2018 European Control Conference (ECC)
June 12-15, 2018. Limassol, Cyprus

Set-Induced Anomaly Detectors for Networked Power Systems under Bias Injection Cyber-Attacks

Efstathios Kontouras[†], Anthony Tzes[††] and Leonidas Dritsas[†††]

***Abstract*— This paper addresses the concept of a set-induced anomaly detector of bias injection cyber-attacks affecting the load frequency control loop of a networked power system. An adversary corrupts the frequency sensor measurements causing abnormal system behavior. A set-theoretic methodology is used for the extraction of a convex and compact polyhedral robust invariant set under the overall discretized network dynamics. An attack is considered disclosed when the state vector exits the invariant set. Simulation studies demonstrate the impact of an intermittent attack on a two-area power plant and provide an assessment of the proposed detector, when the attack happens simultaneously with changes in the power load demand.**

I. Introduction

Modern power grids are based on an extensive network of sensors and smart meters, that provide system measurements at a high resolution. Feedback loops use these measurements, in order to ensure the precise and reliable communication of the various interconnected control areas. Each area processes digitally the acquired data and a suitable course of action is decided. However, the data transmitted from the sensors to the corresponding control centers sometimes travel through unprotected communication channels, leaving the power network vulnerable to cyber-attacks [1, 2].

Attacks on the load frequency control loop of power grids were previously studied in [3]. The impact of a cyber-attack on a two-area power plant was quantified using the concept of positive invariance in [4]. The design of stealthy or covert adversaries was addressed in [5], while the fundamental limitations on the implementation of attack detectors monitoring the network were presented in [6]. A generic framework that classifies different attack scenarios according to the available resources was proposed in [7].

The subject of this work is the study of the load frequency control loop of a power network. In particular, we consider the case where an adversary injects a bias attack signal corrupting the frequency measurements, which are transmitted from the sensors to the automatic generation control unit of the compromised control area. The detector design process is generalized for an arbitrarily large number of interconnected control areas and the simulations concern a case study of the benchmark two-area power plant.

[†]The author is with the Electrical & Computer Engineering Department, University of Patras, Rio 26500, Greece.

[††]The author is with the Electrical & Computer Engineering Program, New York University Abu Dhabi, Abu Dhabi, P.O. Box 129188, United Arab Emirates.

[†††]The author is with the Department of Electrical & Electronic Engineering Educators, School of Pedagogical & Technological Education, ASPETE, Athens 14121, Greece.

Corresponding author's email: kontouras@ece.upatras.gr

This article extends previous results of the authors [8–10] as follows. In comparison to [8, 9], we apply the concept of a set-induced anomaly detector to a power plant that consists of several interconnected control areas, moving on from the trivial study of an isolated control area. The detection mechanism drives an alarm signal, which is triggered when the state vector exits a robust positively invariant polyhedral set. The robustness property is used to amend for any potential system disturbances, such as the power load changes due to the demand of the consumers. In [10], a similar method was developed, but the proposed anomaly detector required two distinct robust invariant sets, in order to determine whether or not an alarm should be activated. The system dynamics were partitioned and each invariant set was associated either with the asymptotically stable or the Lyapunov stable component of the plant. In this work, we extract a single robust invariant set using the overall network dynamics and we simplify the anomaly detection mechanism at the expense of an increased computational effort during the calculation of the invariant set. Our approach remains centralized and it is valid, when we are concerned with the study of islanded power networks. The efficiency of the proposed detector is assessed in terms of a hysteresis-based intermittent attack pattern that causes large frequency and power oscillations.

The rest of the paper is organized in the following manner. In Section II the mathematical model of the power network is sketched and in Section III the detector design method is discussed. In Section IV we present simulation results and in Section V we provide concluding remarks.

II. System Description

Let us consider a networked power system that consists of N interconnected control areas. We assume that each control area is described in terms of the block-diagram depicted in Fig. 1. According to [10], the discrete-time state space model of the overall networked power system can be given as

$$\begin{aligned} S_{net}: x_{net}[k+1] &= A_{net}x_{net}[k] + B_{net}\left[\alpha_{net}, \sigma_{net}[k]\right] + \\ &+ D_{net}\Delta P_{L,net}[k], \quad x_{net}[0] = x_{net,0} \\ y_{net}[k] &= C_{net}x_{net}, \end{aligned} \tag{1}$$

where $k \in \mathbb{N}$ is the time variable.

The state vector of the networked power system contains the states of each control area and is defined as

$$x_{net}[k] = \left[\xi_1^\top[k] \ \dots \ \xi_N^\top[k] \ \ \Delta P_{tie,1}[k] \ \dots \ \Delta P_{tie,N}[k]\right]^\top$$

and the state vector of the i-th control area is defined as

$$\xi_i[k] = \left[\Delta f_i[k] \quad \Delta P_{G,i}[k] \quad z_{1,i}[k] \quad z_{2,i}[k]\right]^\top.$$

The state variables $\Delta P_{tie,i}[k]$ denote the electrical power that is exchanged between the i-th control area and the rest of the network through the tie line interconnection.

