2019 American Control Conference (ACC)
Philadelphia, PA, USA, July 10-12, 2019

A Novel Control Architecture for the Detection of False Data Injection Attacks in Networked Control Systems

Mohsen Ghaderi Kian Gheitasi Walter Lucia

Abstract— **In this manuscript, we propose a novel control architecture capable of detecting deception attacks affecting networked control systems. In the proposed solution, we borrow and combine the existing concepts of watermarking signal and auxiliary systems in order to detect a broad class of false data injection attacks. We show that by combining the aforementioned concepts, we can detect false data injection attacks without sacrificing control performance. Moreover, we propose a novel nonlinear auxiliary system which is static and does not require any dynamical coupling with the plant dynamics. Finally, the effectiveness of the proposed method is shown by means of a simulation campaign.**

I. Introduction

With the term Cyber-Physical Systems (CPS) we denote physical systems equipped with communication and computation/control capabilities. In the last decade, CPSs have received increasing attention due to their diffusion in the society, see in this regard e.g. the increasing interest towards smart grids, autonomous transportation, industry 4.0, and Internet of Things (IoT) [1]–[3].

From one side, CPSs have undoubtedly the great opportunity of improving the existing engineering systems both in performance and reliability. On the other hand, the increasing computation and communication capabilities bring security concerns. These security challenges must be properly faced otherwise, they might prevent CPS diffusion in safety-critical infrastructures. Several cyber-attacks targeting different CPSs have been reported during the last years [4]–[6].

In a networked control system setup, where the plant and the controller are spatially distributed, of interest are cyber-attacks affecting the communication channels, see Fig. 1. Attackers' capabilities are distinguished according to the available disclosure/disruptive resources and control system knowledge, see [7] for an interesting 3D representation of networked attacks. Of particular interest in the literature are two main classes of cyber-attacks: Denial of Service (DoS) [8], [9] and False Data Injection (FDI) [10], [11] attacks (also known as deception attacks). The firsts aim at jamming the network, preventing the legitimate data to reach their destination node, while the seconds alter transmitted data in order to mislead the receiver with incorrect information.

The attacks considered for this work are well-studied replay, zero-dynamics, and covert attacks which fall under the category of FDI attacks [7]. In the related literature, different attack detection tools have been proposed, see e.g. [12]–[16] and references therein. In [12], the class of FDI attacks on set-point signal is presented and the detection mechanism is proposed. In [13], the authors have investigated the class of undetectable and unidentifiable attacks. They have shown that dynamic detectors outperform static ones and that stealthy attacks against static detectors are easier to be generated. In [16] the class of passive detectors is considered and the authors have explored the conditions under which an attack is stealthy if the defender has partial or complete awareness of the plant initial condition. Moreover, it has been shown that, under certain conditions, even a perfect passive detector cannot detect covert and zero-dynamics attacks. The latter is aligned with the results in [14] where it has been proved that if the attacker is aware of the dynamical model of the system and he/she has complete access to the communication channels, a covert attack is stealthy regardless of the controller and detection algorithms.

The above results motivate researchers to investigate alternative detection solutions, see e.g. [17]–[21]. In [18], a coding scheme for sensor measurements is proposed to detect stealthy sensor false data injection attacks. In [17], a watermarking signal is superposed on the control command in order to detect replay attacks. The method in [19] is an improvement to [17], where a sub-optimal solution is presented to obtain a trade-off between detection rate and control performance degradation. In [20], the authors have presented a novel control architecture to detect covert attacks. In particular, the plant dynamics are augmented by resorting to an auxiliary switching system (the moving target). These extra dynamics are randomly changed in time and coupled with the plant dynamics to prevent attackers from obtaining perfect model knowledge. As a result, covert attacks are not doable. A quite similar result is also obtained in [21]. The main difference relies on the design of the extended dynamics which in [20] are completely random and in [21] are designed to resemble the plant dynamics.

