Design of a robust Controller/Observer for TCP/AQM network: First application to intrusion detection systems for drone fleet

Thierry Miquel, Jean-Philippe Condomines, Riad Chemali, Nicolas Larrieu

Design of a robust Controller/Observer for TCP/AQM network: First application to intrusion detection systems for drone fleet

Thierry Miquel[1], Jean-Philippe Condomines[1], Riad Chemali[2] and Nicolas Larrieu[2]

***Abstract*— This paper proposes a robust controller/observer for UAVs network anomaly estimation which is based on both Lyapunov Krasovkii functional and dynamic behavior of TCP (Transmission Control Protocol). Several research works on network anomaly estimation have been led using automatic control techniques and provide methods for designing both observer and command laws dedicated to time delay problem while estimating the anomaly or intrusion in the system. The observer design is based on a linearized fluid-flow model of the TCP behavior and must be associated to an AQM (Active Queue Management) to perform its diagnosis. The developed robust controller/observer in this paper has to be tuned by considering the time delay linear state-space representation of TCP model. As a first result, the designed controller/observer system has been successfully applied to some relevant practical problems such as topology network for aerial vehicles and the effectiveness is illustrated by using real traffic traces including Denial of Service attacks. Our first results show promising perspectives for Intrusion Detection System (IDS) in a fleet of UAVs.**

I. INTRODUCTION

The number and diversity of applications involving Unmanned Aerial Vehicles (UAVs) is growing every year. The necessary resort to use a fleet of versatile UAVs has led to an important interest from network community to design algorithms for Anomaly Detection Systems (ADS) or Intrusion Detection Systems (IDS) based on TCP (Transmission Control Protocol) network. Among abnormal patterns in TCP network [1], [2], [3] such as overload, flash crowds, worms, port scans, the malicious anomalies have the worst impact on the fleet of UAV by creating congestion and reducing significantly the Quality of Service (QoS) of the whole network. This is the worst case for UAV certification and integration into civil airspace. That is the reason why, nowadays, malicious anomaly detection is an important issue. In [3] an overview is provided spanning multiple research areas and application domains.

Network anomalies and security-related problems (such as Distributed Denial of Service (DDoS) attacks) is an important issue of active security threats detection. A variety of tools for anomaly detection are mainly based on data packet signature. This behavior is fully operational with well known DDoS attacks. However, this mechanism is inefficient when a new type of attack is performed. For such a reason, we are designing in this paper a new type of IDS able to detect different type of DDoS. The detection model is based on a traffic characterization analysis (performed through an automatic control estimation). All types of attacks which are not following the initial automatic control estimation trigger an alarm and consequently, the malicious traffic can be analysed in details. This automatic control based approach has the main advantage not to be associated to a specific type of attacks. Any attacks which are not following the initial model can be analysed, detected and managed. The security and performances of the whole network are then improved.

Exploiting the capabilities of observers or estimators allows, by generating consolidated signals, to extend the way malicious intrusion can be controlled while enhancing fleet of UAVs intrinsic flight handling qualities. Among the nonlinear methods [4] the Super-Twisting Algorithm (STA) [6], [7], [8] 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 [5] which are often used to design robust nonlinear observers or control laws. Unfortunately, building upon this peculiar observer provides for bounded input-bounded state (BIBS) finite-time stability only [9] restricting 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 dynamical systems such as 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 [10] is based on both Lyapunov Krasovkii 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 (AQM) consists in adjusting data flow rates sent by the UAV into the network. The principle consists in dropping (or marking when ECN, Explicit Congestion Notification [11] option is enabled) some packets before buffer saturates. Consequently, the estimator must be associated to a robust AQM to perform its diagnosis. The study of congestion control in a time delay system framework is not new and has been successfully [13], [14], [15], [16] exploited. A relevant constructive algorithm [17] has been proposed.

