing on general misbehaviors of a member and requiring prior knowledge of all possible behaviors of the system. In contrary, we are proposing a new IDS method based on both spectral signature analysis and robust control/estimation theory aiming specifically at detecting network intrusion within the network. The two methods are considered complimentary to the future design of FANET IDS systems.

2.3. Spectral analysis for traffic characterization

Several research studies have been conducted for traffic characterization using spectral analysis. One of the most consistent is [16]. 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 [17] 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 [17] developed by H. Wendt more recently called Wavelet Leader Multi-fractal (WLM) analysis toolbox(see [18, 19, 20, 21] for details).

2.4. 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 [22] described in the literature, the Super-Twisting Algorithm (STA) [23, 24, 25] 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 [26] 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 [27]. 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 [28] 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) [29] 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 [30, 31, 32, 33]. A relevant constructive algorithm [34] has been proposed.

3. Intrusion Detection Methodology

Our methodology introduced in this section is a two-step process (see Figure 1 for details). The first step is dedicated to traffic characterization. Its objective is to calculate a specific signature of the traffic we want to analyze. We will see in Section 4 that we are able to obtain two completely different attack signatures according to Wavelet Leader Multi-fractal 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.

3.1. Step 1: spectral analysis-based traffic signature with WLM method

Internet traffic exhibits scale invariance property by its nature. As proposed in [35] scaling and multifractal properties exists in computer network traffic throughout different time scales. Accordingly, multifractal analysis is a frequently used

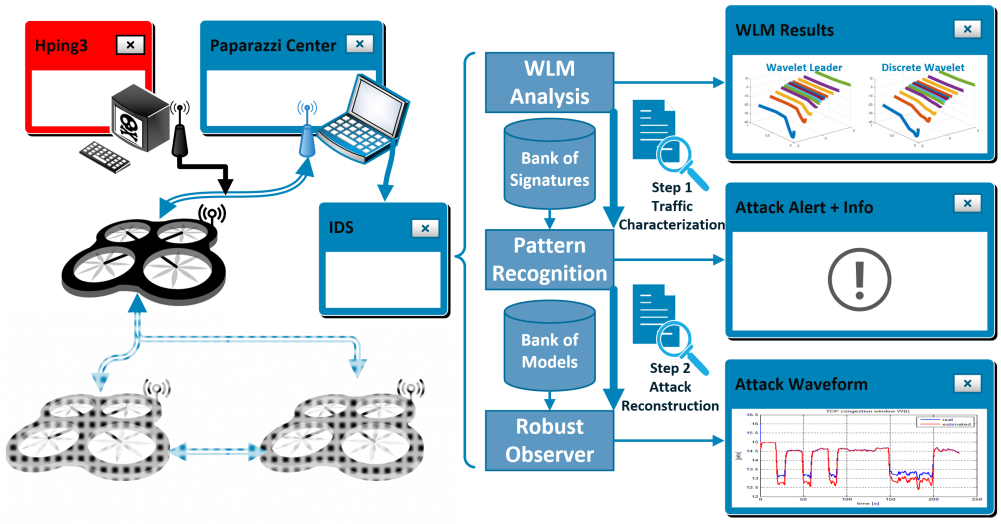


Figure 1: General two-step framework of the proposed IDS system

tool to analyze this type of traffic. Wavelet coefficient and wavelet leader analysis are common tools to analyze self-similarity and scaling properties. Here we adapted a Wavelet Leader Multifractal (WLM) method introduced in [18, 19, 20, 21]. This method was first introduced to study hydrodynamic turbulence data which is also regarded as a good example of a signal containing scale invariance properties.

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. It considers multifractality of a signal by computing not only the wavelet coefficients of power law at the 2^{nd} order, but also other arbitrary orders. This toolbox is well defined and proven by various applications.[19, 36, 37] This process produces a graphical result (called a spectral signature) which is used to find the differences between legitimate traffic and traffic which contains an anomaly. To best capture the complexity of the traffic, we also consider the different statistic moments of analysis. The result is a set of 3-dimensional curves that represent the dynamic of the traffic at different moments and time scales.

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 need to verify scale invariance in order to justify the self-similarity feature. This feature is also observed in the analyzed data when a power law is observed when the static signature is plotted (by a log-log diagram) for specific time scales of this

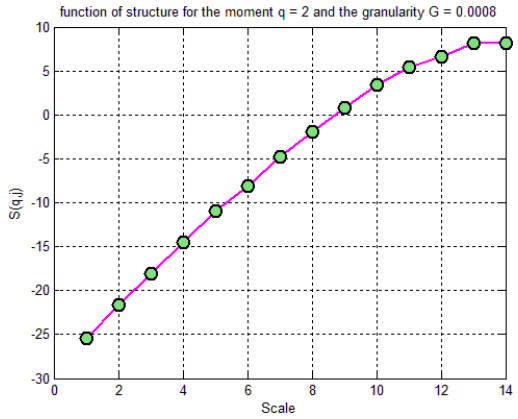


Figure 2: Example of WLM signature of a data series at statistic moment $q = 2$

data. We show in Figure 2 an example of the power law we can observe for one of the network traffic series analyzed. Section 4 will present in detail the different attacks we have analyzed and the different signatures we obtained for each one. 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

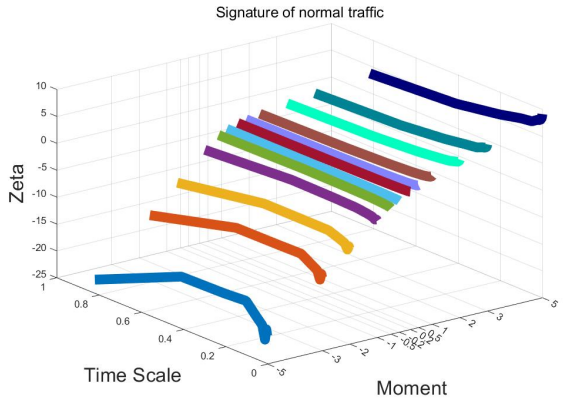


Figure 3: Example of WLM signature at multiple statistical moments

Figure 3. This figure represents the spectral characteristics of the data (i.e. the *zeta* parameter) according to the time scale of analysis and the moment of observation. We will illustrate in Section 4 how this signature can be different according to the type of attack we wish to analyze and detect.

These differences are useful for traffic characterization but can also be very helpful in selecting a dedicated robust estimation model. 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.

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

In order to improve future design of network IDS devices against unknown type of attacks, we need to reconstruct the exact properties of the attack. This process is performed by using Step 1's signatures to select, in Step 2, different kinds of model and to, finally, tune the controller / observer. When representing the dynamics of a observed / controlled system such as the TCP dynamics of an ad hoc network mathematically, we often use the concept of state. By definition, the state of a system is the set of parameters whose values must be known at a given moment in time, in order to predict the future evolution of the system. This idea is very natural for systems whose evolution over time can be described by differential equations. The solution of a system of differential equations of order $n \in \mathbb{N}^*$ depends on a set of n initial conditions. These initial values determine the subsequent states taken by the system over time. Thus, modeling dynamic systems by means of state representations, whether linear or non-linear, tends to be more fruitful than other types of model (such as input / output black boxes), since it gives us access to a direct formulation of the underlying physics of the process. The role of an controller / observer is therefore to produce an accurate estimate $\underline{\hat{x}}$ of non-measured states $\underline{x}$ (states that cannot be accessed directly by performing measurements) given knowledge of the inputs and an array of imperfect measurements. Various implementations of TCP models in terms of assumptions and numerical techniques [38, 39, 40] exist. TCP network is commonly represented using a linearized fluid-flow model [38] 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 (see Figure 4). 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.

