Detection of replay attacks in autonomous vehicles using a bank of QPV observers

Helem S. Sánchez[1,2] , Damiano Rotondo[3], Vicenç Puig[1,2,4], Teresa Escobet[1,5] and Joseba Quevedo[1,2]

***Abstract*— This paper addresses the problem of replay attack detection in autonomous vehicles. Due to the strong presence of nonlinearities, traditional approaches based on linear approximations of the dynamics would not work effectively. For this reason, the proposed approach is based on a bank of quadratic parameter varying (QPV) observers, designed in such a way that each observer is insensitive to a replay attack that affects one specific sensor channel. This feature allows the development of a decision algorithm, whose effectiveness is validated by means of simulation results.**

I. Introduction

The profound integration between computation, networking and physical processes has led to the development of a new generation of systems, that are commonly referred to as *cyber-physical systems* (CPSs) [14]. CPSs have revolutionized many fields, such as energy systems [11] and aviation [3], since the aforementioned integration has increased the overall efficiency. However, at the same time, CPSs are affected by *cyber attacks*, i.e., actions that exploit the system's vulnerabilities to cause some kind of damage [21].

The security of CPSs has been studied by several researchers during the last few years, among which [24], who proposed to classify attacks by placing them on a three dimensions space, characterizing the prior knowledge of the attacker about the system, the degree of disruption and the degree of disclosure, respectively. Replay attacks are among the most dangerous cyber attacks, due to the fact that state-of-the-art fault detection methods fail in diagnosing them correctly. When a replay attack is carried out, at first the attacker records a set of sensor measurements. Then, in another phase of the attack, the real measurements are replaced with the previously recorded ones. As a consequence, the control system shows a deterioration of the performance, and other malicious actions can be performed without being detected.

[1] Research Center for Supervision, Safety and Automatic Control, UPC, Rambla Sant Nebridi, 22, 08022 Terrassa, Spain. helemsabina@gmail.com

[2] Automatic Control Department, UPC-ESAII,Rambla Sant Nebridi, 11, 08022 Terrassa, Spain

[3] Department of Electrical and Computer Engineering (IDE), University of Stavanger (UiS), Kristine Bonnevies vei 22, 4021 Stavanger, Norway

[4] Institut de Robòtica i Informàtica Industrial, CSIC-UPC, Llorens i Artigas 4-6, 08028 Barcelona, Spain

[5] Department of Mining, Industrial and ICT Engineering, UPC, Av. de les Bases de Manresa, 61-73, 08242 Manresa, Spain

* This work was partially supported by the University of Stavanger through the project IN-12267. 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.

The first technique to detect replay attacks was proposed by [17], who suggested to add a time-varying noisy authentication signal (*signature*) to the control input in order to enable replay attack detection. This kind of approach, known as *watermarking*, was later extended by [26], where a more advanced adversary, that could access only a subset of the inputs/outputs but had knowledge about the system, was considered. [13] proposed to destabilize the difference between the estimated and measured output of the systems, while preserving the main system's stability. [22] proposed to use a sinusoidal signal with a time-varying frequency as authentication signal, which was later enhanced by [25] by introducing an observer-based compensation which decreased the performance loss usually found in other watermarking-based methods. Notably, a few recent works have addressed also the problem of making a control system resilient against replay attacks, see e.g. [7] and [9].

Vehicle automation is one of the sectors in which CPSs are introducing fast innovations, with the goal of creating intelligent transportation systems. For example, the possibility of sharing data such as position and speed of movement has led to the development of connected and autonomous vehicles (CAVs) [16], which are potentially vulnerable to cyber attacks [18]. For this reason, the identification of cyber vulnerabilities and their mitigation has been addressed by several researchers, see e.g. [27] and [8].

The goal of this paper is to contribute to the state-of-the-art of cyber security in autonomous vehicles by addressing the problem of replay attack detection in these systems. Due to the high nonlinearity of these systems, traditional approaches based on the system's linearity would not work. For this reason, we investigate the application of quadratic parameter varying (QPV) observers [20]. The QPV framework was introduced by [19] to characterize a class of time-varying nonlinear systems with quadratic terms depending on state variables, and has found some applications in automotive, such as [12], where it was shown that the suspension shock performance of a vehicle could be improved by employing a QPV suspension system. This paper shows that under some mild approximations, the dynamics of the tracking error between some desired trajectory and the real vehicle trajectory can be brought to a QPV form. In this way, a bank of QPV observers can be designed so that each observer is insensitive to a replay attack affecting one specific sensor channel, so that an attack diagnosis algorithm can be implemented.

The paper is structured as follows. Section II introduces the vehicle's model and the mathematical description of

replay attacks. Section III shows how the closed-loop error system can be reshaped in a QPV form, recalls the structure of a QPV observer and the design conditions that ensure the asymptotical convergence to zero of the estimation error. Section IV analyzes the effect of the replay attacks on the QPV observers, and describes the decision algorithm used to infer about the occurrence and localization of the attacks. The proposed approach is validated by means of simulation results in Section V. Finally, the main conclusions are drawn in Section VI.