The contribution of this paper is to propose a robust controller/observer algorithm able to detect traffic anomalies (i.e. DDoS). This algorithm has been designed and tested

Thierry Miquel and Jean-Philippe Condomines are with the ENAC Laboratory, Department of Applied Mathematics, Computer Science and Automatics For Air Transport, ENAC University, BP 54005, Toulouse Cedex 4, 31055, France Thierry.miquel@enac.fr, Jean-Philippe.condomines@enac.fr

Riad Chemali and Nicolas Larrieu are with the ENAC Laboratory, Telecom Research Department, ENAC University, BP 54005, Toulouse Cedex 4, 31055, France Nicolas.larrieu@enac.fr, riad.chemali@recherche.enac.fr

in real traffic conditions. Indeed, the simulink design and its theoretical evaluation have been confronted to real traffic traces. These traces have been generated thanks to an hybrid UAV network simulator. Consequently, the validation of the theoretical estimator is improved by testing its behavior with real DDoS attacks, real UAV trajectories, real UAV background traffic and real UAV fleet topology. Guided by the Lyapunov theory, we propose to develop a design to determine all correction terms associated with time delay linear state-space representation of TCP model. In the sequel, §II presents the basics of the modelling 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. §III presents the theoretical background of our proposed controller/observer system. Finally, §IV gathers all the results obtained after solving the time delay linear estimation problem in real conditions.

II. Dynamical System Modeling

In order to tackle a wide range of applications, various implementations of TCP models in terms of assumptions and numerical techniques [18], [19], [20] exist. TCP network is commonly represented using a linearized fluid-flow model [18] associated with our network topology. As shown in Figure 1 this 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 modelling from scratch.

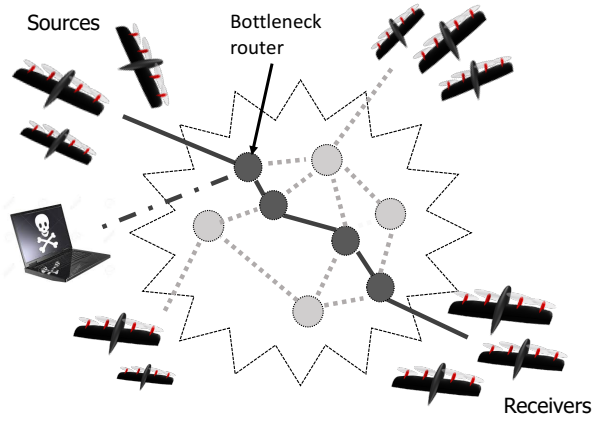

Fig. 1. Sources/receivers connection in a fleet of UAVs

The bottleneck link is shared by N flows and TCP applies the congestion avoidance algorithm described in [21] for example. To recover an Intrusion Detection System (IDS) accuracy using the network topology presented before, it is necessary to use, if possible, additional instruments (e.g. probability of packet, queue of the router buffer) and a 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 mathematically described as follows:

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

In the first differential equation, $W(t)$ represents the TCP window size, $\tau(t)$ the round trip time (RTT) which can be modelled by 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 depends whether 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 modelled by an additional signal $d(t)$ mixed with the regular traffic passing through the router and filling the buffer.

The nonlinear 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. Moreover, a linearization of $\mathcal{M}_s$ was carried out in [24] to allow the use of traditional control theory approaches. The fluid-flow model of TCP now becomes :

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

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 [10] the dynamics of the queue and the congestion window are modelled to address delay issue. Indeed time delay is an intrinsic phenomenon in networks whose control should improve the precision of $\delta\mathcal{M}_s$. 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:

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

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 [22] which is an extension of the traditional Lyapunov theory. It is an effective and practical method which provides LMI (Linear Matrix Inequalities [23]) criteria easy to test.

III. Controller/Observer Design for an IDS

Recent progresses in congestion control systems such as AQM have been led to achieve hight efficiency and reliability of communications in computer networks. Under conditions where a malicious intrusion is not present, various mechanisms exist in the literature such as Random Early Detection [25] (RED), Random Early Marking [26] (REM) and more recently using control theory (proportional and proportional integral controller [27] or state feedback controller [28]). As shown in Figure 2 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).