From above non exhaustive discussion of the state-of-the-art, it is possible to appreciate that different solutions have been proposed to avoid the presence of stealthy attacks. Nevertheless, the resulting control schemes might work only against specific type of attacks [18], or affect the control performance [17], [19] or be too involved [20], [21]. In this paper we aim at combining auxiliary system and watermarking idea in order to design a novel control architecture

This work was supported by the Natural Science and Engineering Council of Canada under Grant RGPIN2018-06713

Mohsen Ghaderi is with the Electrical and Computer Engineering Department (ECE), Concordia University, Montreal, QC, H3G 1M8, CANADA, m_haderi@encs.concordia.ca

Walter Lucia and Kian Gheitasi are with the Concordia Institute for Information Systems Engineering (CIISE), Concordia University, Montreal, QC, H3G 1M8, CANADA, walter.lucia@concordia.ca, k_gheita@encs.concordia.ca

978-1-5386-7926-5/$31.00 ©2019 AACC

where the detector module is capable of detecting FDI attacks such as replay, zero-dynamics, and covert attacks. We will show that we can achieve a watermarked signal without compromising the system performance and that the auxiliary system could be a simple static nonlinear function which does not need to be coupled with the plant dynamics.

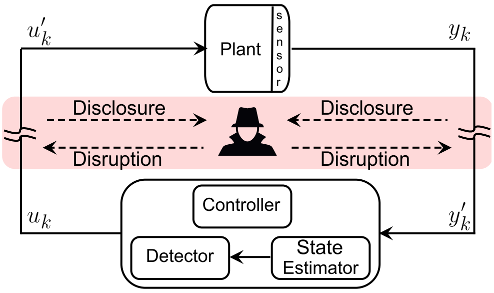


Fig. 1. Networked Control System

II. Preliminaries

Let us consider the networked control system shown in Fig. 1 where we assume that the communication channels are vulnerable to cyber-attacks and data transmitted might be altered by an adversary.

A. System Model

The plant is modeled as the following discrete-time LTI system:

$$\begin{array}{rcl} x_{k+1} & = & Ax_k + Bu'_k + \omega_k \\ y_k & = & Cx_k + \eta_k \end{array} \tag{1}$$

where $k \in \mathbb{Z}_+ := \{0, 1, ...\}$ is the sampling time instant, $x \in \mathbb{R}^n$, $u'_k \in \mathbb{R}^m$, and $y_k \in \mathbb{R}^p$ are states of the plant, received control action, and sensor measurements, respectively. ω_k is an independent and identically distributed (IID) process noise normally distributed with zero mean $\omega_k \sim \mathcal{N}(0, \mathcal{Q})$ and $\mathcal{Q} > 0$. η_k is an independent and identically distributed (IID) measurement noise distributed normally with zero mean $\eta_k \sim \mathcal{N}(0, \mathcal{R})$ and $\mathcal{R} > 0$.
By assuming that the plant (1) is detectable and stabilizable, we consider the steady-state kalman filter as the remote state-estimator

$$\begin{array}{rcl} \hat{x}_{k+1|k} & = & A\hat{x}_k + Bu_k \\ \hat{x}_{k+1} & = & \hat{x}_{k+1|k} + L(y'_{k+1} - C\hat{x}_{k+1|k}) \end{array} \tag{2}$$

where y'_k is the measurement vector received by the state estimator module, $u_k \in \mathbb{R}^m$ is computed control input, $\hat{x}_{k|k-1}$ is the a-priori predicted estimation, and $\hat{x}_{k+1}$ is the a-posteriori state estimation. $L = PC^T(CPC^T + R)^{-1}$, with $P = P^T \geq 0$ the only positive semi definite solution of the Riccati equation

$$P = APA^T + Q - APC^T(CPC^T + R)^{-1}CPA^T$$

For anomaly/attack detection purpose, the following $\mathcal{X}^2$ test is used

$$g_k \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \beta \tag{3}$$

where

$$g_k = \sum_{i=k-\mathcal{J}+1}^{k} e_i^T \mathscr{P}^{-1} e_i \tag{4}$$

and

$$e_i := y'_i - C\hat{x}_{i|i-1} \tag{5}$$

is the filter innovation at the step i, $\mathscr{P} := CPC^T + R$ is the innovation covariance, $\mathcal{J}$ is the length of the observation time window, $\mathcal{H}_0$ and $\mathcal{H}_1$ denote the attack-free and under-attack hypothesis, respectively, and $\beta > 0$ is the threshold value which is chosen according to the plant disturbance/noise as the best compromise between the probability of detection and the probability of false alarms [22].

