Frequency-based detection of replay attacks: application to a quadrotor UAV

Conference Paper · October 2019

DOI: 10.1109/ICSC47195.2019.8950619

Damiano Rotondo
Spanish National Research Council

Joseba Quevedo
Universitat Politècnica de Catalunya

Frequency-based detection of replay attacks: application to a quadrotor UAV

Helem S. Sánchez, Damiano Rotondo, Marc López Vidal, Joseba Quevedo

***Abstract*— Unmanned aerial vehicles (UAVs) are reported to be highly exposed as possible targets of cyber attacks, due to their strong strategic and economic value, and their increasing use in a wide range of operations. Among the most critical cyber attacks, replay attacks are performed by replacing the real data coming from the sensors with previously recorded data, causing deterioration of the control system's performance and potentially allowing other types of attacks without being discovered. The main contribution of this paper is to investigate the applicability of a frequency-based detection method, which uses a sinusoidal signal with a time-varying frequency as authentication signal, to a UAV affected by replay attacks. The effectiveness of the method is illustrated through simulation scenarios.**

I. Introduction

In recent years, the increasing integration of cyber (computation, communication, etc.) and physical processes has led to the introduction of a new class of systems, known as *cyber-physical systems* (CPSs) [1]. CPSs are characterized by a higher efficiency, but also by bigger vulnerabilities, which can be exploited by a malicious agent in order to perform a cyber attacks, resulting in some kind of damage or economical loss [2], [3].

Unmanned aerial vehicles (UAVs) are reported to be highly exposed as possible targets of cyber attacks, due to their strong strategic and economic value, and their increasing use in a wide range of operations, such as border surveillance, reconnaissance, transport, and even civilian tasks, as e.g. fun by hobby enthusiasts [4]. Among the attacks reported for UAVs, we recall the one performed in 2012 during a flight test in South Korea, in which a GPS jamming attack was executed on a S-100 Camcopter, resulting in a crash into the ground control van, which lead to the killing of an engineer and the injuring of two remote pilots [5].

Due to the importance of assessing the vulnerabilities of UAVs, and developing new defense mechanisms, which could help in mitigating them, simulations of cyber attacks on UAVs are being executed [6]. [7] performed a GPS spoofing attack on a quadrotor, resulting in the UAV landing at an incorrect location. A deauthentication attack on a quadrotor was used by [8] to demonstrate its vulnerability, resulting in the loss of control by the operator. The work [9] showed that a hacker can exploit shared data and predictable collision avoidance properties in order to control and alter the UAV's trajectory.

Among the most critical cyber attacks, there are the *replay attacks*. When an attack of this type is carried out, at first the attacker records the measurements coming from the sensors. Later, the attacker replaces the real data with the recorded one, causing deterioration of the control system's performance and potentially allowing other types of attacks without being discovered. The threats to the security of UAVs brought by this type of attack have been well documented, see e.g. [10], [11]. In the last few years, different approaches have been proposed to detect these attacks, which may be classified roughly into two categories: i) watermarking-based approaches [12]–[16], in which an authentication signal is added to the control signal (at the cost of sacrificing the control performance), and the received sensor measurements are analyzed to check whether there is or there is not the effect of the authentication signal on the physical system; and ii) alternative methods [17], [18], which try to detect replay attacks without injecting signals in the control input.

The work [16] presented a method to detect replay attacks using a frequency-based signature, which was applied to a multiple tank system. The main contribution of the present paper is to investigate its applicability to a UAV affected by replay attacks. In particular, the method introduces a sinusoidal signal with a time-varying frequency (authentication signal) into the closed-loop system, and checks whether the time profile of the frequency components in the output signals are compatible with the authentication signal or not, by comparing the energies of appropriate signals.

The remaining of the paper is structured as follows. In Section II, the frequency-based replay attack detection technique is presented. Section III describes the application of the proposed method to a quadrotor. Section IV presents the simulation results. Finally, Section V provides the conclusions.

II. Replay attack detection method

A. Attack definition and overview of the detection method

Replay attacks corrupt the measurements coming from the sensors, and are carried out in two stages [12]:

1) in the first stage, the attacker records sensor data $y(t)$ in a time window $[t_0, t_0 + w]$, where w denotes the attack duration, without compromising their integrity;

This work has been partially funded by the Spanish State Research Agency (AEI) and the European Regional Development Fund (ERFD) through the projects SCAV (ref. MINECO DPI2017-88403-R) and DEOCS (ref. MINECO DPI2016-76493), and also by AGAUR ACCIO RIS3CAT UTILITIES 4.0 – P7 SECUTIL. This work has been also supported by the AEI through the Maria de Maeztu Seal of Excellence to IRI (MDM-2016-0656) and the grant Juan de la Cierva-Formacion (FJCI-2016-29019).