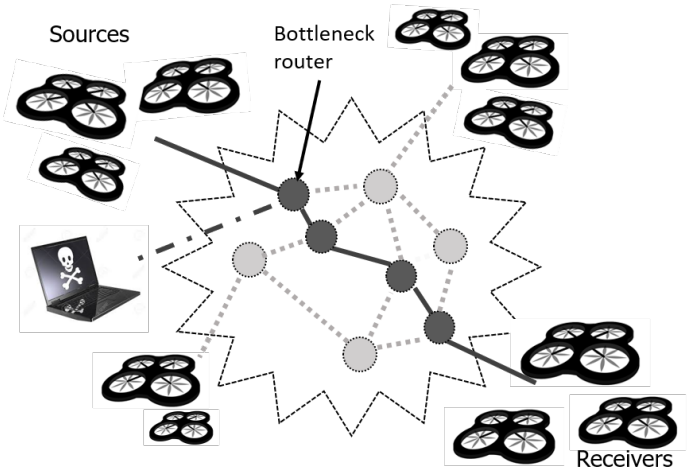


Figure 4: sources / receivers connection in a fleet of UAVs

To implement an Intrusion Detection System (IDS) according to the network topology presented previously, the estimation module inserts itself between the other modules as follows: the estimation system receives noisy measurements (e.g. probability of packet, queue of the router buffer) as inputs from the sensors, then merges this data using the TCP model of the network to compute a solution to the estimation problem. 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:

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

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

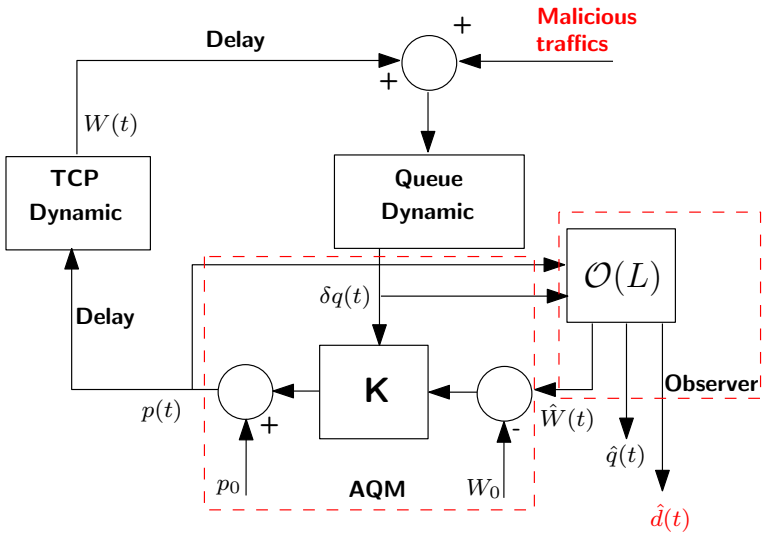


Figure 5: Step 2 : attack reconstruction

state space representation corresponding to $\mathcal{M}_s$ 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. Our objective from Step 1 is to provide a model that is as complete and sufficient as possible, and in particular capable of representing any attack modeled by $d(t)$ as accurately as possible. Based on such a model, formulated in the general form of a time-delay system, it is possible to design both AQM and estimator in order to estimate the malicious intrusion while taking into account a level of QoS (i.e. the drop probability $p(t)$) . As shown in Figure 5 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). Various AQM mechanisms exist in the literature such as Random Early Detection [41] (RED), Random Early Marking [42] (REM) and more recently using control theory (proportional and proportional integral controller [43] or state feedback controller [44]). The estimator has to be designed in addition to an efficient AQM. We proposed a robust controller / observer for IDS by solving an LMI criteria (see [46], for details of proof) on the following augmented model:

$$\delta\mathcal{M}_s^+ \left\{ \begin{array}{rl} \delta\dot{\tilde{\underline{x}}}(t) & = \bar{\mathbf{A}}\delta\tilde{\underline{x}}(t) + \bar{\mathbf{A}}_d\delta\tilde{\underline{x}}(t-\tau(t)) + \bar{\mathbf{B}}\delta p(t-\tau(t)) \\ y(t) & = \bar{\mathbf{C}}\delta\tilde{\underline{x}}(t) \end{array} \right. \tag{2}$$

With

$$\begin{cases} \bar{\mathbf{A}} = \begin{bmatrix} -\frac{N}{\tau_0^2 C} & \frac{1}{\tau_0^2 C} & 0 \\ \frac{N}{\tau_0} & -\frac{1}{\tau_0} & 1 \\ 0 & 0 & 0 \end{bmatrix} \\ \bar{\mathbf{A}}_d = \begin{bmatrix} -\frac{N}{\tau_0^2 C} & -\frac{1}{\tau_0^2 C} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \\ \bar{\mathbf{B}} = \begin{bmatrix} -\frac{C^2 \tau_0}{2N^2} \\ 0 \\ 0 \end{bmatrix} \\ \bar{\mathbf{C}} = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \end{cases} \tag{3}$$

where the perturbed variables $\delta\underline{\tilde{x}}(t)^T = [\delta W(t) \;\; \delta q(t) \;\; d(t)]^T$ around the desired equilibrium (W_0, τ_0, q_0) represents the augmented state. Practically, the objective is to reconstruct $d(t)$ from any attack modeled by wavelet analysis from Step 1, and design an output feedback AQM. In this paper, the malicious intrusion $\dot{d}(t)$ has been chosen constant (i.e $\dot{d}(t) = 0$) due to the assumption of flash crowd attack which can be mathematically represented by a step function. Consequently, we are looking for gain controller $\mathbf{K}$ and gain observer $\mathbf{L}$ defined as (see [46], for details of proof):

$$\mathcal{O}(L) \begin{cases} \delta u(t-\tau(t)) &= -\mathbf{K}y(t) = -\mathbf{K}\mathbf{C}\delta\underline{x}(t) \\ \delta\dot{\underline{\hat{x}}}(t) &= \bar{\mathbf{A}}\delta\underline{\hat{x}}(t) + \bar{\mathbf{A}}_d\delta\underline{\hat{x}}(t-\tau(t)) + \bar{\mathbf{B}}\delta u(t-\tau(t)) \\ & \quad + \mathbf{L}\left(y(t) - \mathbf{C}\delta\underline{\hat{x}}(t)\right) \end{cases} \tag{4}$$

The first equation corresponds to the dynamics of the AQM. The second equation corresponds to the estimation of the state vector $\delta\underline{\hat{x}}$ and describe the dynamics of the observer. We recognize the typical mathematical expression of a linear state estimator with correction terms $\mathbf{L}$. The idea is to build an additive correction term based on linear gains $\mathbf{L}$ which keeps stabling the dynamics of the estimation error $e(t)$. Such an approach is systematic for more complex dynamical systems than the ones represented by a single router.

4. Intrusion Detection System Validation

4.1. UAV ad hoc network hybrid platform

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 visualization tool because it is an easy-to-use and efficient hypervisor. The virtualized system is a 12.04 version Ubuntu, working with the

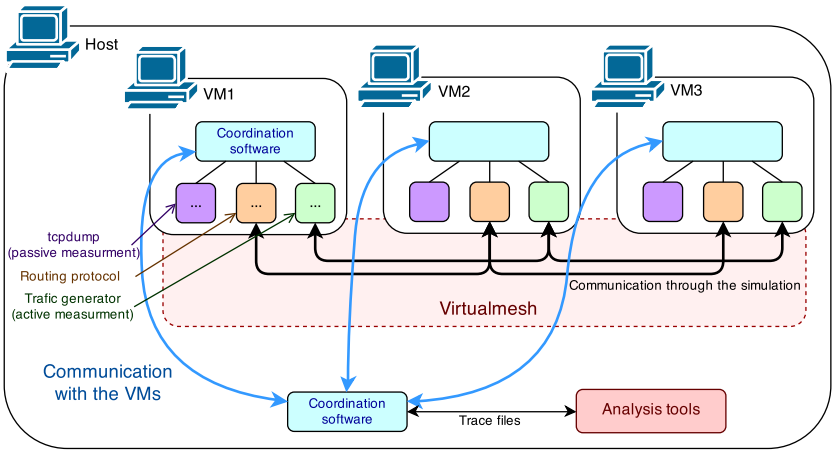


Figure 6: Testbed implementation

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 6. In [45], 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.