B. Attack Model and Resources

In this subsection, the considered cyber-attacks are defined both in terms of capabilities and resources. By referring to Fig. 1, we model a networked FDI as follows

$$\begin{array}{l} u'_k := u_k + u_k^a \\ y'_k := y_k + y_k^a \end{array} \tag{6}$$

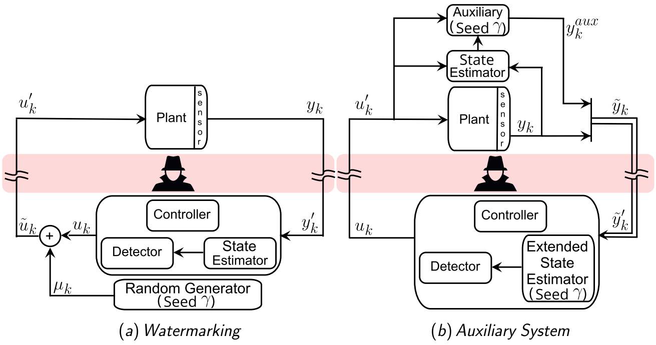
where $u_k^a \in \mathbb{R}^m$ and $y_k^a \in \mathbb{R}^p$ are vectors injected by the attackers in the actuation and measurement channels, respectively.

III. Problem Formulation

In this section, the considered problem is first introduced and then main limitations/drawbacks of existing approaches are highlighted.
The control problem of interest is the following:
Detection of false data injection attacks: *Given the networked control system shown in Fig. 1 subject to FDI attacks (6), design a detection mechanism capable of avoiding the existence of undetectable FDI attacks without compromising the control system performance.*

Since the considered problem is not new in the CPS community, it is important to clarify why we want to propose a novel detection mechanism to prevent stealthy Replay, Zero-Dynamics and Covert Attacks. To this end, we will briefly discuss the limitations of two well-known approaches based on the ideas of auxiliary systems and watermarking signal, see Fig. 2:

- *Watermarked control inputs*: By denoting with u_k the "optimal" control action prescribed by the controller, then the watermarked signal $\tilde{u}_k := u_k + \mu_k$ is by definition a non optimal solution . It is shown that by increasing the magnitude of μ_k, the attack detection probability increases while the control system performance decreases [17], [19], [23]. As a consequence, a trade-off between the two contrasting objectives must be reached. Moreover, watermarking solutions are effective in preventing steady-state replay attacks, but they are ineffective against covert and zero-dynamics attacks.
- Auxiliary systems: A randomly switching dynamical auxiliary system is coupled with the plant dynamics [20], [21]. It introduces auxiliary sensor measurements



(a) *Watermarking* (b) *Auxiliary System*

Fig. 2. (a) Networked control architecture with superimposed watermarking signal, (b) Networked control architecture with a switching auxiliary system local to the plant.

which need to be transmitted over the network along with the plant outputs. For coupling the auxiliary and the system, a state estimation module needs to be deployed on the plant side. In addition, the detection scheme must be extended to take into account the switching auxiliary dynamics. The solution is effective against covert and replay attacks; however, there are no existing results showing its effectiveness against zero-dynamics attacks.

Starting from the above analysis, the question to which we provide a solution is the following

Is it possible to combine watermarking and auxiliary system ideas to design a control architecture capable of detecting FDI attacks while avoiding limitations and complexity of existing approaches?

IV. Proposed Control Architecture and Detector Module

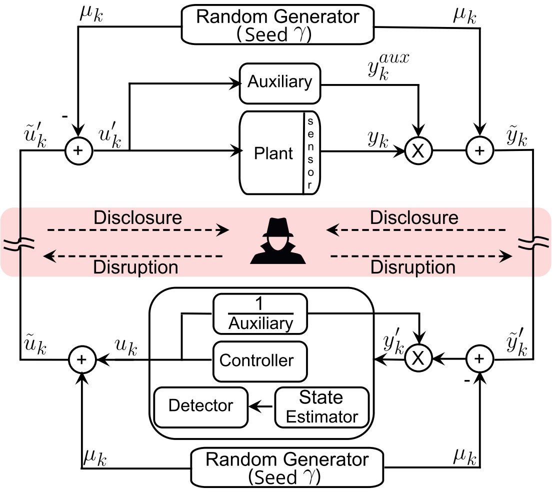


Fig. 3. Proposed networked control architecture

The proposed control architecture is shown in Fig. 3. It consists of the following main ingredients:

- The standard networked control architecture (plant, sensors, controller, state estimator, communication infrastructure, and cyber-attacks detector);
- Two pseudo random number generators (on both plant and controller sides) sharing the same seed γ and producing the same random signal μ_k.
- An auxiliary non-zero single-valued nonlinear function $\mathcal{F} : u'_k \to \mathcal{F}(u'_k)$ where $u'_k \in \mathbb{R}^m$ and $\mathcal{F}(u'_k) := y_k^{aux} \in (\mathbb{R} \setminus 0)$.

In a nutshell, the main features of the proposed control architecture are: the watermarking signals μ_k intentionally corrupt the data before they are transmitted in order to mitigate the attacker's awareness of the control system operations; the twin random generators on both the plant and controller sides allow us to arbitrary corrupt the transmitted data and to recover the original data once they reach their legitimate destination; the non-zero single-valued function $\mathcal{F}$ allows us to design an auxiliary system which is not coupled with plant dynamics and avoids any stealthy attack based on the zero-dynamics of (1); the multiplicative block between the plant outputs and the auxiliary output allows us to keep the size of the transmitted sensor measurements constant. This creates a structural non-linearity, hard to be estimated by the attacker. The following assumption on the operating scenario is made:

Assumption 1: We assume that in the proposed control architecture (Fig. 3) the only secret information is the seed number γ which can be secretly shared between the plant and the controller [24]. Therefore, the plant model, the controller algorithm, the auxiliary function $\mathcal{F}$ and the reference architecture are known to both the defender (Detector) and attacker. □

We can summarize the networked control system operations by means of the following procedure:

Networked Control System - Operations (***NCS-O***)

———— *controller-side* ————

Receive: $\tilde{y}'_k$, **Send:** $\tilde{u}_k$

1: The watermarking signal μ_k and the contribution given by the auxiliary system are removed from $\tilde{y}'_k$, i.e.

$$y'_k = \frac{\tilde{y}'_k - \mu_k}{\mathcal{F}(u_k)} \tag{7}$$

2: The estimator takes u_k and y'_k and compute the best estimation $\hat{x}_k$ according to the Kalman filter (2);

3: The detection rule (3) is used to verify the presence of FDI attacks;

4: The controller computes the control action u_k (the control logic can be either a state-feedback controller or an output controller and this is irrelevant for the purpose of this paper);

5: The watermarking signal μ_k is superposed on u_k, i.e. $\tilde{u}_k = u_k + \mu_k$;

6: The command $\tilde{u}_k$ is transmitted.

```
———— plant-side ————
Receive: $\tilde{u}'_k$, Send: $\tilde{y}_k$
The watermarking signal $\mu_k$ is removed from the received command $\tilde{u}'_k$, i.e. $u'_k = \tilde{u}'_k - \mu_k$;
The Auxiliary output is computed, i.e. $y^{axu}_k = \mathcal{F}(u'_k)$;
First the plant output vector $y_k$ is multiplied by the scalar $y^{aux}_k$ and then the watermarking signal $\mu_k$ is superimposed
    $\tilde{y}_k = (y_k y^{aux}_k) + \mu_k;$    (8)
The command $\tilde{y}_k$ is transmitted.
```

A. Attack Detection and Auxiliary System

It is possible to prove (the proof is omitted for the sake of space) that the stealthy attack condition $y'_k = y_k, \forall\, k$ can never be reached by an attacker regardless of the available resources. However, for the sake of completeness, it is important to mention that the proposed detector might not be able, in theory, to detect covert FDI attacks producing small innovation errors e_k. Nevertheless, such event is unlikely for the following reasons:

In the Kalman filter, in the absence of attacks, the estimation error asymptotically converges to zero and the mean value of the innovations process, namely $E[e_k]$,

$$E[e_k] = E[y'_k - C\hat{x}_{k|k-1}] = E[y_k - C\hat{x}_{k|k-1}] \tag{9}$$

is a Gaussian white noise with zero mean. In presence of FDI attacks u^a_k and y^a_k the output vector y'_k changes as follows:

$$\begin{aligned} y'_k &= \tfrac{\tilde{y}'_k - \mu_k}{\mathcal{F}(u_k)} = \tfrac{(\tilde{y}_k + y^a_k) - \mu_k}{\mathcal{F}(u_k)} \\ &= \tfrac{(y_k \mathcal{F}(u'_k) + \mu_k + y^a_k) - \mu_k}{\mathcal{F}(u_k)} = \tfrac{y_k \mathcal{F}(u_k + u^a_k) + y^a_k}{\mathcal{F}(u_k)} \end{aligned} \tag{10}$$

By substituting (10) into (9) we obtain

$$E[e_k] = E\left[\frac{y_k \mathcal{F}(u_k + u^a_k) + y^a_k}{\mathcal{F}(u_k)} - C\hat{x}_{k|k-1}\right] \tag{11}$$

where the mean value is now a function of $\mathcal{F}(\cdot)$, y^a_k, and u^a_k. It is evident that, an attacker, to satisfy the $\mathcal{X}^2$ test (3), has to keep the mean value of the innovation small. This can be achieved only if the attacker can find an accurate solution $\forall\, k$ to the optimization problem:

$$y^a_k = y_k \left(\mathcal{F}(u_k) - \mathcal{F}(u_k + u^a_k)\right) \tag{12}$$

However, such task is not well posed for the attacker because the vectors u_k, y_k are unknown and $\mathcal{F}$ is nonlinear. Furthermore, since $\mathcal{F}$ is a free parameter, we can design such a function to be very sensitive to small variation of its input, e.g. $\mathcal{F}(u_k + u^a_k) >> \mathcal{F}(u_k)$ or $\mathcal{F}(u_k + u^a_k) << \mathcal{F}(u_k)$, and render the innovation error $E[e_k]$ proportional to the magnitude of $\frac{\mathcal{F}(u_k + u^a_k)}{\mathcal{F}(u_k)}$. For instance, an exponential auxiliary function, e.g. $\mathcal{F}(u'_k) := e^{||u'_k||^2_2}$, represents a good candidate because it meets the desired requirements (single values, non-zero, nonlinear) plus it is very sensitive to small variation of its input.

B. Advantages of the proposed solution

It is possible to summarize the main advantages of the proposed control scheme with respect to the competitor schemes [17], [19], [20], [21] (please refer to Section III for a detailed discussing about their drawbacks) as follows:

- *Attack detection:* The proposed control scheme is capable to detect zero-dynamics, replay and covert attacks. Moreover, the sensitivity of the attack detector can be increased by properly designing the auxiliary function $\mathcal{F}$.
- *Control performance:* In absence of attacks, the control system performance is not affected. E.g. the watermarking signal does not reduce the control system performance therefore it can be increased in order to improve detection of replay attacks.
- *Architecture:* The auxiliary function $\mathcal{F}$ is a static function which does not need to be secret or dynamically coupled with the plant. The size of measurement vector is not increased due to the presence of the auxiliary function. The state estimator and $\mathcal{X}^2$ test do not need to deal with an extended state space model or with the presence of the auxiliary system. In conclusion, the designed architecture (Fig. 3) can be deployed without changing the existing communication infrastructure, controller, state estimation, and detector.

V. Simulation Example

In this section, the quadruple-tank system depicted in Fig. 4 is used to show the effectiveness of the proposed attacks-detection strategy against FDI attacks.

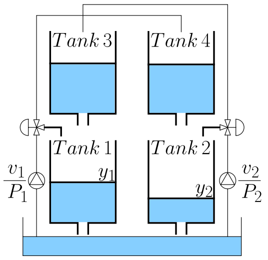


Fig. 4. Quadruple-tank process

In this process, the goal is to regulate the water levels (h_1 and h_2) in the Tanks 1 and 2. The water supplied into the tank is a function of the voltage level (v_1 and v_2) provided to the pumps P_1 and P_2. By denoting with h^0_i the equilibrium heights of water in the Tanks $i = 1, ..., 4$ and with v^0_j the equilibrium voltage for each pump $j = 1, 2$, we can define the system state, input, and output vectors, namely $x = [x_1, x_2, x_3, x_4]^T$, $u = [u_1, u_2]$ and $y = [y_1, y_2]^T$, respectively. Each state component x_i, represent the tank water level deviation from the equilibrium h^0_i, i.e. $x_i := h_i - h^0_i$. The input components u_1, and u_2 are the pumps' voltage deviation from v^0_1, and v^0_2, respectively. Finally, the output components y_1 and y_2 are the water levels in the Tanks 1 and 2.