The authors are with the Research Center for Supervision, Safety and Automatic Control (CS2AC) of the Universitat Politècnica de Catalunya (UPC), Spain. D. Rotondo is also with the Institut de Robòtica i Informàtica Industrial, CSIC-UPC , Llorens i Artigas 4-6, 08028 Barcelona, Spain.

2) in the second stage, the recorded data are used to replace the real data, such that the controlled system is exposed to some kind of harm without the supervisory unit/agent being aware of it, e.g., the system could be driven to a different operating point, or some act of theft/sabotage could be performed.

Hereafter, we recall the method proposed in [16], which detects replay attacks (also identifying which output channels are being attacked) by introducing a sinusoidal signal with a time-varying frequency into the system. Then, the detector makes a decision by checking if the measured output is compatible with the introduced signature or not. More specifically, by applying a dynamical decoupling technique based on *vector fitting* [19], it can be ensured that a given input channel will affect only an output channel, which allows identifying which channel is being attacked. Finally, the detector compares the energies of band-pass signals to determine if a replay attack is being carried out or not.

B. Signal generation

Let us consider a continuous-time linear time invariant system:

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{1}$$

$$y(t) = Cx(t) \tag{2}$$

where $x \in \mathbb{R}^n$ is the state, $u \in \mathbb{R}^m$ is the input, $y \in \mathbb{R}^p$ is the output, and A, B, C denote matrices of appropriate dimensions. The system (1)-(2) is controlled by means of a state-feedback control law:

$$u(t) = -Kx(t) \tag{3}$$

such that the closed-loop system is described by:

$$\dot{x}(t) = (A - BK)x(t) \tag{4}$$

The frequency-based method for replay attack detection introduces a signature $\varsigma(t)$ into the input $u(t)$, such that:

$$u(t) = -Kx(t) + \varsigma(t) \tag{5}$$

It is straightforward to see that $\varsigma(t)$ will affect the output $y(t)$ according to the transfer function:

$$G(s) = C\left(sI - A + BK\right)^{-1} B \tag{6}$$

which usually contains coupling, i.e. a signature signal $\varsigma_i(t)$ introduced in the i-th input channel will contribute to the response of all the output signals contained in $y(t)$. Since we would like to use the signature signals to identify which channel is affected by the replay attack, we introduce a decoupler $F(s)$ with input $\tilde{\xi}(t)$ and output $\varsigma(t)$, such that the series interconnection $G_d(s) = G(s)F(s)$ is a decoupled system, i.e. made up by a diagonal transfer matrix. Then, we can introduce frequency-varying sinusoidal signals:

$$\tilde{\xi}_i = \tilde{\alpha}_i \cos\left(\omega_{\sigma_i(t)} t\right) \quad i = 1, \ldots, m \tag{7}$$

into the decoupler, where $\tilde{\alpha}_i$ denotes the signals' magnitudes, and $\sigma_i(t)$ denote piecewise constant signals, taking integer values between 1 and N, such that at each instant of time $\omega_{\sigma_i(t)}$ take values within a set of predetermined frequencies $\{\omega_1, \ldots, \omega_N\}$, according to the value of $\varsigma_i(t)$. The idea behind introducing (7) is that by analyzing the output signals, we can decide about the attack occurrence by checking if the received output is compatible with the introduced signals or not.

It is clear that, since a complete decoupling of $G(s)F(s)$ is very demanding, and in some cases cannot be achieved at all [20], we can require decoupling for the finite set of frequencies ω_i, $i = 1, \ldots, N$. More specifically, by requiring that $F(\imath\omega_i) = G(\imath\omega_i)^{-1}$, a set of N constraints that the decoupler should satisfy is obtained. Then, the robust numerical method for rational approximation known as *vector fitting* can be applied [21].

C. Detection logic

The output signal $y(t)$ will contain the effects of the different inputs to the process, e.g. the input signal $u(t)$. With the aim of analyzing only the content due to the signature signal $\tilde{\tilde{\xi}}(t)$, $y(t)$ is processed through a bank of band-pass filters (each filter corresponding to a different frequency ω_i, $i = 1, \ldots, N$), whose transfer functions are obtained as follows [22]:

$$H_i(s) = diag\left\{\frac{\frac{\omega_i}{Q_i}s}{s^2 + \frac{\omega_i}{Q_i}s + \omega_i^2}\right\} \tag{8}$$

where Q_i is the selectivity of the filter, bigger values of which correspond to a narrower frequency response, but also a slower dynamic response.