4.2. Traffic characterization results for intrusion detection system calibration

The objective of this analysis is to create a bank of signatures, 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 (Zeta) with respect to the statistic moments (q), which can take positive or negative values, and also with respect to the time scale of the traffic. We now illustrate the results obtained by our wavelet multifractal 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 $C = 1,250$ packets/s (which is equivalent to 3 Mbit/s), and $T_p = 30ms$ the propagation delay.

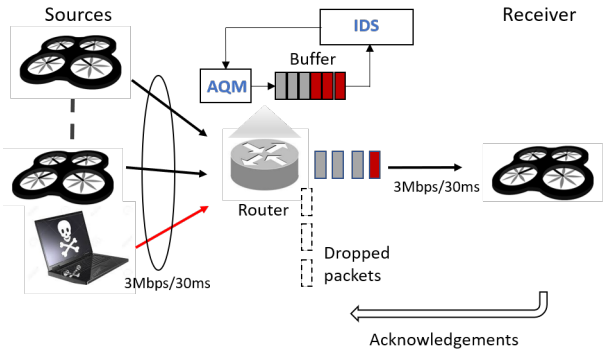


Figure 7: Considered topology

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[1] tool. This software is run on the hacker node

[1]http://www.hping.org/hping3.html

(see Figure 7 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 8a 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.

4.2.1. Attack signature for traffic with Constant Flash-Crowd CFC

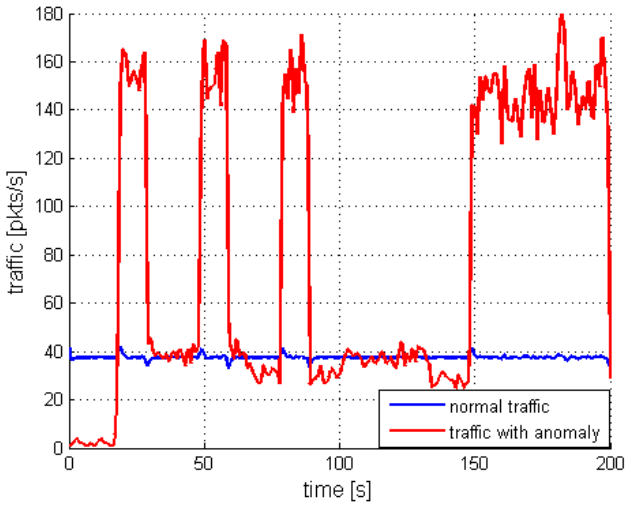
We consider in this section, the CFC attacks which have been generated. The objective is to obtain a dedicated spectral analysis for this specific type of DDoS attack. This spectral analysis (based on WLM analysis) provides a specific attack signature for each type of network traffic. Consequently, in Figures 8b and 8c, a comparison of the signatures of the regular traffic and traffic including CFC attacks is illustrated. The obtained results show a large variation in the scaling function $\zeta(q)$ (zeta), 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 $\zeta(q) \leq -33$ for traffic including DDoS attacks while it does not exceed the value of $\zeta(q) \leq -23$ for normal traffic.

4.2.2. Attack signature for traffic with Progressive Flash-Crowd PFC

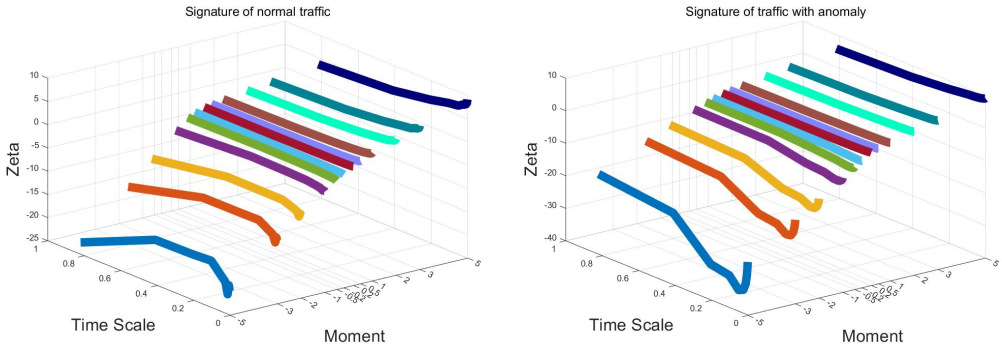
In a second time, the network is exposed to PFC attacks (see Figure 9a for details about the traffic profile of this DDoS). The comparison between traffic with and without attack shows that the variation of the scaling function $\zeta(q)$ is always noteworthy in negative statistic moments (here $q = -5$). Indeed, we can see in Figure 9b the values of the scale function are ranged between $-30 \leq \zeta(q) \leq 0$ for regular traffic. On the contrary, in the case of traffic including PFC attack, the values $\zeta(q)$ are ranged between$-31 \leq \zeta(q) \leq -5$ (see Figure 9c for details).

4.2.3. Discussion on traffic signature characterization

These characterization results show that it is possible to extract unique signatures 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 performed at this time by our intrusion detection system algorithm.



(a)



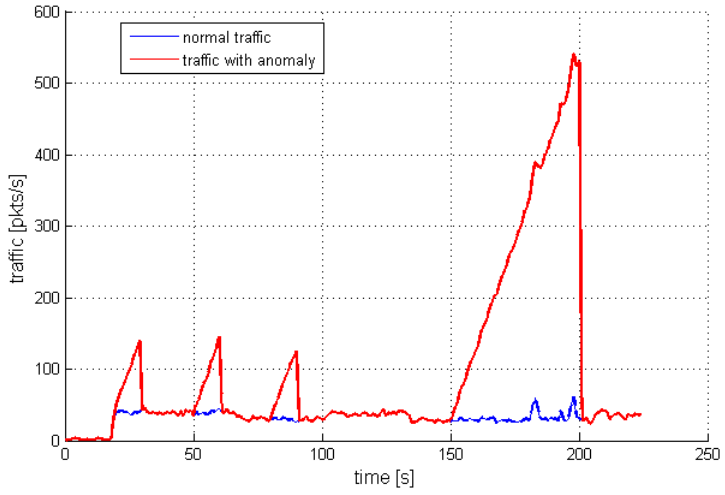
(b) (c)

Figure 8: (a) Waveform and (b,c) signature comparison between normal and CFC flooded traffics

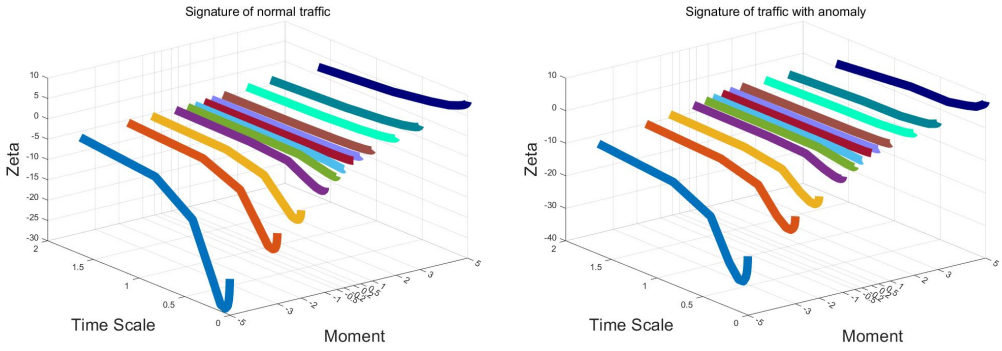
Indeed, these two steps (characterization and anomaly reconstruction) are performed separately. It is worth noting that the whole process is considered as a work-in-progress task. In the rest of this paper, we are going to present additional results related to the second step of this process: anomaly reconstruction and detection using robust controller / observer.