II. Problem Formulation

Let us consider the kinematic model for a vehicle that, assuming null skidding and small lateral forces, is described by [1]:

$$\begin{cases} \dot{x}(t) = v(t)\cos\theta(t) \\ \dot{y}(t) = v(t)\sin\theta(t) \\ \dot{\theta}(t) = \omega(t) \end{cases} \tag{1}$$

where x, y and θ represent the current position and orientation of the vehicle in meters and radians with respect to the global frame, respectively, v is the linear velocity, and ω is the angular velocity. The vehicle tracks a trajectory described by some desired values x_d, y_d, θ_d, obtained by fixing the desired linear and angular velocities v_d and ω_d, respectively. By means of a rotation, it is possible to express the tracking errors in the body vehicle frame, as follows [6]:

$$\begin{bmatrix} x_e(t) \\ y_e(t) \\ \theta_e(t) \end{bmatrix} = \begin{bmatrix} \cos\theta(t) & \sin\theta(t) & 0 \\ -\sin\theta(t) & \cos\theta(t) & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_d(t) - x(t) \\ y_d(t) - y(t) \\ \theta_d(t) - \theta(t) \end{bmatrix} \tag{2}$$

Then, taking into account the non-holonomic constraint:

$$\dot{x}(t)\sin\theta(t) = \dot{y}(t)\cos\theta(t) \tag{3}$$

after some trigonometric manipulations, the following open-loop error system is obtained:

$$\begin{cases} \dot{x}_e(t) = \omega(t)y_e(t) + v_d(t)\cos\theta_e(t) - v(t) \\ \dot{y}_e(t) = -\omega(t)x_e(t) + v_d(t)\sin\theta_e(t) \\ \dot{\theta}_e(t) = \omega_d(t) - \omega(t) \end{cases} \tag{4}$$

Given the kinematic error of the vehicle (4), it can be shown that the control law:

$$\begin{cases} v(t) = k_1 x_e(t) + v_d(t)\cos\theta_e(t) \\ \omega(t) = \omega_d(t) + k_2 v_d(t)\frac{\sin\theta_e(t)}{\theta_e(t)}y_e(t) + k_3\theta_e(t) \end{cases} \tag{5}$$

stabilizes the closed-loop dynamics in the Lyapunov sense if the controller parameters k_1, k_2 and k_3 are chosen to be positive [2].

In this paper, we consider the case in which the autonomous vehicle sends some information about its position to a remote supervision station. This information, denoted in the following as $\Psi(t)$, can be affected by a *replay attack*, which is carried out in two stages[1]:

- the attacker gathers the data without disturbing the system, starting from time t_0 until $t_0 + w$, where w is the size of the attack window;

[1]Note that the replay attack does not affect the control algorithm running on the vehicle.

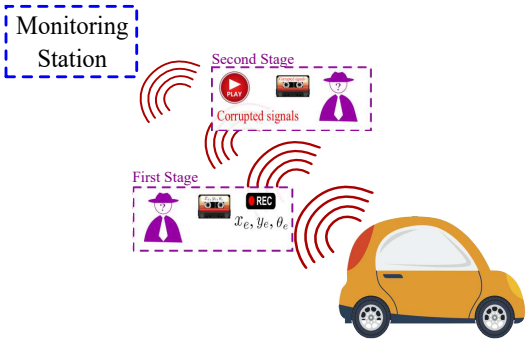

Fig. 1. Conceptual representation of the attack scenario.

- at time t_1, the attacker begins to replay the collected data, such that the real data in the intervals $[t_1 + (N_f - 1)w, t_1 + N_f w]$, $N_f \in \mathbb{N}$, $N_f \geq 1$, is replaced with the data recorded in the previous stage.

Since control systems are not resilient to replay attacks, there is a need to develop methods to detect them. In this paper, we show that if the autonomous vehicle sends to the remote supervision station its relative position with respect to the reference trajectory, i.e. the states x_e, y_e, θ_e, then it is possible to design an observer-based detection scheme which, by means of a signature signal introduced in the input channel, is able to detect a replay attack and identify which channel is being attacked.

III. QPV Observer for the Autonomous Vehicle

Let us consider a slightly modified control law, similar to (5) as follows:

$$\begin{cases} v(t) = k_1 x_e(t) + v_d(t)\cos\theta_e(t) + v^\star(t) \\ \omega(t) = \omega_d(t) + k_2 v_d(t)\frac{\sin\theta_e(t)}{\theta_e(t)}y_e(t) + k_3\theta_e(t) + \omega^\star(t) \end{cases} \tag{6}$$

where the signature signals $v^\star$, $\omega^\star$ have been added. These signals are assumed to be known by the defender (the remote supervision station), but unknown to the attacker.