Let us denote as $z_{il}(t)$ the output of the filter $H_i(s)$ fed by $y_l(t)$. Then, we can obtain an estimate $\hat{\sigma}_l(t)$ of $\sigma_l(t)$ by comparing the different signals $z_{il}(t)$. As proposed in [16], a possible way to obtain $\hat{\sigma}_l(t)$ is to compare the energies of $z_{il}(t)$ over the largest period associated with the frequencies ω_i:

$$T_\omega = \max_{i=1,\ldots,N} \frac{2\pi}{\omega_i} \tag{9}$$

while also taking into account the time t_{trans} needed after a switch in $\sigma_l(t)$ in order for the transient to become neglectable. Then, the signals $\hat{\sigma}_l(t)$ are calculated as (10) (see top of the next page), where $t_s^* = \lfloor t/T_s \rfloor T_s$ denotes the last switching time. Then, the replay attack detection algorithm will compare the known signals $\sigma_l(t)$ with the estimated signals $\hat{\sigma}_l(t)$. If a mismatch is found, the algorithm will warn about $y_l(t)$ being corrupted by a replay attack.

III. Application to a quadrotor

In this section, we present the application of the frequency-based replay attack detection method to a quadrotor.

A. Linearized model

The quadrotor is a vehicle that has four rotors in a cross configuration. Two rotors can rotate in a clockwise direction, while the other two can rotate anticlockwisely. The four rotors are controlled independently, and their speeds affect the overall movement of the quadrotor. It is assumed that the quadrotor has a rigid and symmetrical structure, with

$$\hat{\sigma}_l(t) = \begin{cases} \sigma_l(t) & if\ \sigma_l(t) \neq \sigma_l(t-T_s) \wedge t \in [t_s^*, t_s^* + t_{trans} + T_\omega] \\ \arg \max\limits_{i=1,\dots,N} \int\limits_{t-T_\omega}^{t} |z_{il}(\tau)|^2 d\tau & \text{otherwise} \end{cases} \tag{10}$$

center of gravity that coincides with the body fixed frame, and rigid propellers, which provide thrust and drag forces that are proportional to the square of the propellers' speeds.

Let us introduce the state vector $x = \left[z, \dot{z}, \phi, \dot{\phi}, \theta, \dot{\theta}, \psi, \dot{\psi}\right]^T$ and the input vector $u = [\Omega_1, \Omega_2, \Omega_3, \Omega_4]^T$, where z is the height, ϕ, θ, ψ are the roll, pitch and yaw angle, respectively, and $\Omega_1, \Omega_2, \Omega_3, \Omega_4$ are the rotor speeds. By applying a constant feedforward input $u_e = [\Omega_{1,e}, \Omega_{2,e}, \Omega_{3,e}, \Omega_{4,e}]^T$, with:

$$\Omega_{1,e} = \Omega_{2,e} = \Omega_{3,e} = \Omega_{4,e} = \sqrt{\frac{gm}{4b}} \tag{11}$$

a hovering equilibrium point is obtained, characterized by a constant equilibrium state x_e (in particular, the equilibrium height is a value z_e, and the equilibrium angles ϕ_e, θ_e and ψ_e are all zero). Then, by considering deviations Δx of the state variables from x_e, and performing a linearization of the nonlinear state equations (see [23], [24]), a model akin to (1) is obtained:

$$\Delta\dot{x}(t) = A\Delta x(t) + B\Delta u(t) \tag{12}$$

with:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 \\ \sqrt{g\frac{b}{m}} & \sqrt{g\frac{b}{m}} & \sqrt{g\frac{b}{m}} & \sqrt{g\frac{b}{m}} \\ 0 & 0 & 0 & 0 \\ 0 & -\frac{l}{I_x}\sqrt{gmb} & 0 & \frac{l}{I_x}\sqrt{gmb} \\ 0 & 0 & 0 & 0 \\ -\frac{l}{I_y}\sqrt{gmb} & 0 & \frac{l}{I_y}\sqrt{gmb} & 0 \\ 0 & 0 & 0 & 0 \\ -\frac{d}{I_z}\sqrt{g\frac{m}{b}} & \frac{d}{I_z}\sqrt{g\frac{m}{b}} & -\frac{d}{I_z}\sqrt{g\frac{m}{b}} & \frac{d}{I_z}\sqrt{g\frac{m}{b}} \end{bmatrix}$$

which, together with a linear error-feedback control law $\Delta u(t) = -K\Delta x(t)$, leads to the closed-loop system:

$$\Delta\dot{x}(t) = (A - BK)\Delta x(t)$$

We will assume that both the altitude and the attitude of the quadrotor are monitored by a ground station. The communication between the UAV and the station can be hacked through a replay attack. Hence, the system's description (1)-(2) is completed by the output matrix C, which is given by:

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

TABLE I

SYSTEM PARAMETERS VALUES

Parameter	Value	Unit	Parameter	Value	Unit
I_x	$8.1e-3$	Nms^2	J	$104e-6$	Nms^2
I_y	$8.1e-3$	Nms^2	l	0.24	m
I_z	$14.2e-3$	Nms^2	b	$54.2e-6$	Ns^2
m	1	kg	d	$1.1e-6$	Nms^2
g	9.81	ms^{-2}			

or, equivalently, by defining $\Delta y(t) = y(t) - [z_e, \phi_e, \theta_e, \psi_e]^T$:

$$\Delta y(t) = C\Delta x(t)$$

Also, for the remaining of the manuscript, we will assume that the quadrotor's parameters are the ones provided in Table I, where I_x, I_y, I_z denote the body inertia along x, y, z axes, m is the quadrotor's mass, g denotes the gravity acceleration, J is the propeller inertia, l is the lever's length, and b and d are the thrust and drag factor, respectively.

B. Choice of the design parameters

Let us consider a replay attack detector, as described in the previous section, with $N = 2$ and $\omega_2 = 2\omega_1$. Due to the fact that by design:

$$G(\imath\omega_i) \approxeq F(\imath\omega_i)^{-1} = \left[C\left(\imath\omega_i - A + BK\right)^{-1} B\right]^{-1} \tag{13}$$

the following relationship holds between the magnitudes $\tilde{\alpha}_1$, $\tilde{\alpha}_2$, $\tilde{\alpha}_3$, $\tilde{\alpha}_4$ of $\tilde{\xi}_1$, $\tilde{\xi}_2$, $\tilde{\xi}_3$, $\tilde{\xi}_4$ (input signals to the decoupler) and the maximum magnitudes $\bar{\alpha}_1$, $\bar{\alpha}_2$, $\bar{\alpha}_3$, $\bar{\alpha}_4$ of ξ_1, ξ_2, ξ_3, ξ_4 (outputs of the decoupler, which are inputs of the actuators);

$$\begin{bmatrix} \bar{\alpha}_1 \\ \bar{\alpha}_2 \\ \bar{\alpha}_3 \\ \bar{\alpha}_4 \end{bmatrix} = \max_{i=1,2} \left| \left[C(\imath\omega_i - A + BK)^{-1}B\right]^{-1} \right| \begin{bmatrix} \tilde{\alpha}_1 \\ \tilde{\alpha}_2 \\ \tilde{\alpha}_3 \\ \tilde{\alpha}_4 \end{bmatrix} \tag{14}$$

where the max is understood element-wise. By requiring that:

$$\bar{\alpha}_l \leq \kappa_l u_{e,l}, l = 1, \dots, n_u \tag{15}$$

where $\kappa_l \ll 1$ and $u_{e,l}$ is the l-th element of u_e, such that the increment of the input signal brought by the signature signal is relatively small, a set of feasible frequencies is calculated, and ω_1 is chosen as the maximum value among these frequencies. The values $\tilde{\alpha}_l$, $l = 1, \dots, 4$ are design parameters whose values should be chosen small enough such that $\tilde{\xi}(t)$ is not clearly visible in the output signals, and big enough to overcome the effect of exogenous disturbances and measurement noise. In the following, we select $\kappa_1 = \kappa_2 = \kappa_3 = \kappa_4 = 1/10$ and $\tilde{\alpha}_1 = 0.005$ and $\tilde{\alpha}_2 = \tilde{\alpha}_3 = \tilde{\alpha}_4 = 0.01$.

Four different controllers K_1, K_2, K_3, K_4 have been considered in order to study how the particular choice of the controller affected both the set of feasible frequencies for

TABLE II

CLOSED-LOOP POLES POSITION

Controller	Dominant poles	Fast poles
K_1	$\{-3,-3,-3,-3\}$	$\{-10,-10,-10,-10\}$
K_2	$\{-3,-3,-3,-3\}$	$\{-20,-20,-20,-20\}$
K_3	$\{-3,-3,-3,-3\}$	$\{-50,-50,-50,-50\}$
K_4	$\{-3,-3,-3,-3\}$	$\{-100,-100,-100,-100\}$

ω_1 and the decoupling performance of the decoupler $F(s)$. All the controllers have been designed by pole placement, by requiring that the closed-loop poles were placed in different positions of the complex plane, as resumed in Table II. Eq. (14) has been used to calculate the expected $\bar{\alpha}$ (due to symmetry of the quadrotor, $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4$) for the different controllers, such that (15) can be checked graphically, as shown in Fig. 1. Using the controller K_1, a value $\omega_1 = 5.1 rad/s$ has been found, while with the controllers K_2 and K_3, $\omega_1 = 3.3 rad/s$ and $\omega_1 = 0.3 rad/s$ have been obtained. On the other hand, no feasible frequency ω_1 was found for controller gain K_4. Although in principle it is desired to obtain a value of ω_1 as high as possible, so that T_ω in (9) becomes smaller, and the detection algorithm based on estimating $\hat{\sigma}_l(t)$ using (10) behaves faster, the choice of ω_1 should take into account the decoupler performance which, looking at (13), depends on the specific controller gain (the decoupler can be obtained applying the VFIT3 routine[1] [19], [25], as described in [16]).