We assume that the controller is remote to the plant and an insecure networked control system architecture is in place to allow data exchange between the plant and the controller (see Fig. 1).

A linearized state-space representation of the system as in (1) has been obtained by linearizing the system dynamics around the equilibrium vectors $h^0 = [12.4, 12.7, 1.8, 1.4]^T$ and $v^0 = [3, 3]^T$ (see [25] for further details on how the linearized model has been obtained). The matrices A, B, C are

$$A = \begin{bmatrix} -0.016 & 0 & 0.042 & 0 \\ 0 & -0.011 & 0 & 0.033 \\ 0 & 0 & -0.042 & 0 \\ 0 & 0 & 0 & -0.033 \end{bmatrix}$$

$$B = \begin{bmatrix} 0.083 & 0 \\ 0 & 0.063 \\ 0 & 0.048 \\ 0.031 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \qquad (13)$$

In the simulations, we use the following modules

- *Controller:* The controller logic

$$u_k = K_1 \sum e_k - K_2 \hat{x}_{k|k}$$

  consists of a feedback term $K_2\hat{x}_{k|k}$ and a integral feedforward action $K_1 \sum e_k$, where the tracking error e_k is defined as $e_k = r_k - y'_k$. The controller gains are

$$K_1 = 10,$$

$$K_2 = \begin{bmatrix} 0.0013 & -0.0000 & -0.0035 & 0.0010 \\ -0.0000 & 0.0007 & 0.0020 & -0.0021 \end{bmatrix}$$

- *The State Estimator:* The state estimator is the Kalman filter (2)
- *The Detector:* The detection rule is (3) with $\mathcal{J} = 5$. The detection threshold β is chosen according the worst case realization of the system noises in absence of attacks.
- *The Auxiliary function:* As auxiliary function we use

$$\mathcal{F}(u'_k) := e^{||u'_k||_2^2}$$

In the sequel, we perform an intensive simulation campaign to testify the effectiveness of the proposed control architecture (Fig. 3). To this end, replay attack is considered. For the purpose of simulation, the constant reference signal $r = [5,\ 2.5]^T$ has been used. For each attack scenario, we assume that the attacker has the required resources.

A. Replay attack

In this section, the capability of proposed strategy is tested under a replay attack, performed when the system reaches to the steady-state condition. Attack scenario is described as follows:

- Step 1 ($41 \leq k \leq 60;$): $\tilde{y}_k$ is recorded;
- Step 2 ($61 \leq k \leq 80$): the constant input vector $u_k^a = [10, 0]^T$ is injected while the collected measurements $\{\tilde{y}_k\}_{k=41}^{60}$ are replayed instead of $\{\tilde{y}_k\}_{k=60}^{79}$.

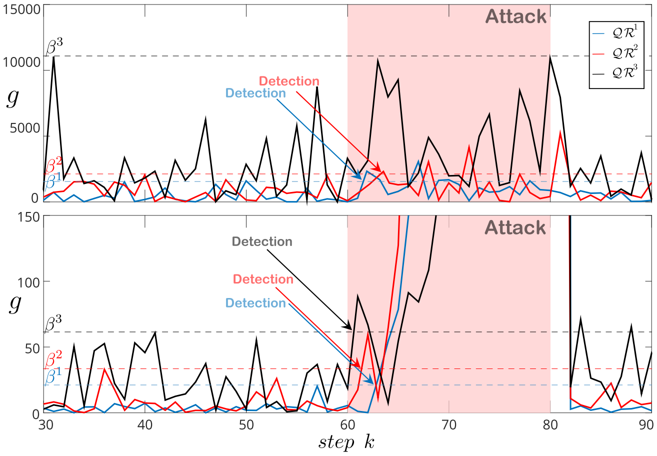


Fig. 5. ***NCS-O*** vs [17] for 3 different levels of system noises. The upper graph is [17] and the lower is ***NCS-O***. The dashed lines show the used threshold β for each level of plant noises. Threshold levels and signals g are matched by color.