By merging (4) and (6), after some manipulations, one obtains the following closed-loop error system:

$$\begin{cases} \dot{x}_e(t) = \omega_d(t)y_e(t) + k_2 v_d(t)\frac{\sin\theta_e(t)}{\theta_e(t)}y_e(t)^2 + k_3\theta_e(t)y_e(t) \\ \qquad +\omega^\star(t)y_e(t) - k_1 x_e(t) - v^\star(t) \\ \dot{y}_e(t) = -\omega_d(t)x_e(t) - k_2 v_d(t)\frac{\sin\theta_e(t)}{\theta_e(t)}x_e(t)y_e(t) \\ \qquad -k_3\theta_e(t)x_e(t) - \omega^\star(t)x_e(t) + v_d(t)\sin\theta_e(t) \\ \dot{\theta}_e(t) = -k_2 v_d(t)\frac{\sin\theta_e(t)}{\theta_e(t)}y_e(t) - k_3\theta_e(t) - \omega^\star(t) \end{cases} \tag{7}$$

which, under small angle assumption:

$$\sin\theta_e(t) \approx \theta_e(t)$$

and defining the state vector $\xi = [x_e, y_e, \theta_e]^T$, the input vector $u = [v^\star, \omega^\star]^T$, and the scheduling vector $\rho = [v_d, \omega_d + \omega^\star]^T$, can be brought to a quasi-QPV form [19] (the term *quasi* refers to the fact that the scheduling vector depends on the endogenous signal $\omega^\star$):

$$\dot{\xi}(t) = A(\rho(t))\xi(t) + N(\rho(t), \xi(t))\xi(t) + Bu(t) \tag{8}$$

where the matrix functions $A(\rho(t))$, $N(\rho(t),\xi(t))$ and the matrix B are defined as follows:

$$A(\rho(t)) = \begin{bmatrix} -k_1 & \rho_2(t) & 0 \\ -\rho_2(t) & 0 & \rho_1(t) \\ 0 & -k_2\rho_1(t) & -k_3 \end{bmatrix}$$

$$N(\rho(t),\xi(t)) = \begin{bmatrix} \xi(t)^T N_1(\rho(t)) \\ \xi(t)^T N_2(\rho(t)) \\ 0 \end{bmatrix} \quad B = \begin{bmatrix} -1 & 0 \\ 0 & 0 \\ 0 & -1 \end{bmatrix}$$

with:

$$N_1(\rho(t)) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & k_2\rho_1(t) & k_3/2 \\ 0 & k_3/2 & 0 \end{bmatrix}$$

$$N_2(\rho(t)) = \begin{bmatrix} 0 & -k_2\rho_1(t)/2 & -k_3/2 \\ -k_2\rho_1(t)/2 & 0 & 0 \\ -k_3/2 & 0 & 0 \end{bmatrix}$$

Under the assumption that the remote supervision station has access to the states x_e, y_e, θ_e, the state-space model is completed by the output matrix $C = I$.

Following [5], a possible approach to identify which outputs are not behaving as expected is to employ a bank of observers, each one sensitive to malfunctions in all but one of the outputs. To do so, each observer should generate the state estimate using a set of measurements that excludes the specific measurement against whose malfunctions the observer is to be made insensitive.

Hence, let us consider three state observers $\mathcal{O}_1$, $\mathcal{O}_2$, $\mathcal{O}_3$ which use output matrices C_1, C_2 and C_3, respectively, where each output matrix C_h is obtained from C by replacing its h-th row with a zero row.

Given the QPV system (8), a polytope $\mathcal{P} = \mathrm{Co}\{\xi_{(1)}, \xi_{(2)}, \ldots, \xi_{(p)}\} \subset \mathbb{R}^3$, with $0 \in \mathcal{P}$, and a scalar $\alpha > 0$, the results described in [20] can be used for designing a QPV state observer that achieves convergence to zero of the estimation error $e(t) \triangleq \xi(t) - \hat{\xi}(t)$ with rate of convergence α in $\mathcal{P}$, where $\hat{\xi}$ denotes the observed state, under the following two assumptions.

Assumption 1: The scheduling vector $\rho(t)$ is assumed to be known, and varies (arbitrarily fast) within some known set Π. Note that this assumption makes sense in the case of the QPV system (8), since ρ contains desired state values and signature signals, which are known by the defender.

Assumption 2: The trajectory of $\xi(t)$ is contained in:

$$\mathcal{F} = \{\xi \in \mathbb{R}^3 : \xi^T Q^{-1} \xi \leq 1\} \tag{9}$$

with $Q \succ 0$ and $\mathcal{P} \subset \mathcal{F}$. Note that if a bound on the initial error $\xi(0)$ is available, this assumption can be guaranteed by means of an appropriate design of the control law, e.g., using quadratic boundedness [4].