In particular, Fig. 2 shows the Bode plot of the transfer function from the input 1 to the output 1 of the cascade $G(s)F(s)$, for the different controller gains K_1, K_2, K_3. Note that the values on the x-axis are normalized with respect to ω_1, such that $\omega_{norm} = 1\, rad/s$ corresponds to $\omega = 5.1\, rad/s$, $\omega = 3.3\, rad/s$ and $\omega = 0.3\, rad/s$, respectively. It can be seen that the best decoupling performance is achieved with the controller K_3. However, using K_3 would lead to $\omega_1 = 0.3\, rad/s$ and, through (9), to $T_\omega = 20.94\, s$, ultimately leading to a very slow attack detector. For this reason, using K_2 ($\omega_1 = 3.3\, rad/s$, $T_\omega = 1.91\, s$) is deemed to be a good tradeoff between a fast detector and a good decoupling, and will be the controller used in the next section. By requiring an attenuation of $-20\, dB$ at frequency ω_2 for the first band-pass filter, and at frequency ω_1 for the second band-pass filter, the selectivity parameters are calculated as $Q_1 = Q_2 = 2\sqrt{11}$. Also, t_{trans} is chosen as the biggest among the settling times of the band-pass filters $H_i(s)$, and T_s is chosen as $T_s = 4t_{trans}$, as in [16], thus obtaining $t_{trans} = 15.87\, s$ and $T_s = 63.48\, s$. For the sake of completeness, Fig. 3 shows the comparison between the magnitude Bode plot of the non-decoupled (blue line) system and the decoupled one (red line). It can be seen that the series interconnection $G(s)F(s)$ approximates an identity matrix, such that a good decoupling is achieved.

IV. SIMULATION RESULTS

In order to assess the effectiveness of the proposed strategy, two simulation scenarios are considered. In Scenario 1, the attacker records the measurements of the first output during the first $200\, s$, and replays periodically the data starting from $t = 200\, s$. The arising mismatch between the outputs of the band-pass filters $z_{11}(t)$, $z_{21}(t)$ and the time-varying frequency profile of $\omega_{\sigma_1(t)}$ (see Fig. 4) allows detecting the attack after $8.21\, s$, as shown in Fig. 5, which depicts the logical assessment of $\sigma_i(t) == \hat{\sigma}_i(t)$, $i = 1,2,3,4$. In Scenario 2, the attacker corrupts the measurements $y_2(t)$ and $y_3(t)$ instead. In this case, the mismatches $\hat{\sigma}_2(t) \neq \sigma_2(t)$ and $\hat{\sigma}_3(t) \neq \sigma_3(t)$ allow identifying correctly the output channels as being attacked at time $398.65\, s$ and $208.21\, s$, respectively (see Figs. 6-7).

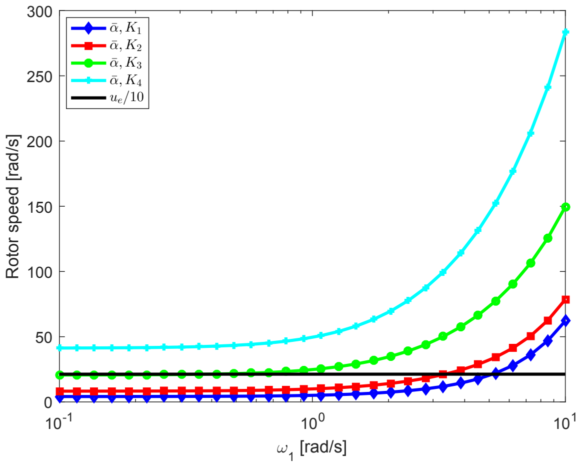

Fig. 1. Graphical check of condition (15).

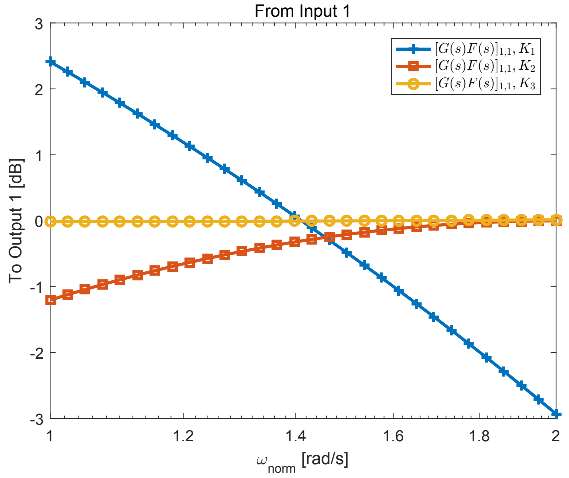

Fig. 2. Decoupling performance (Bode plot of the transfer function from input 1 to output 1 for the cascade $G(s)F(s)$, using different controller gains).