4.3. Anomaly detection and 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 1 the values of the congestion window size and the router



(a)



(b) (c)

Figure 9: (a) Waveform and (b,c) signature comparison between normal and PFC flooded traffics

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 [28] 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.

4.3.1. Attack reconstruction for traffic with constant flash-crowd (CFC)

Figures 10, 11 and 12 illustrate a typical realization of traffic including CFC attack which can be detected by our time-delay linear observer. This CFC attack

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

Table 1: Equilibrium point

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 12 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 11 shows the time response of the estimated 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 10 shows the time response of the TCP congestion windows $W(t)$. As expected, the TCP congestion window evolution is reconstructed with great accuracy.

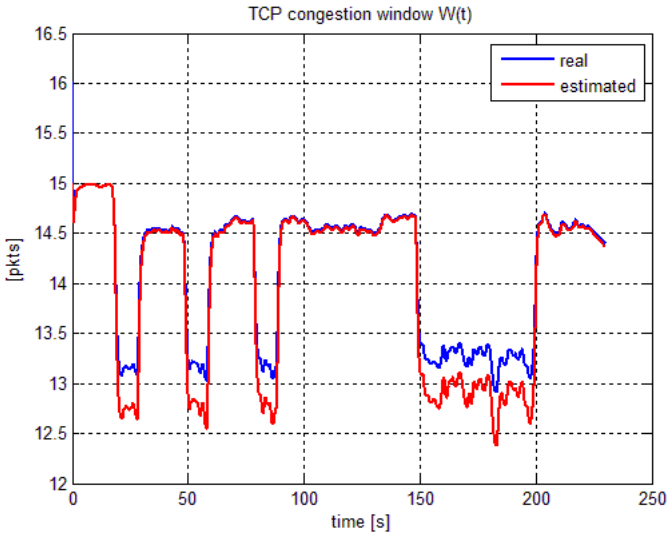


Figure 10: TCP congestion window W(t) - CFC attack

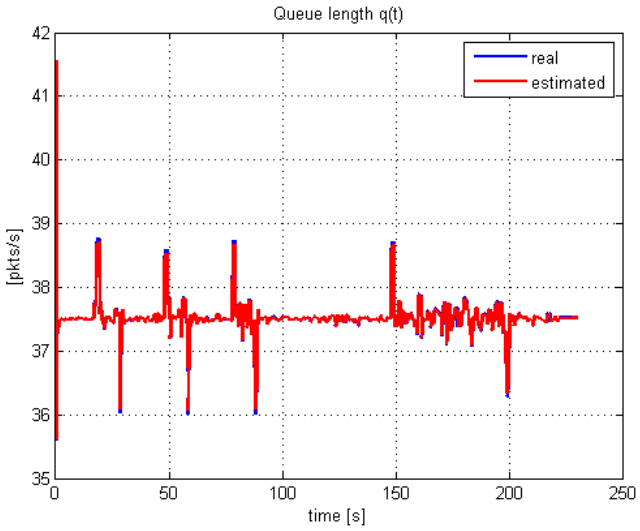


Figure 11: Queue length q(t) - CFC attack

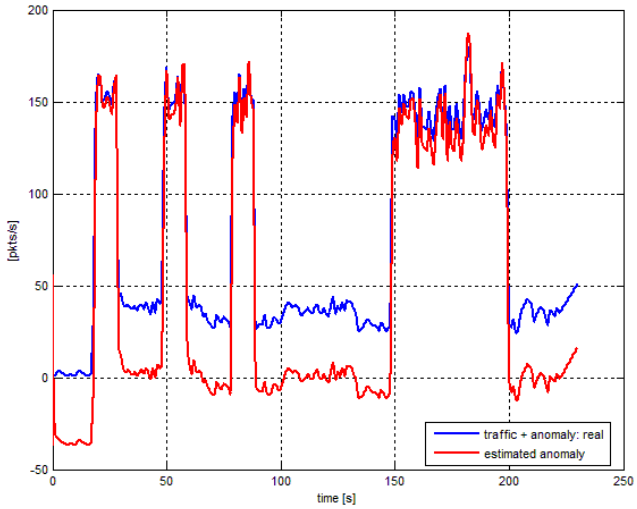


Figure 12: Estimation with real traffic replay - CFC attack

4.3.2. 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 15 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 ob-

serve 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 15). In addition to this, our controller / observer is able to estimate the states of system $W(t)$ and $q(t)$ with accuracy (see Figures 13 and 14 for details).

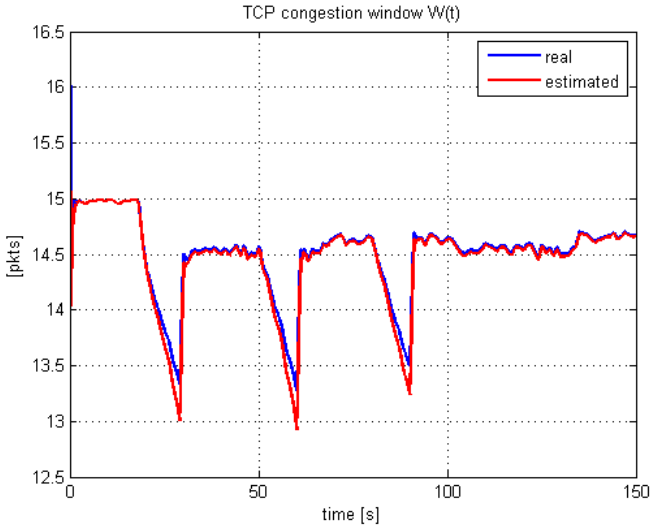


Figure 13: TCP congestion window W(t) - PFC attack

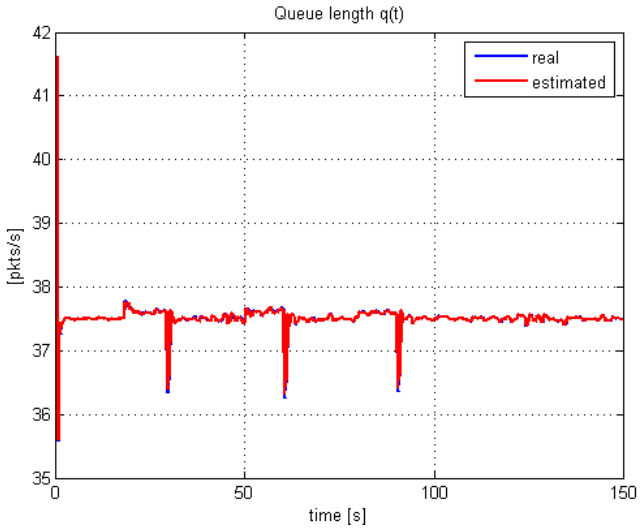


Figure 14: Queue length q(t) - PFC attack

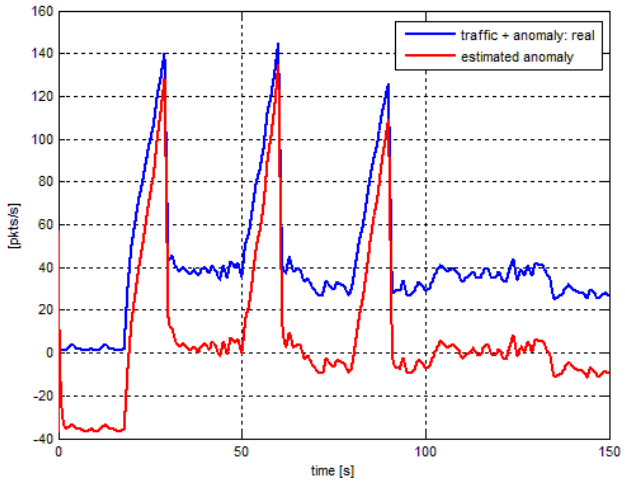


Figure 15: Estimation with real traffic replay - PFC attack

4.3.3. 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. In the next section, we will consider a more complex environment. Indeed, we will deploy our IDS in a real drone system and analyze if the first promising results we got with both our hybrid simulation / emulation platform and the Matlab Simulink estimator are confirmed.