More specifically, each QPV state observer $\mathcal{O}_h$ is given by:

$$\dot{\hat{\xi}}_h(t) = A(\rho(t))\hat{\xi}_h(t) + N\left(\rho(t), \hat{\xi}_h(t)\right)\hat{\xi}_h(t) + Bu(t) + L_h(\rho(t))\left(\Psi_h(t) - C_h\hat{\xi}_h(t)\right) \tag{10}$$

where $\Psi_h(t)$ is obtained from $\Psi(t)$ by replacing the h-th element with a 0. Then, the following lemma provides the conditions for designing the observer gains $L_h(\rho(t))$, $h = 1,2,3$, such that $e_h(t) \triangleq \xi(t) - \hat{\xi}_h(t)$ converges to zero with rate of convergence α in $\mathcal{P}$.

Lemma 1: Let $P \succ 0$, $0 < \gamma < 1$, and the matrix function $\Gamma_h(\rho) \in \mathbb{R}^{3\times 2}$ be such that $\forall i \in \{1,\ldots,p\}$, $\forall j \in \{1,\ldots,p\}$, $\forall k \in \{1,\ldots,q\}$ and $\forall \rho \in \Pi$:

$$\begin{pmatrix} 1 & \xi_{(i)}^T \\ \xi_{(i)} & P \end{pmatrix} \succeq 0 \tag{11}$$

$$\begin{pmatrix} 1 & \gamma a_k^T P \\ \gamma P a_k & P \end{pmatrix} \succeq 0 \tag{12}$$

$$\begin{pmatrix} 1 & \gamma a_k^T Q \\ \gamma Q a_k & Q \end{pmatrix} \succeq 0 \tag{13}$$

$$He\{\gamma[PA(\rho) - \Gamma_h(\rho)C_h] - P\begin{pmatrix} \xi_{(j)}^T He\{N_1(\rho)\} - \xi_{(i)}^T N_1(\rho) \\ \xi_{(j)}^T He\{N_2(\rho)\} - \xi_{(i)}^T N_2(\rho) \\ 0 \end{pmatrix}\} + \gamma\alpha P \prec 0 \tag{14}$$

where the vectors a_k are given by an equivalent representation of $\mathcal{P}$ in terms of half-spaces:

$$\mathcal{P} = \{\xi \in \mathbb{R}^3 : a_k^T \xi \leq 1, k = 1,\ldots,q\} \tag{15}$$

with q appropriate number.

Then, the observer (10) with $L_h(\rho(t)) = P^{-1}\Gamma_h(\rho(t))$ is such that the estimation error $e_h(t)$ converges to zero with rate of convergence α in $\mathcal{P}$.

Proof: See [20]. □

Note that Lemma 1 corresponds to an infinite number of conditions due to the dependence of (14) on the scheduling vector ρ. One way to reduce the conditions to a finite number is by means of a polytopic characterization, as discussed in [20], which is the approach used to obtain the results in Section V.

IV. Observer-based attack diagnosis

First of all, let us consider the attackless case, for which the estimation error dynamics is given by:

$$\dot{e}_h(t) = \dot{\xi}(t) - \dot{\hat{\xi}}_h(t) = [A(\rho(t)) - L_h(\rho(t))C_h]e_h(t) - N(\rho(t), e_h(t))e_h(t) + \tilde{N}(\rho(t), e_h(t))\xi(t) \tag{16}$$

with:

$$\tilde{N}(\rho(t), e_h(t)) = \begin{bmatrix} e_h(t)^T He\{N_1(\rho(t))\} \\ e_h(t)^T He\{N_2(\rho(t))\} \\ 0 \end{bmatrix}$$

which converges to zero according to Lemma 1.

When the information sent by the sensors to the remote supervision station is affected by a replay attack, the observer uses the current *known* values of $\rho(t)$ and $u(t)$ to compute the updated state estimate, using corrupted measurements $\Psi(t) = \Xi_m C\xi(t) + (I - \Xi_m)C\xi(\tilde{t})$ where $\xi(\tilde{t}) = [x_e(\tilde{t}), y_e(\tilde{t}), \theta_e(\tilde{t})]^T$, with $\tilde{t}$ denoting a previous time instant corresponding to replayed data, and the matrix

Ξ_m is a matrix that characterizes a replay attack in the m-th channel (it is obtained from the identity matrix by replacing its m-th diagonal element with a 0). In this case, the observed estimation error using the observer $\mathcal{O}_h$ can be defined as the difference between the received measurements and the current state estimate, i.e., $\varepsilon_h(t) = \Xi_m C_h \xi(t) + (I - \Xi_m) C_h \xi(\tilde{t}) - C_h \hat{\xi}_h(t)$. In order to analyze whether $\varepsilon_h(t)$ would converge to zero or not, let us recall that the dynamics of $\xi(\tilde{t})$ are described by (8), but shifted to time $\tilde{t}$ instead of t:

$$\dot{\xi}(\tilde{t}) = A\left(\rho(\tilde{t})\right)\xi(\tilde{t}) + N\left(\rho(\tilde{t}), \xi(\tilde{t})\right)\xi(\tilde{t}) + Bu(\tilde{t}) \quad (17)$$