V. CONCLUSIONS

This work has investigated the applicability of a frequency-based replay attack detection method to a quadrotor UAV. In particular, the method introduces a sinusoidal signal with a time-varying frequency into the closed-loop

[1] https://www.sintef.no/projectweb/vectfit

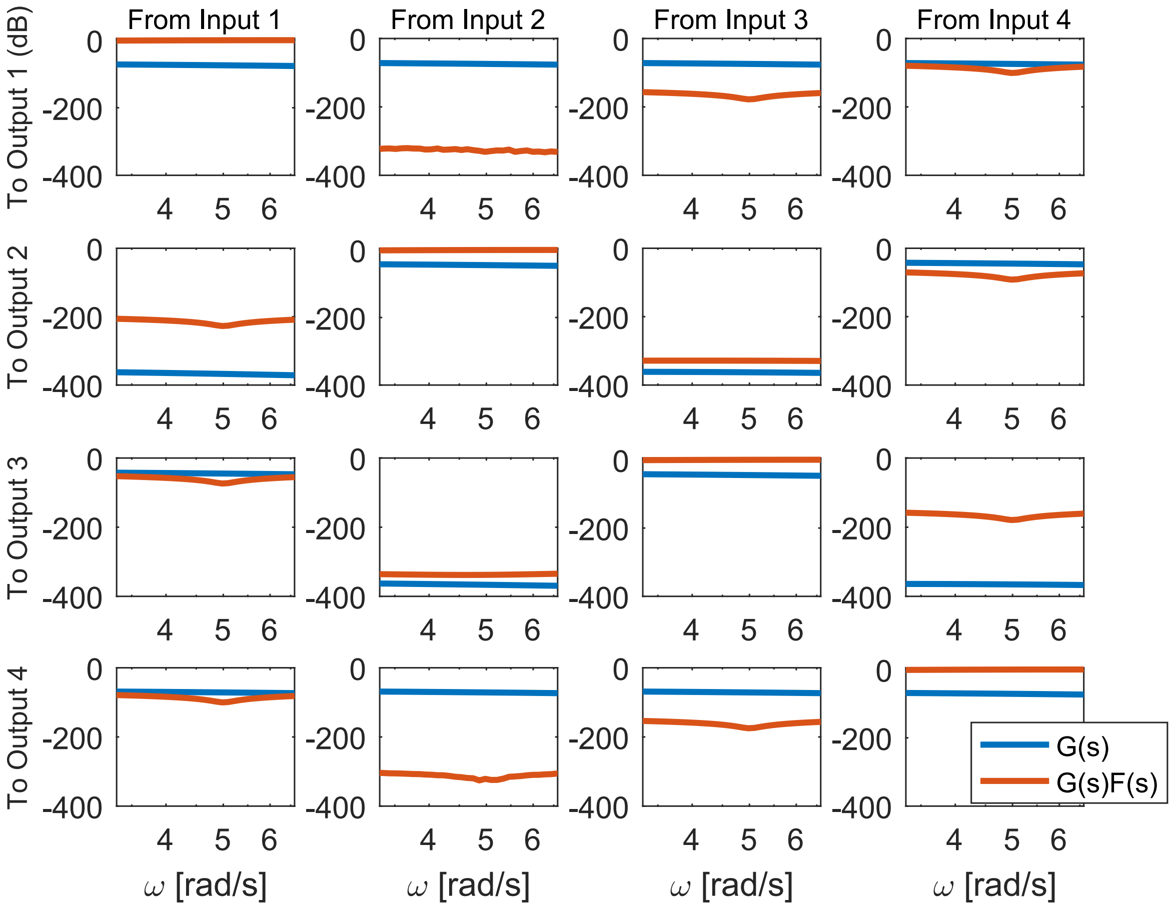

Fig. 3. Decoupling performance (Bode plots).

system, and checks whether the time profile of the frequency components in the output signals are compatible with the authentication signal or not, by comparing the energies of appropriate signals. The simulation scenarios have shown that the method can be applied to the considerate case study, being capable of not triggering false alarms and identifying correctly the attacked output channels.

References

[1] P. Antsaklis, "Goals and challenges in cyber-physical systems research editorial of the editor in chief," *IEEE Transactions on Automatic Control*, vol. 12, no. 59, pp. 3117–3119, 2014.