We contrast the proposed architecture (Fig. 3) with the method provided in [17] for three different magnitudes of the watermarking signal μ_k. To this end the following covariance matrices are considered:

- $\mu_k^1 \sim \mathcal{N}(0, 1), \quad \mu_k^2 \sim \mathcal{N}(0, 5), \quad \mu_k^3 \sim \mathcal{N}(0, 10)$

Furthermore, we also investigate the detection and control performances for different levels of process and measurement noises (ω_k and η_k), namely:

- $QR^1 = (\mathcal{Q} = 0.3I_4,\, \mathcal{R} = 0.3I_2)$
- $QR^2 = (\mathcal{Q} = 0.6I_4,\, \mathcal{R} = 0.6I_2)$
- $QR^3 = (\mathcal{Q} = 2I_4,\, \mathcal{R} = 2I_2)$

For each level of noise a properly threshold β is used. In [17] the threshold take also into account the superimposed watermarking signal.

The simulation results are collected in the Figs. 5-6. In Fig. 5 we contrast the two methods for three different levels of system noises (QR^1, QR^2, QR^3) when the watermarking signal is fixed (case μ^1). It is possible to notice that the detector performance in [17] deteriorates by increasing the plant and measurement noise levels. In particular, the detector fails to detect the replay attack for QR^3. In [17] the effectiveness of the detector depends on the ratio between the noises and the watermarking signal while in our solution, it depends only on the watermarking magnitude. Also, in the proposed architecture, the tracking performance is not affected by changing the watermarking signal level while in [17] the tracking performance is degraded by increasing watermarking level. Therefore, in [17] the watermarking signal cannot be arbitrary small because it has degradation in detection performance and it cannot be arbitrary big because of degradation in tracking performance. However, in the proposed method, we can arbitrary increase the watermarking signal to improve attack detection rate without reducing the tracking performance.

In Fig. 6 we contrast the two methods for three different levels of the watermarking signals (μ_k^1, μ_k^2, and μ_k^3,) when

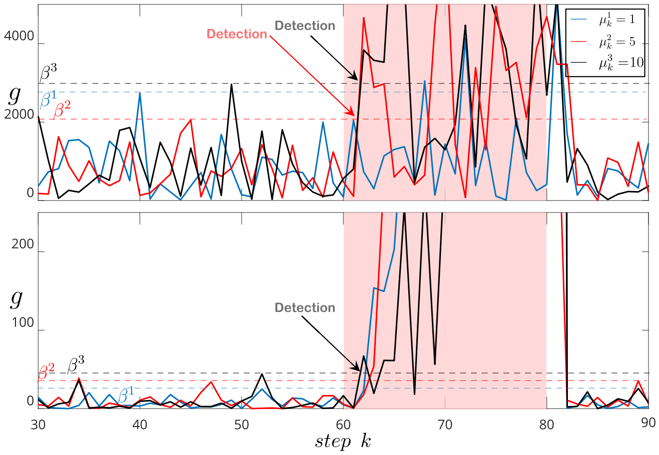


Fig. 6. ***NCS-O*** vs [17] for three different levels of watermarking signal. The upper graph is [17] and the lower is ***NCS-O***. The dashed lines show the used threshold β for each level of watermarking signals μ. Threshold levels and signals g are matched by color.

the noises covariance is fixed (case QR^2). Here it is possible to appreciate that in both methods, bigger the covariance of the watermarking signal is, better the χ^2 detectors perform (see the increasing magnitude of the signal g_k). However, it is important to recall that if we increase the watermarking signal then, in [17] the tracking performance is reduced (in absence of attacks) while for the proposed solution this has no impact. The latter finds justification in the fact that in the proposed architecture we superimpose a watermarking signal on u_k which is removed before its application to the plant, see the Step 1 of the ***NCS-O*** algorithm.

VI. Conclusions

In this paper, we have proposed a control architecture capable of detecting FDI attacks in a networked control system. The detection strategy has been obtained by merging and simplifying the exiting concepts of watermarking and auxiliary systems. It has been shown that FDI attacks can be detected regardless of the attacker's available resources. Finally, a numerical example has been presented to show the effectiveness of the proposed strategy.