In general, the dynamics of $\varepsilon_h(t)$ follows:

$$\begin{aligned}\dot{\varepsilon}_h(t) &= \Xi_m C_h \dot{\xi}(t) + (I - \Xi_m) C_h \dot{\xi}(\tilde{t}) - C_h \dot{\hat{\xi}}_h(t) \quad (18)\\ &= \Xi_m C_h A\left(\rho(t)\right)\xi(t) + \Xi_m C_h N\left(\rho(t), \xi(t)\right)\xi(t)\\ &+ \Xi_m C_h B u(t) + (I - \Xi_m) C_h A\left(\rho(\tilde{t})\right)\xi(\tilde{t})\\ &+ (I - \Xi_m) C_h N\left(\rho(\tilde{t}), \xi(\tilde{t})\right)\xi(\tilde{t}) + (I - \Xi_m) C_h B u(\tilde{t})\\ &- C_h A\left(\rho(t)\right)\hat{\xi}(t) - C_h N\left(\rho(t), \hat{\xi}(t)\right)\hat{\xi}(t) - C_h B u(t)\\ &- C_h L_h\left(\rho(t)\right)\left(\Xi_m C_h \xi(t) + (I - \Xi_m) C_h \xi(\tilde{t}) - C_h \hat{\xi}(t)\right)\end{aligned}$$

which is affected by the mismatch $\xi(t) \neq \xi(\tilde{t})$, $v^*(t) \neq v^*(\tilde{t})$ and $\omega^*(t) \neq \omega^*(\tilde{t})$, such that $\varepsilon_h(t)$ would not converge to zero. However, let us consider the case $h = m$ (i.e., the observer does not take into account the measurement corrupted by the replay attack). In this case, since $\Xi_h C_h = C_h$ and $(I - \Xi_h) C_h = 0$, (18) reduces to:

$$\dot{\varepsilon}_h(t) = C_h\left(\dot{\xi}(t) - \dot{\hat{\xi}}_h(t)\right) \quad (19)$$

where $\dot{\xi}(t) - \dot{\hat{\xi}}_h(t)$ is as in (16), which shows convergence to zero of the estimation error.

Based on the above discussion, the following observer-based attack diagnosis algorithm is proposed ($e_{h,j}(t)$ denotes the j-th component of $e_h(t)$).

Decision Algorithm.

```
if O1: e1,1(t) ≠ 0, e1,2(t) = 0, e1,3(t) = 0
  then ''replay attack affecting sensor 1''
if O2: e2,1(t) = 0, e2,2(t) ≠ 0, e2,3(t) = 0
  then ''replay attack affecting sensor 2''
if O3: e3,1(t) = 0, e3,2(t) = 0, e3,3(t) ≠ 0
  then ''replay attack affecting sensor 3''
else ''no replay attack''
```

Note that in a setting where unknown exogenous disturbances and measurement noise affect the system, the above conditions $e_h(t) \neq 0$ and $e_h(t) = 0$ should be replaced by $|e_h(t)| \geq e_h^{th}$ and $|e_h(t)| \leq e_h^{th}$, respectively, where e_h^{th} denotes appropriate thresholds that are not exceeded in the attackless scenario.

V. Simulation Results

Let us consider an autonomous vehicle which follows the trajectory shown in Fig. 3 (blue line), which starts from

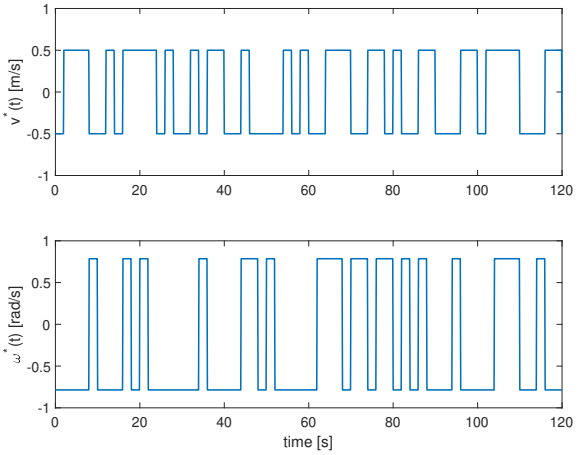

Fig. 2. Signature signals $v^*(t)$ and $\omega^*(t)$.

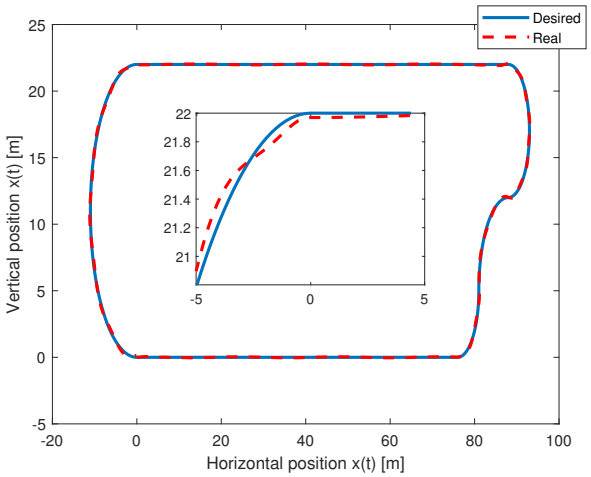

Fig. 3. Desired and real position.