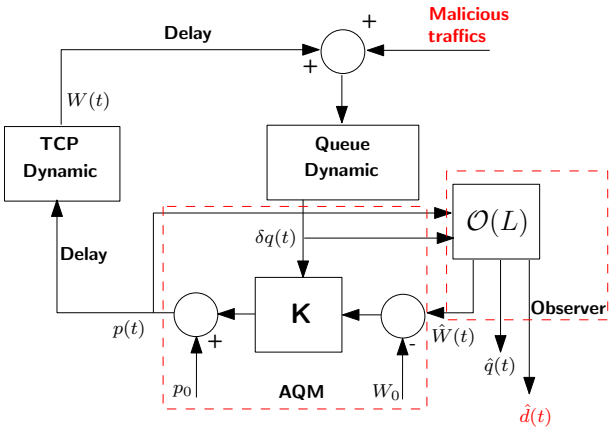

Fig. 2. Introduction of an additional TCP traffic as anomaly

A major issue in the certificating of a fleet of UAVs is to estimate the malicious intrusion while taking into account a level of QoS (i.e., the drop probability $p(t)$). In that way, the non modelled malicious traffic $d(t)$ has to be estimated. The estimator has to be designed in addition to an efficient AQM. Thus, we propose to design a robust controller/observer for IDS by solving an LMI criteria on the following augmented model:

$$\delta\mathcal{M}_s^+ \begin{cases} \delta\dot{\underline{\tilde{x}}}(t) &= \bar{\mathbf{A}}\delta\underline{\tilde{x}}(t) + \bar{\mathbf{A}}_d\delta\underline{\tilde{x}}(t-\tau(t)) \\ & \quad + \bar{\mathbf{B}}\delta p(t-\tau(t)) \\ y(t) &= \bar{\mathbf{C}}\delta\underline{\tilde{x}}(t) \end{cases} \tag{7}$$

With

$$\begin{cases} \bar{\mathbf{A}} = \begin{bmatrix} \mathbf{A} & & 0 \\ & & 1 \\ 0 & 0 & 0 \end{bmatrix} \\ \bar{\mathbf{A}}_d = \begin{bmatrix} \mathbf{A_d} & & 0 \\ & & 0 \\ 0 & 0 & 0 \end{bmatrix} \\ \bar{\mathbf{B}} = \begin{bmatrix} \mathbf{B} \\ 0 \end{bmatrix} \\ \bar{\mathbf{C}} = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \end{cases} \tag{8}$$

where $\delta\underline{\tilde{x}}(t)^T = [\delta W(t)\ \ \delta q(t)\ \ d(t)]^T$ represents the augmented state. Practically, the objective is to reconstruct the whole state of Eq. (7), in particular the non-TCP malicious flows modelled by $d(t)$, and design an output feedback AQM. Consequently, we are looking for gain controller $\mathbf{K}$ and gain observer $\mathbf{L}$ defined as:

$$\begin{cases} \delta u(t-\tau(t)) &= -\mathbf{K}y(t) = -\mathbf{KC}\delta\underline{x}(t) \\ \delta\dot{\underline{\hat{x}}}(t) &= \bar{\mathbf{A}}\delta\underline{\hat{x}}(t) + \bar{\mathbf{A}}_d\delta\underline{\hat{x}}(t-\tau(t)) \\ & \quad + \bar{\mathbf{B}}\delta u(t-\tau(t)) \\ & \quad + \mathbf{L}\left(y(t) - \mathbf{C}\delta\underline{\hat{x}}(t)\right) \end{cases} \tag{9}$$

The first equation corresponds to the dynamics of the AQM. We assume that the time-delayed system described by Eq. (4) is controlled by a static output feedback AQM such as the dynamics of the closed loop system is the following:

$$\delta\dot{\underline{x}}(t) = \mathbf{A}_{cl}\delta\underline{x}(t) + \mathbf{A}_d\delta\underline{x}(t-\tau(t)) \tag{10}$$

where:

$$\mathbf{A}_{cl} = \mathbf{A} - \mathbf{BKC} \tag{11}$$

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 stable the dynamics of the estimation error $e(t)$.