5. Intrusion Detection System Implementation

In this section, we describe how we have implemented in a real environment the IDS methodology described in Section 3 and validated in Section 4. This real environment is built on real communications between a drone (Parrot ARDrone) and a dedicated Ground Control Station (GCS). The GCS is performed with Paparazzi software. A malicious data will be generated to stress the communications between the GCS and the drone and we will be able to perform a real validation of our IDS methodology.

5.1. Real test environment: Paparazzi software

The overall Paparazzi UAS (Unmaned Aerial System) can be decomposed into three segments (Figure 16):

- Ground segment: it is composed by all the ground software and hardware infrastructures (Ground Control Station (GCS), antennas, modems, video, receivers) that are used to prepare, monitor and analyze the flight. A ground station includes HMI interfaces (screen, keyboard, joystick, ...) that are used to interact with one or more UAV. This station can be centralized in one place or it can be distributed into several computers / locations;

- Airbone segment: it is composed by the aircraft, its hardware parts including payload and all the embedded software to control the flight (from stabilization to decision making). The embedded software is usually split into several on-board computers with real time capabilities (MCU using interrupts, with RT OS or not) or higher computation power (dedicated hardware such as FPGA, high-end embedded processors such as OMAP or ATOM);

- Communication segment (red and blue lines) : all the communication links and protocols between the ground and airborne segments. It mostly consists in defining the communication links to define bandwidth, frequency, type of communication (unidirectional, bidirectional), transmission protocols, message content and the structure of the communication network (centralized, dynamic point-to-point, ad-hoc, etc.).

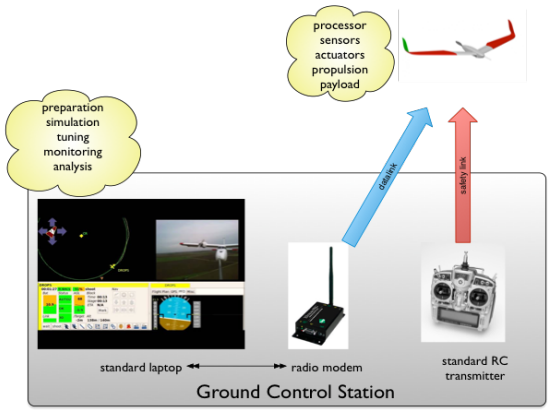


Figure 16: Global view of Paparazzi system

Autopilot and ground control station (a part of ground segment) are closely bonded, and usually developed and proposed by the same provider. The autopilot uses an onboard GPS receiver for navigation and returns this information to the ground station. In an autonomous flight phase, the pilot can monitor in real time the device and intervene if a deviation from the preset mission is detected. Thus, the ground control station is dedicated to visualizations for flight preparation, monitoring, control, and engineering tasks (flight tuning, logs post-processing). Onboard and ground systems cannot be mixed, consequently, there are two types of control system. Moreover, the first available systems were proprietary closed. Today they are challenged by the open source community that proposed opened hardware and source code solutions (cf. Paparazzi project at: `https://wiki.paparazziuav.org/`). Open source autopilots are mainly used by universities, laboratories for research and development activities such as our IDS system proposed by ENAC. These systems are constantly improved by its community members.

5.2. IDS method implementation into Paparazzi

Paparazzi software is developed in a modular fashion, such that it allows easy development of individual function blocks. To be specific, the communication between GCS and test UAV node is done by a Linker module.
Our IDS software is designed to first intercept / sniff packets between the Linker module and the UAV, then apply WLM analysis, in real-time, on collected packets and compare resulted signature with a bank of signatures to determine the nature of the traffic. Then, according to the attack information, the corresponding model is chosen from a bank of models to perform signature characterization of the attack.

The aforementioned WLM analysis Matlab toolbox has been then implemented in C++ environment for the best performance and easiest implementation into different platforms. This first implementation of the WLM analysis tool is an independent program running in Windows/Linux environment and it is to demonstrate the functionality and performance of this algorithm. Besides the calculation of signatures, the program also visualizes the results by calling open-source libraries: MathGL[2] and FLTK[3] and plotting the result in a new window. This allows us to have a global perspective of how the results will differ when malicious traffic

[2]http://mathgl.sourceforge.net
[3]http://www.fltk.org

is injected into the communication, before the actual acquisition of the bank of signatures.
Once we verified the steady performance of our WLM analysis module, the bank of signatures can be acquired by feeding the tool with collected packets from known normal or malicious traffics and recording the resulted signatures. To have a more general understanding of different traffics, we consider an extra degree of freedom: acquisition period, in addition to moments of analysis and time scales (sampling frequencies). This is because the duration of an attack is actually an important parameter to distinguish the type and intensity of the attack.

In the end, the IDS software module will provide us, in real-time, an animated window updating the signatures of current traffic, an alert when the signatures of current traffic are matched in the bank of signatures; some detailed information on the nature of the attack; the model to represent the attack; and the figure of the simulated attack from the observer.

5.3. Flooding attack generation

The main objective of our flooding attack scenario is to stress the communication network (between the GCS and the drone for instance) with malicious packets in order to saturate either the GCS or the drone and to generate a denial of service (DoS) into the communication. This malicious traffic will be generated thanks to Hping3 tool with the same experimental process than described in Section 4. This tool helps us to forge and generate as many TCP or UDP packets as we want in the network and for whatever network destination (e.g. IP address) we define. Moreover, an additional tool has been used to monitor the network and to analyse the traffic in real-time. This is the Wireshark sniffer packet analyser[4]. This tool helps us to observe, count and separate packets for both malicious and normal traffic.

5.4. Real traffic based flooding attack analysis

One of the communication use case we envision to conduct during the flooding attack is detailed in Figure 17 as shown below. One of our research application scenario involves three agents (one UAV named ARDRONE, a GCS and a monitor) in order to have the network topology considered in Figure 7. In the beginning, GCS continuously sends telemetry (attitude, flight plans) to the UAV. We then assume that based on HPing3, thousands of small TCP flows are exchanged in order to generate a SYN flood attack on the UAV. With such a flooding process, we are able to generate a Constant Flash-Crowd in the network. With this

[4]https://www.wireshark.org

type of real application use case, we will be able to test and validate the software communication architecture proposed in this paper within a real environment.