[2] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[3] D. Rotondo, H. S. Sánchez, V. Puig, T. Escobet, and J. Quevedo, "A virtual actuator approach for the secure control of networked LPV systems under pulse-width modulated dos attacks," *Neurocomputing*, 2019.

[4] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks-an approach to the risk assessment," in *Cyber Conflict (CyCon), 2013 5th International Conference on*. IEEE, 2013, pp. 1–23.

[5] K. Wesson and T. Humphreys, "Hacking drones," *Scientific American*, vol. 309, no. 5, pp. 54–59, 2013.

[6] C. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *Safety, Security and Rescue Robotics (SSRR), 2017 IEEE International Symposium on*. IEEE, 2017, pp. 194–199.

[7] S.-H. Seo, B.-H. Lee, S.-H. Im, and G.-I. Jee, "Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal," *Journal of Positioning, Navigation, and Timing*, vol. 4, no. 2, pp. 57–65, 2015.

[8] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson, and W. Alexis, "Securing commercial wifi-based UAVs from common security attacks," in *Military Communications Conference, MILCOM 2016-2016 IEEE*. IEEE, 2016, pp. 1213–1218.

[9] P. Pierpaoli, M. Egerstedt, and A. Rahmani, "Altering UAV flight path by threatening collision," in *Digital Avionics Systems Conference (DASC), 2015 IEEE/AIAA 34th*. IEEE, 2015, pp. 4A4–1.

[10] M. Verup and M. Olin, "Security models and exploitations in theory and practice for unmanned aerial vehicles," 2016.

[11] K. Highnam, K. Angstadt, K. Leach, W. Weimer, A. Paulos, and P. Hurley, "An uncrewed aerial vehicle attack scenario and trustworthy repair architecture," in *Dependable Systems and Networks Workshop, 2016 46th Annual IEEE/IFIP International Conference on*. IEEE, 2016, pp. 222–225.

[12] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*. IEEE, 2009, pp. 911–918.

[13] S. Weerakkody, Y. Mo, and B. Sinopoli, "Detecting integrity attacks on control systems using robust physical watermarking," in *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*. IEEE, 2014, pp. 3757–3764.

[14] C. Fang, Y. Qi, P. Cheng, and W. X. Zheng, "Cost-effective watermark based detector for replay attacks on cyber-physical systems," in *Control Conference (ASCC), 2017 11th Asian*. IEEE, 2017, pp. 940–945.

[15] A. Khazraei, H. Kebriaei, and F. R. Salmasi, "A new watermarking approach for replay attack detection in LQG systems," in *Decision*

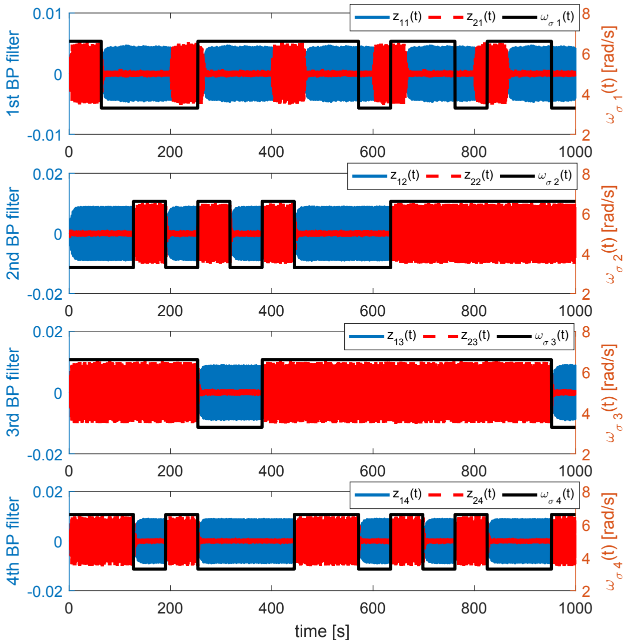

Fig. 4. Scenario 1. Outputs of the band-pass filters $z_{il}(t)$ and time-varying frequency $\omega_\sigma(t)$.

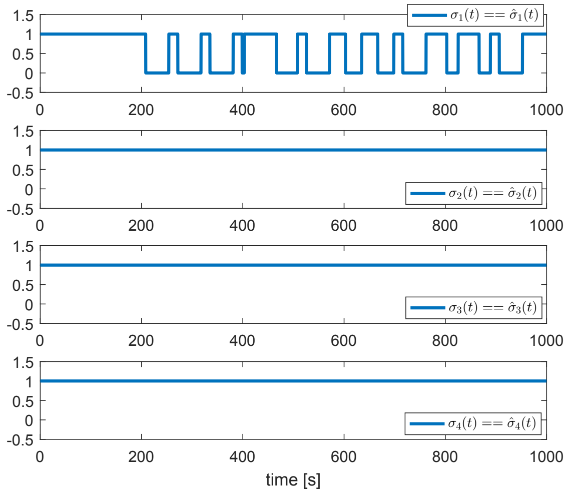

Fig. 5. Scenario 1. Result of the replay attack detection test.