References

[1] N. Jazdi, "Cyber physical systems in the context of industry 4.0," *IEEE Int. Conference on Automation, Quality and Testing, Robotics*, pp. 1–4, 2014.

[2] G. Xiong, F. Zhu, X. Liu, X. Dong, W. Huang, S. Chen, and K. Zhao, "Cyber-physical-social system in intelligent transportation," *IEEE/CAA Journal of Automatica Sinica*, vol. 2, no. 3, pp. 320–333, 2015.

[3] S. Sridhar, A. Hahn, M. Govindarasu *et al.*, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[4] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," *Int. Conference on Critical Infrastructure Protection*, pp. 73–82, 2007.

[5] M. N. Al-Mhiqani, R. Ahmad, W. Yassin, A. Hassan, Z. Z. Abidin, N. S. Ali, and K. H. Abdulkareem, "Cyber-security incidents: a review cases in cyber-physical systems," *Int. Journal of Advanced Computer Science and Applications*, vol. 9, no. 1, pp. 499–508, 2018.

[6] T. Chen, "Stuxnet, the real start of cyber warfare?[editor's note]," *IEEE Network*, vol. 24, no. 6, pp. 2–3, 2010.

[7] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[8] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," *International Workshop on Hybrid Systems: Computation and Control*, pp. 31–45, 2009.

[9] A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," *IEEE Conference on Decision and Control (CDC)*, pp. 1096–1101, 2010.

[10] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," *American Control Conference (ACC)*, pp. 3344–3349, 2013.

[11] W. Lucia, B. Sinopoli, and G. Franze, "A set-theoretic approach for secure and resilient control of cyber-physical systems subject to false data injection attacks," *Science of Security for Cyber-Physical Systems Workshop (SOSCYPS)*, pp. 1–5, 2016.

[12] W. Lucia, K. Gheitasi, and M. Ghaderi, "A command governor based approach for detection of setpoint attacks in constrained cyber-physical systems," *IEEE Conference on Decision and Control (CDC)*, pp. 4529–4534, 2018.

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

[14] R. S. Smith, "Covert misappropriation of networked control systems: Presenting a feedback structure," *IEEE Control Systems*, vol. 35, no. 1, pp. 82–92, 2015.

[15] A. Hoehn and P. Zhang, "Detection of covert attacks and zero dynamics attacks in cyber-physical systems," *IEEE American Control Conference (ACC)*, pp. 302–307, 2016.

[16] Y. Chen, S. Kar, and J. Moura, "Dynamic attack detection in cyber-physical systems with side initial state information," *IEEE Trans. on Automatic Control*, vol. 62, no. 9, pp. 4618–4624, 2017.

[17] Y. Mo and B. Sinopoli, "Secure control against replay attacks," *Allerton Conf. on Comm., Control, and Computing*, pp. 911–918, 2009.

[18] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Trans. on Control of Network Systems*, vol. 4, no. 1, pp. 106–117, 2017.

[19] F. Miao, M. Pajic, and G. J. Pappas, "Stochastic game approach for replay attack detection," *IEEE Conf. on Decision and Control (CDC)*, pp. 1854–1859, 2013.

[20] S. Weerakkody and B. Sinopoli, "Detecting integrity attacks on control systems using a moving target approach," *IEEE Conference on Decision and Control (CDC)*, pp. 5820–5826, 2015.

[21] C. Schellenberger and P. Zhang, "Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system," *IEEE Conference on Decision and Control (CDC)*, pp. 1374–1379, 2017.

[22] R. Tunga, C. Murguia, and J. Ruths, "Tuning windowed chi-squared detectors for sensor attacks," *2018 Annual American Control Conference (ACC)*, pp. 1752–1757, 2018.

[23] C.-Z. Bai, F. Pasqualetti, and V. Gupta, "Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs," *Automatica*, vol. 82, pp. 251–260, 2017.

[24] B. Ripley, "Thoughts on pseudorandom number generators," *Journal of Computational and Applied Mathematics*, vol. 31, no. 1, pp. 153–163, 1990.

[25] K. H. Johansson, "The quadruple-tank process: A multivariable laboratory process with an adjustable zero," *IEEE Trans. on control systems technology*, vol. 8, no. 3, pp. 456–465, 2000.