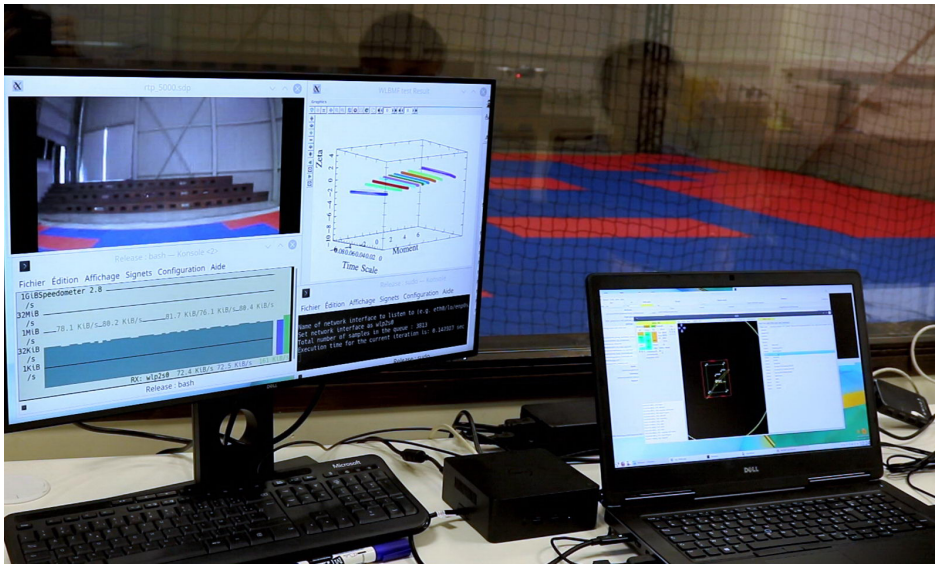


Figure 17: Intrusion Detection System use case

The real-world performance testings of the WLM analysis tool have been performed on traffic collected on the aforementioned test scenario. The packet rate is extracted from Wireshark recordings split into segments each contained 12,500 samples. Then the segmented samples are fed continuously into the WLM toolbox to simulate a real-time application scenario. The resulted signatures of the whole test period are plotted in the same figure to better demonstrate the characteristics of this analyze method.

It is shown in Figure 18 and 19, that for normal traffic, the signatures are more uniform and stay in a relatively small range of zeta. Meanwhile, when the traffic is under CFC attack, the signatures are clearly disturbed and lowered significantly especially at the negative moments.

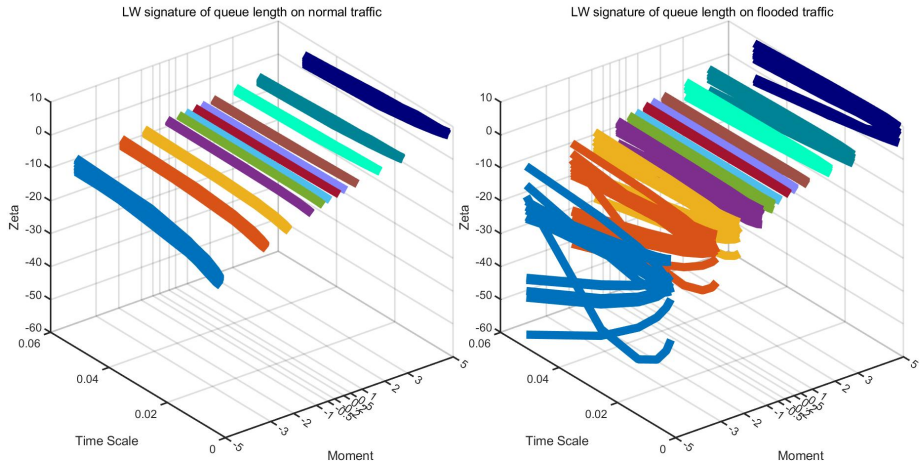


Figure 18: WLM Wavelet Leader analysis result on normal traffic(left) and flooded traffic(right)

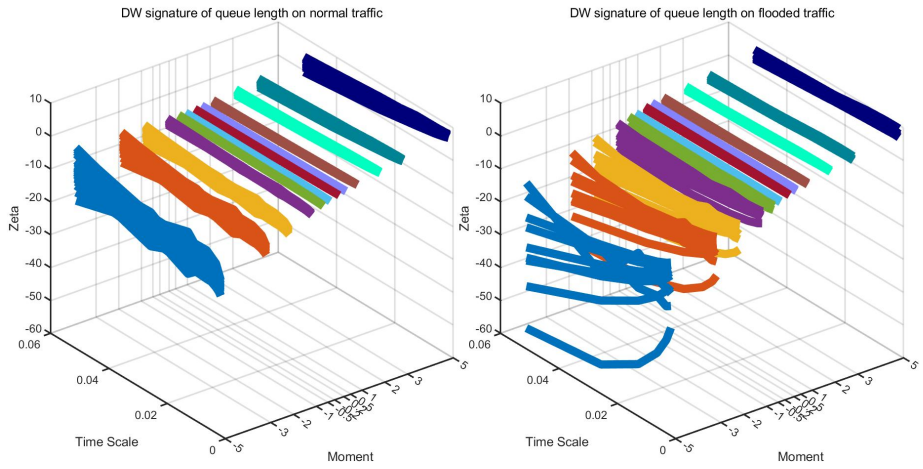


Figure 19: WLM Discrete Wavelet analysis result on normal traffic(left) and flooded traffic(right)

5.5. Real-time Implementation and Testings with Paparazzi UAV Emulation

Paparazzi software included a very convenient yet very realistic emulation setup. It allows us to test our methodology without the use of a real UAV and gives us better control over its network traffics. This specific Paparazzi module has been convenient to perform some tests in real time of our IDS methodology. No need to generate a huge important flooding attack between a real drone and the Paparazzi GCS. Consequently, the emulation only takes into account the UDP traffic between the GCS and the UAV which contains periodic updates of

the UAV's vital information. The network part of the emulation is realistic and it is done through sockets on the local host. Our IDS demonstration program takes advantage of this setup and by altering the reception port of the simulated Linker module, we can achieve the interception of packets transmitted between the GCS and the simulated UAV. The sums of packets' length during a given sample period are then collected in a ring buffer and fed into the WLM toolbox in batch. This implementation performs packet forwarding upon the reception of each packet to keep the emulation in the right order.

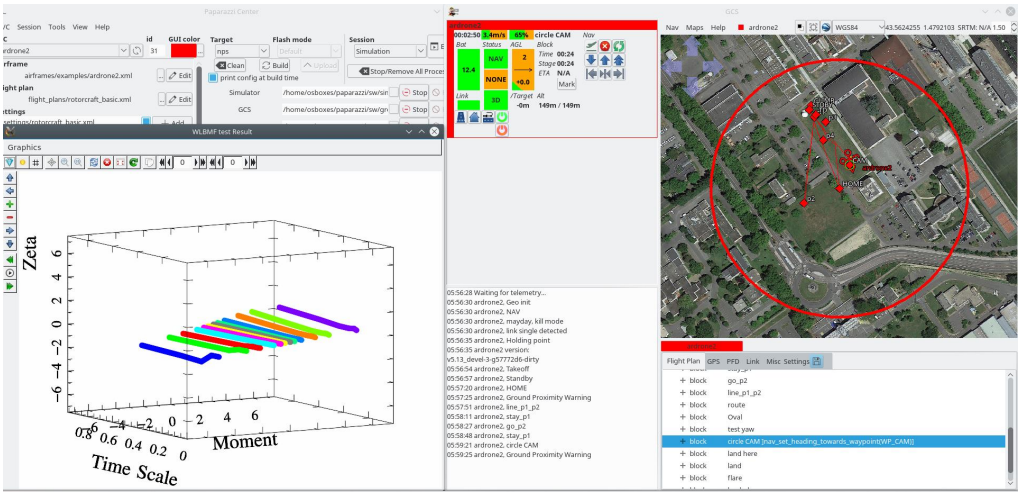


Figure 20: Simulated Real-time Application Scenario with Paparazzi Software

In the particular setup shown above in Figure 20, a sliding-window technique is applied: for a sampling window of 10 thousand samples, we extract 10 thousand previous samples upon the reception of each 1 thousand samples and perform the calculation of the signatures. Thus, for the duration of the sampling windows, we will have 10 frames of signatures. This allows us to avoid the possibility of losing resolution when the attack happens at the exact switching moment of two sampling windows. Also, this allows us to have a more continuously animated figure of the signatures and enables us to test the computation limit by increasing the window-sliding frequency.