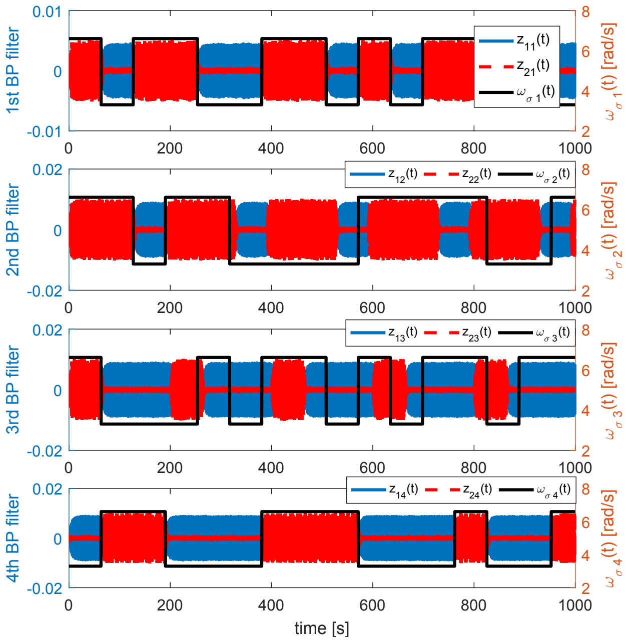

Fig. 6. Scenario 2. Outputs of the band-pass filters $z_{il}(t)$ and time-varying frequency $\omega_\sigma(t)$.

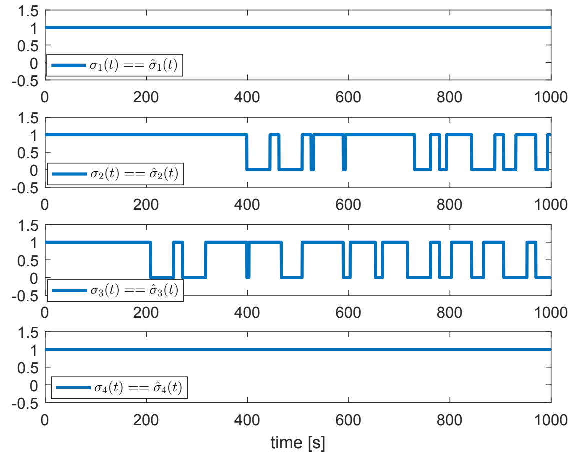

Fig. 7. Scenario 2. Result of the replay attack detection test.

and Control (CDC), 2017 IEEE 56th Annual Conference on. IEEE, 2017, pp. 5143–5148.

[16] H. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo, "Frequency-based detection of replay attacks: application to a multiple tank system," *IFAC-PapersOnLine*, vol. 51, no. 24, pp. 969–974, 2018.

[17] B. Tang, L. D. Alvergue, and G. Gu, "Secure networked control systems against replay attacks without injecting authentication noise," in *American Control Conference (ACC), 2015*. IEEE, 2015, pp. 6028–6033.

[18] A. Hoehn and P. Zhang, "Detection of replay attacks in cyber-physical systems," in *American Control Conference (ACC), 2016*. IEEE, 2016, pp. 290–295.

[19] B. Gustavsen and A. Semlyen, "Rational approximation of frequency domain responses by vector fitting," *IEEE Transactions on Power Delivery*, vol. 14, no. 3, pp. 1052–1061, 1999.

[20] Q.-G. Wang, *Decoupling Control*. Lecture Notes in Control and Information Sciences, Vol. 285, Springer-Verlag Berlin Heidelberg, 2003.

[21] B. Gustavsen and A. Semlyen, "Rational approximation of frequency domain responses by vector fitting," *IEEE Transactions on power delivery*, vol. 14, no. 3, pp. 1052–1061, 1999.

[22] H. Zumbahlen, *Linear circuit design handbook*. Elsevier Newnes Press, 2008.

[23] D. Rotondo, F. Nejjari, and V. Puig, "Model reference quasi-lpv control of a quadrotor uav," in *Control Applications (CCA), 2014 IEEE Conference on*. IEEE, 2014, pp. 736–741.

[24] ——, "Robust quasi–LPV model reference FTC of a quadrotor UAV subject to actuator faults," *International Journal of Applied Mathematics and Computer Science*, vol. 25, no. 1, pp. 7–22, 2015.

[25] B. Gustavsen, "Improving the pole relocating properties of vector fitting," *IEEE Transactions on Power Delivery*, vol. 21, no. 3, pp. 1587–1592, 2006.