$x_d(0) = y_d(0) = \theta_d(0) = 0$ and is obtained by considering the following values for $v_d(t)$ and $\omega_d(t)$:

$$(v_d(t), \omega_d(t)) = \begin{cases} (7.6, 0) & \text{if } \mathrm{mod}(t, 60) < 10 \\ (\pi/2, \pi/10) & \text{if } \mathrm{mod}(t, 60) < 15 \\ (7\pi/10, -\pi/10) & \text{if } \mathrm{mod}(t, 60) < 20 \\ (5\pi/14, \pi/14) & \text{if } \mathrm{mod}(t, 60) < 34 \\ (44/5, 0) & \text{if } \mathrm{mod}(t, 60) < 44 \\ (11\pi/16, \pi/16) & \text{else} \end{cases}$$

As stated in Section II, the controller parameters k_1, k_2, k_3 must be chosen positive to stabilize the closed-loop system. In the remaining of this section, $k_1 = 1$, $k_2 = 2$, $k_3 = 3$ will be used. Moreover, the signature signals shown in Fig. 2 are added. The real system trajectory is shown in Fig. 3, where the mismatch between the desired and the real values (see zoomed portion of the plot) is due to the introduction of $v^*(t)$ and $\omega^*(t)$. Using the CVX software [10], an outer bounding ellipsoid $\mathcal{F}$ that contains the tracking error trajectory $\xi(t)$, as in (9), has been computed, as shown in Fig. 4. Then, the gain-scheduling observer gains $L_h\left(\rho(t)\right)$ have been calculated

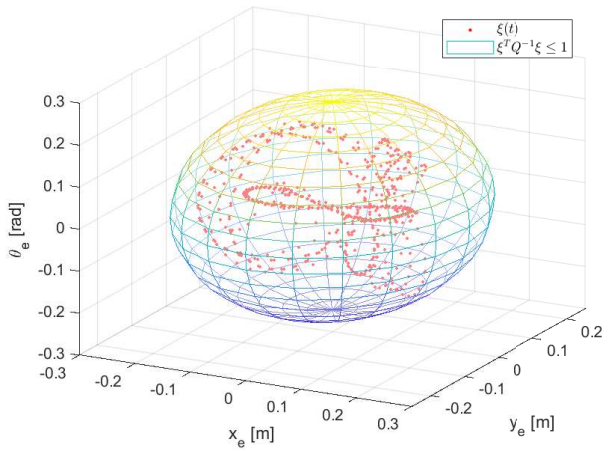

Fig. 4. Tracking error $\xi(t)$ and computed outer bounding ellipsoid $\mathcal{F}$.

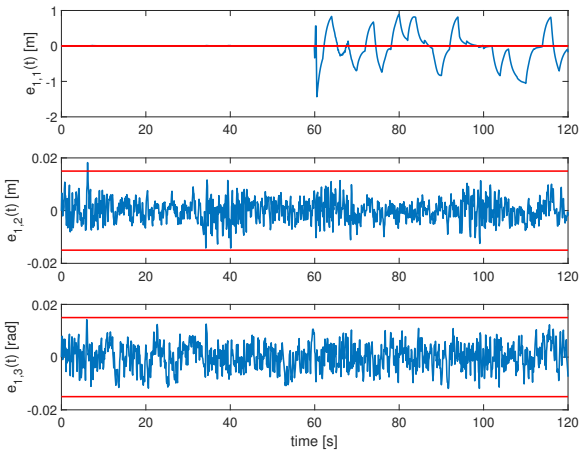

Fig. 5. Estimation error - Attack scenario 1 - Observer $\mathcal{O}_1$.

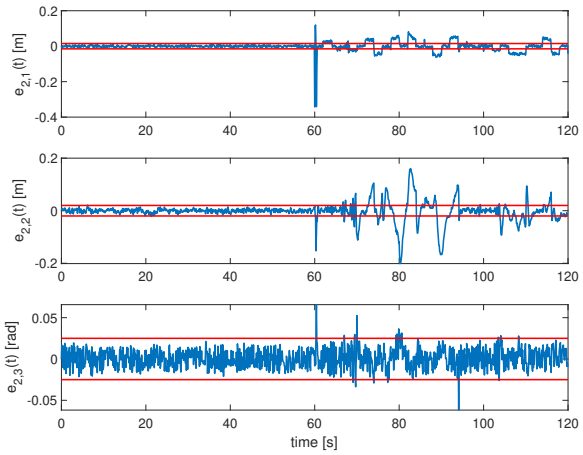

Fig. 6. Estimation error - Attack scenario 1 - Observer $\mathcal{O}_2$.

using Lemma 1, whose LMIs have been solved using the YALMIP toolbox [15] with SeDuMi solver [23].