It can be seen in Figures 21a, 21b and 21c, that the signatures of a flooded traffic have significantly lower zeta values than the ones of a normal traffic, especially at negative moments. It is also noted that the signatures vary depend on the packet data size. By default, HPing3 floods the target socket with empty packets, this will result in the most significant changes in the signatures (shown in Figure 21b),

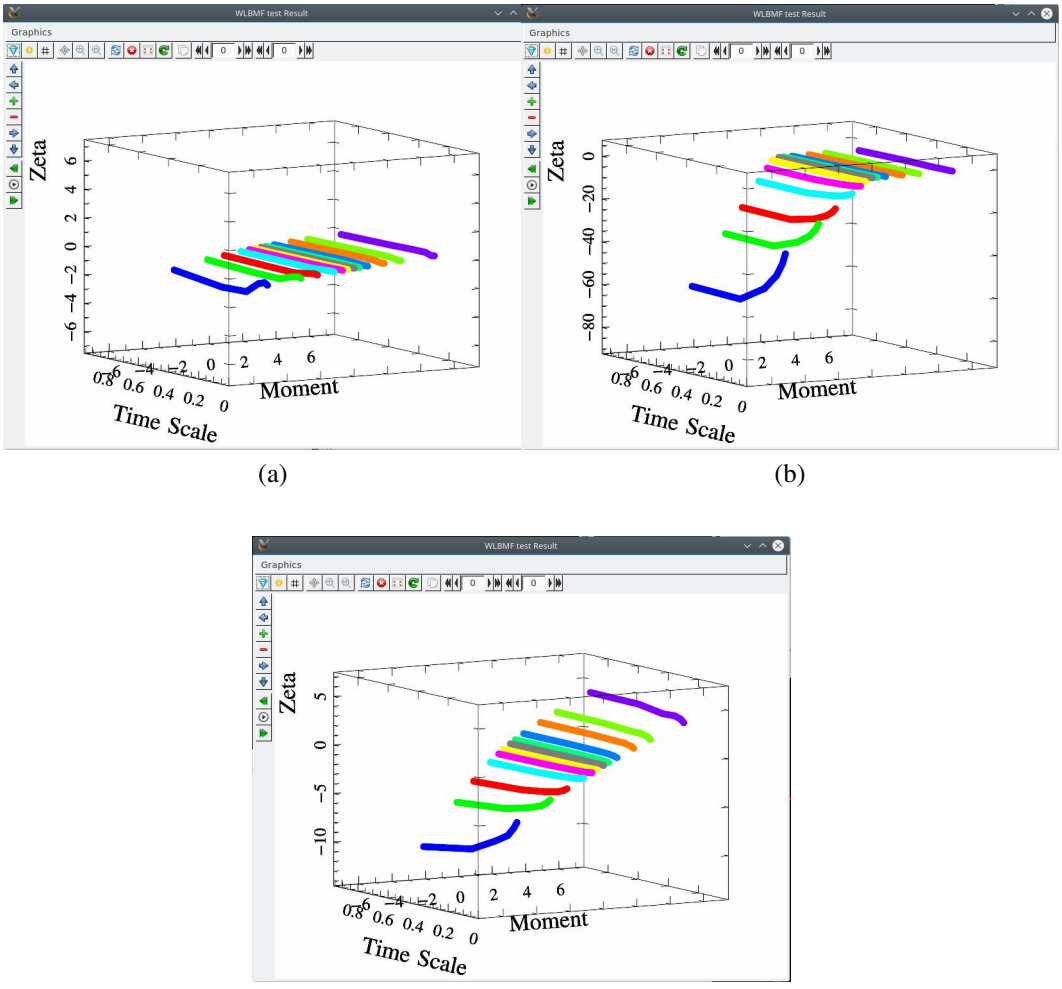


Figure 21: Real-time Signatures of (a) Normal Traffic (b) Traffic flooded with default packet payload data size=0 (c) Traffic flooded with packet payload data size=100

because this current implementation only takes into account message size of the packets received on the socket. The malicious empty packets will not impact the calculation directly but they hinder the normal packet transmission, hence result in a set of very different signatures. When the socket is subject to an attack which is filled with data, the signatures (shown in Figure 21c) show a more inclined pattern w.r.t. moment axis compare to the signatures of a normal traffic.

The real-time testings have provided us an intuitive knowledge of how WLM

analysis can help us to distinguish different types of attack. But how to tune the tool remains to be an open question. Especially, to best preserve the Long Range Dependency (LRD) characteristic of WLM analysis, a bigger sampling window must be chosen. But that will cost the real-time performance of the IDS system.

6. Conclusion and Future Work

In this paper, we have explained how a linear controller / observer can improve intrusion detection systems in the specific context of a 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 individually and can perform specific 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 Sections 3 and 4. Finally, Section 5 has demonstrated how a first version of real-time real-world based implementation of our IDS methodology can be realized.

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. Besides, we plan to investigate the characteristics of WLM analysis. Our previous experiments have indicated that the behavior of this method varies on the the choice of time scale, sampling period and moment. Future work will consider to perform more testing in real-world environments and to tune the different parameters in order to find the ones which provide us the best sensitivity. We also plan to test the impact of wavelet Long Range Dependency (LRD) on our specific case, because network traffic is one of the few signals which naturally possess this property. The question lays upon the realization of wavelet analysis in real-time while preserving its LRD characteristic. One possible solution would be to perform different wavelet analysis in order to get a wider window of observation and make an emphasis on the LRD of network traffic. In addition, we plan to investigate different methods to perform

pattern recognition on the different signatures. This is a crucial step to realize our methodology. There are already some well defined methods to achieve an accurate waveform / surface comparison including analytical methods as well as machine learning algorithms. A further step will be taken to test different methods in our specific case. At current stage, as a result of incompletion of development of the first designed step, we have found difficulties in defining the false positive rate of our proposed method, especially in the case of DDoS attack. New DDoS attack models, stealth/silent attacks described in [47] for instance, have made it increasingly difficult to distinguish DDoS attacks from normal traffic congestions. Our proposed method will have the benefit of exploiting information of the traffic in detail to aid future development of defense against DDoS attacks. 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 (Wireless signal jamming for example). Finally, we plan to investigate a way to implement and test this new generation intrusion detection system operating in a more complex real environment. To address this last objective, we would like to consider additional real experiments with an higher number of UAVs. Each UAV could embed its specific bank of models. Consequently, 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 a separated and isolated approach. We plan to perform this part of the research in the near future in the recently constructed UAV flight arena in ENAC, Toulouse, France.

[1] M. Rodrigues, D. F. Pigatto, J. V. C. Fontes, A. S. R. Pinto, J.-P. Diguet and K. R. L. J. C. Branco, "UAV Integration Into IoIT: Opportunities and Challenges," ICAS 2017, p. 95, 2017.

[2] İ. Bekmezci, O. K. Sahingoz and Ş. Temel, "Flying Ad-Hoc Networks (FANETs): A survey," Ad Hoc Networks, vol. 11, pp. 1254-1270, 2013.