Combining all these results, a direct and analytical design of the observer can be proposed thanks to the error between the state of the system $\delta\underline{x}(t)$ and its estimated value $\delta\underline{\hat{x}}(t)$:

$$\underline{e}(t) = \delta\underline{\hat{x}}(t) - \delta\underline{x}(t) \tag{12}$$

Thus, the dynamics of the estimation error is the following:

$$\dot{\underline{e}}(t) = \mathbf{A}_{cl}\underline{e}(t) + \mathbf{A}_d\underline{e}(t-\tau(t)) \tag{13}$$

where:

$$\mathbf{A}_{cl} = \mathbf{A} - \mathbf{LC} \tag{14}$$

The dynamics of the estimation error $e(t)$ given by Eq. (13) in the observer problem is similar to the dynamics of the closed loop state vector $\delta\underline{x}(t)$ given by Eq. (10) in the controller problem assuming $\mathbf{B} = \mathbb{I}$ and $\mathbf{K} = \mathbf{L}$. This enables to use the same methodology for the observer and the controller design to determine all correction terms associated with the time delay linear state-space representation of TCP model. By using the theorem in annexes which introduces an appropriate Lyapunov Krasovskii functional, the following methodology gives a simple way to construct unknown matrices $\mathbf{K}$ and $\mathbf{L}$ in order to stabilize Eq. (13):

1) Use a static output feedback [30] for the AQM to compute the static output gain matrix $\mathbf{K}$ corresponding to a set of predefined eigenvalues of the closed loop state matrix $\mathbf{A}_{cl}$;
2) Check the robustness of the proposed design by solving the following LMI:

$$\begin{cases} \mathbf{P} = \mathbf{P}^T > \mathbf{0} \\ \mathbf{Q} = \mathbf{Q}^T > \mathbf{0} \\ \mathbf{R} = \mathbf{R}^T > \mathbf{0} \\ \begin{bmatrix} \mathbf{\Gamma}_{11} & \mathbf{\Gamma}_{12} \\ \mathbf{\Gamma}_{12}^T & \mathbf{\Gamma}_{22} \end{bmatrix} < \mathbf{0} \end{cases} \tag{15}$$

where:

$$\begin{cases} \overline{\tau} & = \sup_t(\tau(t)) \\ \mathbf{\Gamma}_{11} & = \mathbf{A}_{cl}^T\mathbf{P} + \mathbf{P}\mathbf{A}_{cl} + \mathbf{Q} - \frac{1}{\overline{\tau}}\mathbf{R} + \overline{\tau}\mathbf{A}_{cl}^T\mathbf{R}\mathbf{A}_{cl} \\ \mathbf{\Gamma}_{12} & = \mathbf{P}\mathbf{A}_d + \overline{\tau}\mathbf{A}_{cl}^T\mathbf{R}\mathbf{A}_d + \frac{1}{\overline{\tau}}\mathbf{R} \\ \mathbf{\Gamma}_{22} & = -\mathbf{Q} + \overline{\tau}\mathbf{A}_d^T\mathbf{R}\mathbf{A}_d - \frac{1}{\overline{\tau}}\mathbf{R} \end{cases} \tag{16}$$

3) The solving of LMI in Eq. (15) has to be done also for $\mathbf{L}$ in order to design the observer.

Such an approach is systematic for more complex dynamical systems than the ones represented by a single router.

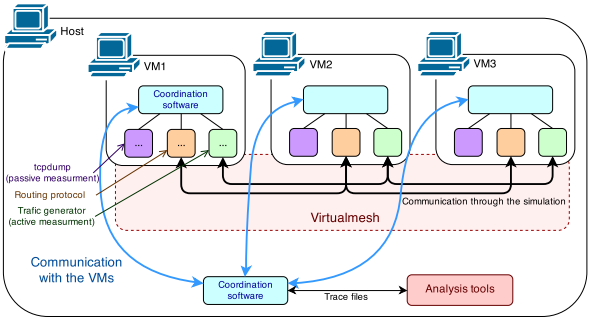

Fig. 3. Testbed implementation

IV. Controller/Observer validation in real traffic conditions

A. Hybrid UAV network simulator

In order to validate the new traffic estimator in real traffic conditions, we use a hybrid experimental system to combine the low cost of a simulation with the accuracy of a real protocol stack. We use virtual machine implementations to deal with the entire complexity of Linux operating system. The traces used to generate UAVs mobility patterns were extracted from real traces so that physical related factors could be as realistic as possible. The system we used to evaluate protocols is divided in several parts. It includes a set of tools that can fit to several scenarios: an 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 depicted in Figure 3. In [29] more details about this hybrid tool can be found.