Three attack scenarios are considered, each one lasting $120\,s$ and exhibiting a replay attack affecting one of the output channels in the time interval from $60\,s$ to $120\,s$. In scenario 1, the first output channel is attacked, whereas in scenarios 2 and 3, the second and third output channels are attacked, respectively.

Figs. 5-7 show the observed estimation errors obtained in attack scenario 1 for each of the designed observers (the red horizontal lines represent thresholds computed such that they are not exceeded in attackless simulations). It can be clearly seen that observers $\mathcal{O}_2$ and $\mathcal{O}_3$ are affected in all the components of the estimation error by the replay attack, whereas for observer $\mathcal{O}_1$, starting from $60\,s$ only $e_{1,1}(t)$ exceeds the corresponding threshold which, according to the Decision Algorithm provided in Section IV, allows a correct diagnosis of *replay attack affecting sensor 1*.

Similar results are obtained in attack scenarios 2 and 3, such that correct diagnosis of *replay attack affecting sensor 2* and *sensor 3* are achieved. For instance, Fig. 8 shows the observed estimation error obtained in attack scenario 2 using the observer $\mathcal{O}_2$, that shows the insensitivity of the first and third component to the replay attack. Similarly, Fig. 9 shows that the first and second component of the observer $\mathcal{O}_3$ are insensitive to a replay attack affecting the third output channel.

VI. Conclusions

In this paper, the problem of replay attack detection in autonomous vehicles has been addressed by means of a bank of observers, each one designed to be insensitive to a replay attack affecting one specific sensor channel. It has been shown that under some mild approximations, the dynamics of the vehicle tracking error can be reshaped into a quadratic parameter varying (QPV) form, in such a way that QPV observers can be used to enforce the convergence of the estimation error to zero in the attackless scenario. On the other hand, when the system is attacked, one of the observers will exhibit the relevant feature that only one of the components of its observed estimation error will be affected by the replay attack. This feature has allowed the development of an algorithm to decide about the occurrence and localization of replay attacks, whose effectiveness has been validated by means of simulation results. Future research will be devoted to increase the robustness of the proposed approach, as well as to perform its experimental validation in a real application.

References

[1] M. Aicardi, G. Casalino, A. Bicchi, and A. Balestrino. Closed loop steering of unicycle like vehicles via Lyapunov techniques. *IEEE Robotics & Automation Magazine*, 2(1):27–35, 1995.

[2] E. Alcala, V. Puig, J. Quevedo, T. Escobet, and R. Comasolivas. Autonomous vehicle control using a kinematic Lyapunov-based technique with LQR-LMI tuning. *Control Engineering Practice*, 73:1–12, 2018.

[3] M. Andreacchio, A. Bekrar, R. Benmansour, and D. Trentesaux. Balancing preventive and corrective maintenance of aircraft assets: A cyber-physical systems approach. In *IEEE 14th International Conference on Industrial Informatics (INDIN)*, pages 500–503, 2016.

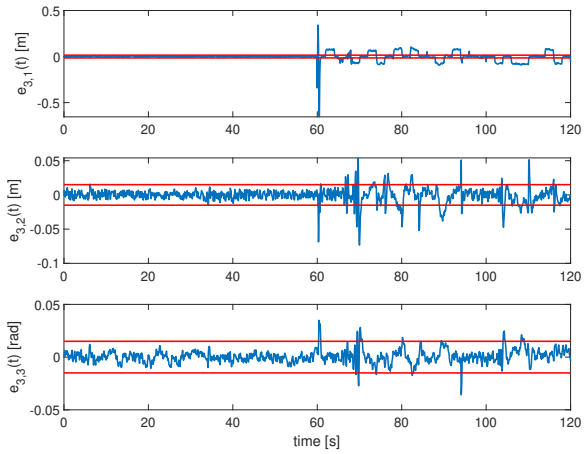

Fig. 7. Estimation error - Attack scenario 1 - Observer $\mathcal{O}_3$.

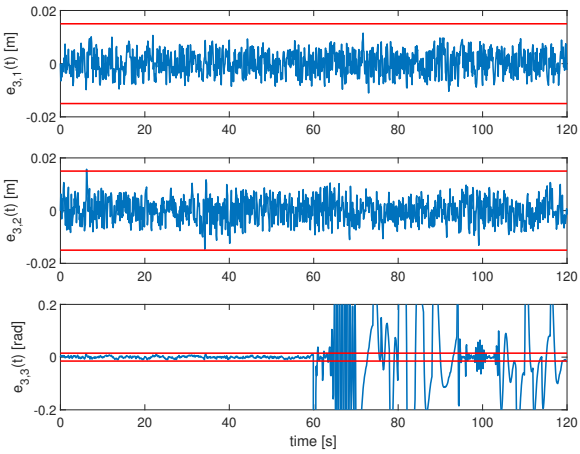

Fig. 9. Estimation error - Attack scenario 3 - Observer $\mathcal{O}_3$.