[3] V. Sharma and R. Kumar, "A Cooperative Network Framework for Multi-UAV Guided Ground Ad Hoc Networks," Journal of Intelligent % Robotic Systems, vol. 77, pp. 629-652, 01 3 2015.

[4] W. T. L. Teacy, J. Nie, S. McClean and G. Parr, "Maintaining connectivity in UAV swarm sensing," in 2010 IEEE Globecom Workshops, 2010.

[5] R. Altawy and A. M. Youssef, ”Security, Privacy, and Safety Aspects of Civilian Drones: A Survey,” ACM Trans. Cyber-Phys. Syst., vol. 1, pp. 7:1–7:25, 11 2016.

[6] C. Rani, H. Modares, R. Sriram, D. Mikulski and F. L. Lewis, ”Security of unmanned aerial vehicle systems against cyber-physical attacks,” The Journal of Defense Modeling and Simulation, vol. 13, pp. 331-342, 2016.

[7] K. Hartmann and C. Steup, ”The vulnerability of UAVs to cyber attacks - An approach to the risk assessment,” in 2013 5th International Conference on Cyber Conflict (CYCON 2013), 2013.

[8] A. Kim, B. Wampler, J. Goppert, I. Hwang and H. Aldridge, ”Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles,” American Institute of Aeronautics and Astronautics, 2018.

[9] İ. Bekmezci, E. Şentürk and T. Türker, ”SECURITY ISSUES IN FLYING AD-HOC NETWORKS (FANETs),” Journal of Aeronautics and Space Technologies; Vol 9 No 2 (2016), 2016.

[10] A. Lakhina, M. Crovella and C. Diot, ”Diagnosing Network-wide Traffic Anomalies,” SIGCOMM Comput. Commun. Rev., vol. 34, pp. 219-230, 8 2004.

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

[12] V. Chandola, A. Banerjee and V. Kumar, ”Anomaly Detection: A Survey,” ACM Comput. Surv., vol. 41, pp. 15:1–15:58, 7 2009.

[13] A. Jøsang and G. Sanderud, ”Security in Mobile Communications: Challenges and Opportunities,” in Proceedings of the Australasian Information Security Workshop Conference on ACSW Frontiers 2003 - Volume 21, Darlinghurst, 2003.

[14] R. N. Akram, P. F. Bonnefoi, S. Chaumette, K. Markantonakis and D. Sauveron, ”Secure Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements,” in 2016 IEEE Trustcom/BigDataSE/ISPA, 23-2.

[15] H. Sedjelmaci, S. M. Senouci and M. A. Messous,”How to Detect Cyber-Attacks in Unmanned Aerial Vehicles Network?,” in 2016 IEEE Global Communications Conference (GLOBECOM), 4-8 .

[16] 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.

[17] P. Abry, D. Veitch and P. Flandrin, "Longrange Dependence: Revisiting Aggregation with Wavelets," Journal of Time Series Analysis, vol. 19, pp. 253-266.

[18] H. Wendt, "Contributions of Wavelet Leaders and Bootstrap to Multifractal Analysis: Images, Estimation Performance, Dependence Structure and Vanishing Moments. Confidence Intervals and Hypothesis Tests.," 2008.

[19] H. Wendt, P. Abry and S. Jaffard, "Bootstrap for Empirical Multifractal Analysis," IEEE Signal Processing Magazine, vol. 24, pp. 38-48, July.

[20] H. Wendt and P. Abry, "Multifractality Tests Using Bootstrapped Wavelet Leaders," IEEE Transactions on Signal Processing, vol. 55, pp. 4811-4820, Oct..

[21] H. Wendt, S. G. Roux, S. Jaffard and P. Abry, "Wavelet Leaders and Bootstrap for Multifractal Analysis of Images," Signal Process., vol. 89, pp. 1100-1114, 6 2009.

[22] 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.

[23] S. Rahm, Y. Labit and F. Gouaisbaut, "Sliding Mode Observer for Anomaly Detection in TCP/AQM Networks," in 2009 Second International Conference on Communication Theory, Reliability, and Quality of Service, 20-2.

[24] S. Rahm, Y. Labit, F. Gouaisbaut and T. Floquet, "Second order sliding mode observer for anomaly detection in TCP networks: From theory to practice," in 49th IEEE Conference on Decision and Control (CDC), 15-1.

[25] S. Rahm, Y. Labit, F. Gouaisbaut and T. Floquet, "Sliding Modes for Anomaly Observation in TCP Networks: From Theory to Practice," IEEE Transactions on Control Systems Technology, vol. 21, pp. pp. 1031-1038, 5 2013.

[26] T. Floquet, C. Edwards and S. K. Spurgeon, "On Sliding Mode Observers for Systems with Unknown Inputs," in International Workshop on Variable Structure Systems, 2006. VSS'06., 5-7 .

[27] 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

[28] Y. Ariba, F. Gouaisbaut, S. Rahme and Y. Labit, "Traffic monitoring in transmission control protocol/active queue management networks through a time-delay observer," IET Control Theory & Applications, vol. 6, pp. 506-517, Marc.

[29] K. K. Ramakrishnan and S. Floyd, "A Proposal to add Explicit Congestion Notification (ECN) to IP," RFC, vol. 2481, pp. 1-25, 1999.

[30] C.-K. Chen, Y.-C. Hung, T.-L. Liao and J.-J. Yan, "Design of robust active queue management controllers for a class of TCP communication networks," Information Sciences, vol. 177, pp. 4059-4071, 10 2007.

[31] S. Manfredi, M. Bernardo and F. Garofalo, "Robust output feedback active queue management control in TCP networks," in 2004 43rd IEEE Conference on Decision and Control (CDC) (IEEE Cat. No.04CH37601), 17-1.

[32] D. Wang and C. V. Hollot, "Robust analysis and design of controllers for a single TCP flow," in International Conference on Communication Technology Proceedings, 2003. ICCT 2003., 9-11.

[33] K. B. Kim, "Design of feedback controls supporting TCP based on the state-space approach," IEEE Transactions on Automatic Control, vol. 51, pp. 1086-1099, July.

[34] Y. Ariba, Y. Labit and F. Gouaisbaut, "Design and performance evaluation of a state-space based AQM," in International Conference on Communication Theory, Reliability, and Quality of Service, Bucharest, 2008.

[35] 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..

[36] E. A. F. Ihlen, ”Multifractal analyses of response time series: A comparative study,” Behavior Research Methods, vol. 45, pp. 928-945, 12 2013.

[37] A. Lakhina, M. Crovella and C. Diot, ”Diagnosing Network-wide Traffic Anomalies,” SIGCOMM Comput. Commun. Rev., vol. 34, pp. 219-230, 8 2004.

[38] S. H. Low, F. Paganini and J. C. Doyle, ”Internet congestion control,” IEEE Control Systems, vol. 22, pp. 28-43, Feb .

[39] R. Srikant, ”The Mathematics of Internet Congestion Control”. Birkhauser, 2004.

[40] S. Tarbouriech and al., ”Advances in communication Control Networks”. Springer, 2005.

[41] S. Floyd and V. Jacobson, ”Random early detection gateways for congestion avoidance,” IEEE/ACM Transactions on Networking, vol. 1, pp. 397-413, Aug .

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

[43] C. V. 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, Jun .

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

[45] J.-A. Maxa, G. Roudire and N. Larrieu, ”Emulation-Based Performance Evaluation of Routing Protocols for Uaanets,” in Nets4Aircraft 2015, Sousse, 2015.Nets4Cars/Nets4Trains/Nets4Aircraft 2015.

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

[47] A. Shevtekar and N. Ansari, ”Is it congestion or a DDoS attack?,” IEEE Communications Letters, vol. 13, pp. 546-548, July.