The main advantage using such an hybrid simulator is to extract any characteristics from the simulation and to inject them in the Simulink design directly. The theoretical model is then confronted to real traffic characteristics and not only theoretical stimulus that are pertinent for a first stage evaluation but that do not take into account the huge variability of real traffic. Consequently, we have been able to generate DDoS between the different virtual machines considering the exact UAV environment of the drone mission we have considered in section II. Then, we captured the network traffic generated (both regular traffic and the DDoS traffic) and finally, we have injected this traffic in the Simulink design.

B. Experimental results

We now illustrate the performances reached by the developed controller/observer on the basis of hybrid UAV network simulator. As it was aforementioned, the normal TCP traffic is generated by 5 TCP sources generating long lived TCP flows to a receiver through a router with a link capacity C=1250 packets/s (which is equivalent to 3Mbit/s), and $T_p = 30ms$ the propagation delay. This is illustrated in Figure 4.

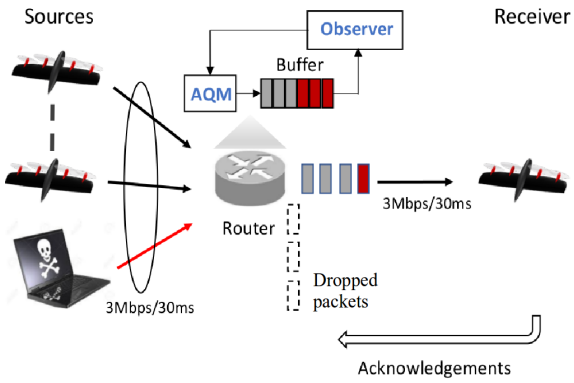

Fig. 4. Considered topology

Moreover, we define in the Table below the values of the congestion window size and the queue length at the equilibrium of the system, i.e. W_0 and q_0 from 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 [10] and observer gains are $\mathbf{L} = [0.024, 1.598, 20.978]^T$. First of all, we present the TCP congestion window $W(t)$ in Figure 5 for which the differences between linear and nonlinear models may be wrong. Indeed, we can observe a slightly influence on the linearized model when $W(t)$ goes down and up strongly (i.e. far from its equilibrium point).

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

In Figures 5, 6 and 7 we illustrate a typical realization of traffic including four different traffic anomalies which can be detected by our time-delay linear observer. The four different intrusions generated by the hybrid simulation tool have been injected in Simulink to confront our IDS model to the real traffic traces. These anomalies have been generated using the HPing3 tool. This software is run on the hacker node (see Figure 4 for details about the network topology simulated) and can run different types of attack (but mainly flooding attacks). In our scenario, HPing3 exchanges thousand of small TCP flows in order to generate a SYN flood attack on the receiver node. The resulting malicious traffic is quite more important than the regular traffic. This is decribed in the Figure 7 where regular traffic is around 50 pkt/s when, for the malicious traffic, the throughput is increased to 150 pkt/s. Then, the real traffic (blue) and estimated intrusion (orange) are plotted on the same figure in order to be compared. Figure 6 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 do not affect the different steady states of the system.

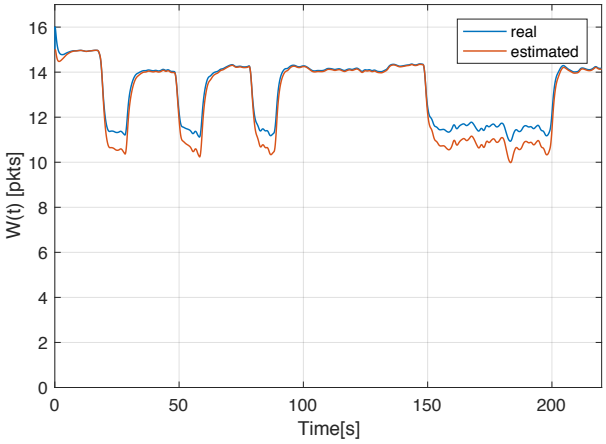

Fig. 5. TCP congestion window W(t)

These results are positive 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 difference between legitimate traffic and intrusion traffic. This is a first promising result for intrusion detection system design applied to drone fleet network.