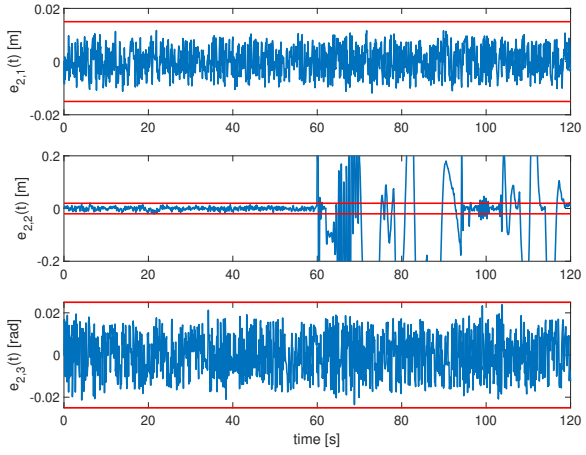

Fig. 8. Estimation error - Attack scenario 2 - Observer $\mathcal{O}_2$.

[4] M. L. Brockman and M. Corless. Quadratic boundedness of nonlinear dynamical systems. In *Proceedings of the 34th IEEE Conference on Decision and Control (CDC)*, volume 1, pages 504–509, 1995.

[5] J. Chen and R. J. Patton. *Robust model-based fault diagnosis for dynamic systems*, volume 3. 2012.

[6] W. E. Dixon, D. M. Dawson, E. Zergeroglu, and A. Behal. *Nonlinear control of wheeled mobile robots*, volume 175. Springer, 2001.

[7] R. El Abbadi and H. Jamouli. Stabilization of cyber physical system exposed to a random replay attack modeled by Markov chains. In *6th International Conference on Control, Decision and Information Technologies (CoDIT)*, pages 528–533, 2019.

[8] A. Ferdowsi, S. Ali, W. Saad, and N. B. Mandayam. Cyber-physical security and safety of autonomous connected vehicles: optimal control meets multi-armed bandit learning. *IEEE Transactions on Communications*, 2019.

[9] G. Franzè, F. Tedesco, and W. Lucia. Resilient control for cyber-physical systems subject to replay attacks. *IEEE Control Systems Letters*, 3(4):984–989, 2019.

[10] M. Grant and S. Boyd. CVX: Matlab software for disciplined convex programming, 2008.

[11] M. D. Ilic, L. Xie, U. A. Khan, and J.M.F. Moura. Modeling of future cyber-physical energy systems for distributed sensing and control. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 40(4):825–838, 2010.

[12] S. Kanarachos, A. M. Dizqah, G. Chrysakis, and M. E. Fitzpatrick. Optimal design of a quadratic parameter varying vehicle suspension system using contrast-based fruit fly optimisation. *Applied Soft Computing*, 62:463–477, 2018.

[13] A. Khazraei, H. Kebriaei, and F. R. Salmasi. A new watermarking approach for replay attack detection in LQG systems. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pages 5143–5148, 2017.

[14] E. A. Lee. Cyber physical systems: Design challenges. In *11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pages 363–369, 2008.

[15] J. Löfberg. YALMIP: A toolbox for modeling and optimization in MATLAB. In *Proceedings of the CACSD Conference*, 2004.

[16] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark. Connected vehicles: Solutions and challenges. *IEEE internet of things journal*, 1(4):289–299, 2014.

[17] Y. Mo and B. Sinopoli. Secure control against replay attacks. In *47th annual Allerton conference on communication, control, and computing*, pages 911–918, 2009.

[18] J. Petit and S. E. Shladover. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):546–556, 2014.

[19] D. Rotondo and T. A. Johansen. Analysis and design of quadratic parameter varying (QPV) control systems with polytopic attractive region. *Journal of the Franklin Institute*, 355(8):3488–3507, 2018.

[20] D. Rotondo and T. A. Johansen. State observer design for quadratic parameter varying (QPV) systems. In *European Control Conference (ECC)*, 2019.

[21] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo. Bibliographical review on cyber attacks from a control oriented perspective. *Annual Reviews in Control*, 2019.

[22] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, J. Saludes, and J. Quevedo. Detection of replay attacks in cyber-physical systems using a frequency-based signature. *Journal of the Franklin Institute*, 356(5):2798–2824, 2019.

[23] J. F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization methods and software*, 11(1-4):625–653, 1999.

[24] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson. Attack models and scenarios for networked control systems. In *Proceedings of the 1st international conference on High Confidence Networked Systems*, pages 55–64, 2012.

[25] C. Trapiello, D. Rotondo, H. Sanchez, and V. Puig. Detection of replay attacks in CPSs using observer-based signature compensation. In *6th International Conference on Control, Decision and Information Technologies (CoDIT)*, pages 1–6, 2019.

[26] S. Weerakkody, Y. Mo, and B. Sinopoli. Detecting integrity attacks on control systems using robust physical watermarking. In *53rd IEEE Conference on Decision and Control*, pages 3757–3764, 2014.

[27] E. Yağdereli, C. Gemci, and A. Z. Aktaş. A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation*, 12(4):369–381, 2015.