V. Conclusion and Future Work

With this paper, we demonstrate that a linear controller/observer can improve intrusion detection systems in the specific context of drone fleet. Our design methodology provides a simple way to construct and instantiate our gain matrices for both the AQM controller and the observer. This approach give us first promising results with a simple topology (within a time-delay framework). We plan to apply this approach also in the context of more dynamical systems (such as fleet of drones) where several nodes are involved in the network topology in order to build an ad hoc network.

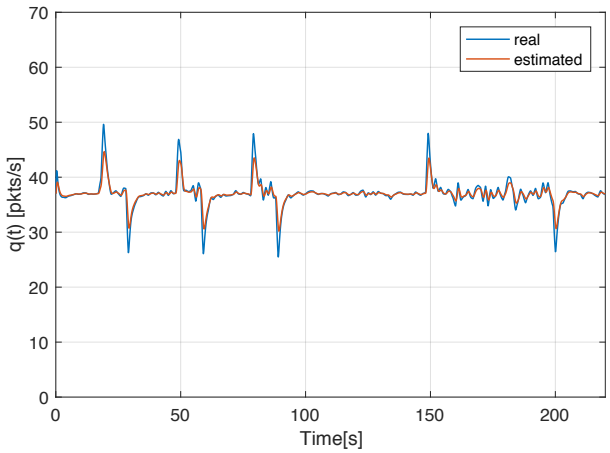

Fig. 6. Queue length q(t)

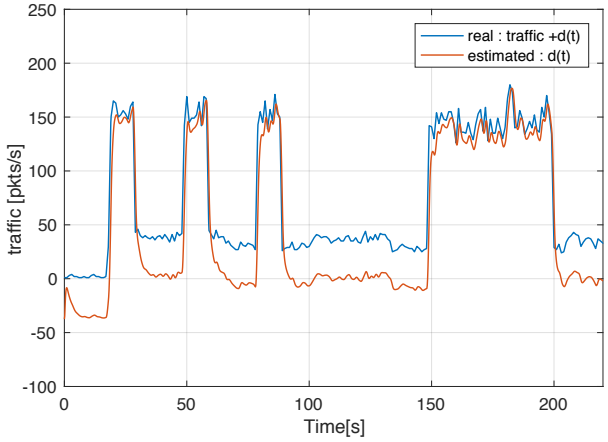

Fig. 7. Estimation with real traffic replay

In our future work we can identify several contributions. First of all, we plan to propose an evolution of the modelling of 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 analyse different types of attack: not only DDoS but also intrusion where the traffic generated in the network is less consistent and then more difficult to detect. A first solution would be to consider a 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 of traffic estimator in real system and real environment. To address this last objective, we would like to consider real experiments with real UAV. Each UAV could integrate the bank of models previously introduced and by

conducting a collaborative mission in the context of a UAV fleet we could test and validate the theoretical estimators validated only in simulations.

VI. Annexes

Theorem 1: For given $\overline{\tau} = \sup_t(\tau(t))$ and $\alpha > 0$, if there exists two definite positive matrices, $\mathbf{W} = \mathbf{PL}$ and $\mathbf{R} = \alpha\mathbf{P}$ of appropriate dimension such that the following LMI holds

$$\begin{cases} \mathbf{P} = \mathbf{P}^T > \mathbf{0} \\ \mathbf{Q} = \mathbf{Q}^T > \mathbf{0} \\ \begin{bmatrix} \mathbf{\Phi}_{11} & \mathbf{\Gamma}_{12} & \mathbf{\Phi}_{12} \\ \mathbf{\Gamma}_{12}^T & \mathbf{\Gamma}_{22} & \mathbf{0} \\ \mathbf{\Phi}_{12}^T & \mathbf{0} & -\mathbf{P} \end{bmatrix} < \mathbf{0} \end{cases} \tag{17}$$

with:

$$\begin{cases} \mathbf{\Phi}_{11} = \mathbf{A}^T\mathbf{P} - \mathbf{C}^T\mathbf{W}^T + \mathbf{PA} - \mathbf{WC} + \mathbf{Q} - \frac{\alpha}{\overline{\tau}}\mathbf{P} \\ \mathbf{\Gamma}_{12} = \mathbf{PA}_d + \overline{\tau}\alpha\left(\mathbf{PA} - \mathbf{WC}\right)^T\mathbf{A}_d + \frac{\alpha}{\overline{\tau}}\mathbf{P} \\ \mathbf{\Phi}_{12} = \sqrt{\overline{\tau}\alpha}\left(\mathbf{PA} - \mathbf{WC}\right)^T \\ \mathbf{\Gamma}_{22} = -\mathbf{Q} + \overline{\tau}\alpha\mathbf{A}_d^T\mathbf{PA}_d - \frac{\alpha}{\overline{\tau}}\mathbf{P} \end{cases} \tag{18}$$

then the system defined by Eq. (13) is asymptotically stable and the observer gain is given by $\mathbf{G} = \mathbf{P}^{-1}\mathbf{W}$.

References

[1] A. Lakhina and al., Diagnosing network-wide traffic anomalies, in ACM SIGCOMM, Portland, 2004, pp. 219-230.

[2] A. Hussain ans al. A framework for classifying denial of service attacks, in SIGCOMM, Karlsruhe, Germany, Aug 2003, pp. 99-110.

[3] V. Chandola and al., Anomaly detection: A survey, ACM Comput. Surv., vol. 41, no. 3, pp. 1-58, 2009.

[4] 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. 393-395.

[5] 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. 638-656, 2007.

[6] S. Rahme ÌĄ,and al., Sliding mode observer for anomaly detection in TCP/AQM networks, in Communication Theory, Reliability, and Quality of Service, 2009. CTRQ âĂŹ09. Second International Conference on, 20-25 2009, pp. 113 -118.

[7] S. Rahme ÌĄ, 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.

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

[9] C. Edwards, and al., Advances in Variable Structure and Sliding Mode Control, Lecture Notes in Control and Information Science, Springer-Verlag, Berlin (2006), pp. 271-292

[10] 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.

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

[12] A. Papachristodoulou, Global stability of a TCP/AQM protocol for arbitrary networks with delay, in IEEE CDC 2004, Dec. 2004, pp. 1029-1034.

[13] 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. 4059-4071, 2007.

[14] 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.

[15] D. Wang and C. V. Hollot, Robust analysis and design of controllers for a single TCP flow, in IEEE International Conference on Communication Technology (ICCT), vol. 1, Apr. 2003, pp. 276-280.

[16] 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.

[17] 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. 89-94.

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

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

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

[21] V. Jacobson, Congestion avoidance and control, in ACM SIG- COMM, Stanford, CA, Aug. 1988, pp. 314-329.

[22] K. Gu, V. L. Kharitonov, and J. Chen, Stability of Time-Delay Systems. Birkhauser Boston, 2003, control engineering.

[23] S. Boyd and al., Linear Matrix Inequalities in System and Control Theory. Philadelphia, USA:SIAM, 1994, in Studies in Applied Mathematics, vol.15.

[24] 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. 151-160.

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

[26] S. Athuraliya and al., An enhanced random early marking algorithm for internet flow control, in IEEE INFOCOM, Dec. 2000, pp. 1425-1434.

[27] C. V. Hollot and al., Analysis and design of controllers for AQM routers supporting TCP flows, IEEE Trans. on Automat. Control, vol. 47, pp. 945-959, Jun. 2002.

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

[29] 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.

[30] Syrmos V.L. and al., Static Output Feedback: a Survey, Proceedings of the 33rd IEEE Conference on Decision and Control, 1994