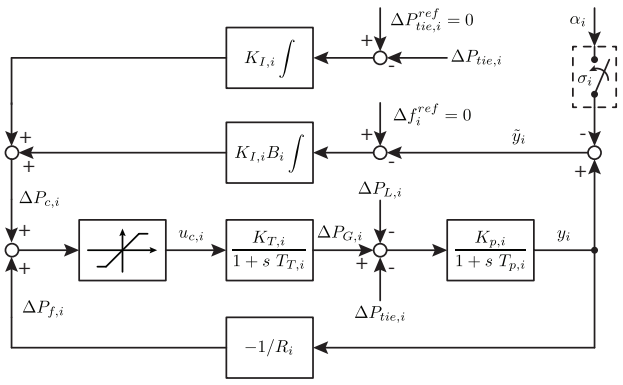

Fig. 1: Load frequency control loop of a generic interconnected control area subject to a bias injection cyber-attack on the frequency measurements. The speed governor dynamics are omitted for brevity.

The state variables $\Delta f_i[k]$ and $\Delta P_{G,i}[k]$ denote the electrical frequency deviation and the deviation of the mechanical power produced in the output of the turbine respectively. On the other hand, $z_{1,i}[k]$, $z_{2,i}[k]$ take the form of accumulated time errors and are the extra state variables, which augment the system due to the presence of the integral control actions regulating the electrical frequency.

The vector of the unknown but bounded disturbances that affect the system as power load changes is defined as

$$\Delta P_{L,net}[k] = \left[\Delta P_{L,1}[k] \quad \Delta P_{L,2}[k] \ \ldots \ \Delta P_{L,N}[k]\right]^\top.$$

The vector α_{net} encapsulates the bias injected signals α_i corrupting the frequency measurements $y_i = \Delta f_i$ as

$$\alpha_{net} = \left[\alpha_1 \quad \alpha_2 \ \ldots \ \alpha_N\right]^\top,$$

the vector σ_{net} encapsulates the switching signals σ_i driving the intermittent attack pattern as

$$\sigma_{net}[k] = \left[\sigma_1[k] \quad \sigma_2[k] \ \ldots \ \sigma_N[k]\right]^\top$$

and each mapping $\sigma_i : \mathbb{N}_+ \to \{0,1\}$ is defined in terms of the hysteresis-based switching signal [11]

$$\sigma_i[k] = \begin{cases} 0 & \text{if} \quad |\tilde{y}_i[k]| > \bar{\alpha}_{i,\max} \quad \text{and} \quad \sigma_i[k-1] = 1 \\ 1 & \text{if} \quad |y_i[k]| < \bar{\alpha}_{i,\min} \quad \text{and} \quad \sigma_i[k-1] = 0 \\ \sigma_i[k-1] & \text{otherwise} \end{cases},$$

where parameters $\bar{\alpha}_{i,\max} = \alpha_{i,\max} - \delta$, $\bar{\alpha}_{i,\min} = \alpha_{i,\min} + \delta$ are the hysteresis bounds and $\delta \in \mathbb{R}^*_+$ is the tolerance factor ensuring that a switching can occur only inside the frequency zone $y_i \in \left[\Delta f^{\alpha}_{i,\min}, \Delta f^{\alpha}_{i,\max}\right] = [\alpha_{i,\min}, \alpha_{i,\max}]$.

The control input driving each control area consists of the primary frequency control action $\Delta P_{f,i}$, which is performed by the speed governor, and the automatic generation control law $\Delta P_{c,i}$, which is digitally implemented. We remark that only the automatic generation control loop can be affected by an adversary in terms of a bias injection cyber-attack, since the speed governor is on many occasions either mechanically or hydraulically coupled with the generator.

The system output vector y_{net}, the explicit representations of the matrices A_{net}, B_{net}, C_{net} and D_{net} and the detailed description of the discretization process used to extract the overall networked system dynamics can be found in [10].

III. Anomaly Detector Design

The key idea behind the design of a set-induced anomaly detection mechanism is to determine a set of state constraints that guarantees the risk-free behavior of the power plant and then compute its maximal robust invariant subset under the overall networked system dynamics.

Large frequency oscillations during the transients are generally undesirable, since they can damage the synchronous generators and the devices of the consumers. According to [4], the frequency deviation Δf_i of each control area should always respect the inequality

$$|\Delta f_i[k]| \leq \Delta f_{i,\max} = 1.5 \ [Hz], \quad \forall k \in \mathbb{N}.$$

The saturation hard constraints imposed on the control law $u_{c,i}$, shown in Fig. 1, also affect its discrete-time counterpart, namely $u_{d,i}$, and have the generic form

$$|u_{d,i}[k]| \leq u_{i,\max}, \quad \forall k \in \mathbb{N}.$$

The aforementioned constraints imply that similar bounds exist for $\Delta P_{G,i}$. According to [10], the mechanical power of the turbine should always respect the inequality

$$|\Delta P_{G,i}[k]| \leq \Delta P_{G,i,\max} = u_{i,\max}, \quad \forall k \in \mathbb{N}.$$

The states $z_{1,i}$ and $z_{2,i}$ are measured in time units and it is necessary to limit the deviation of the synchronous clocks driven by the network frequency. According to [12], the time errors should always respect the inequalities

$$|z_{1,i}[k]| \leq z_{1,i,\max} = 3 \ [s], \quad \forall k \in \mathbb{N}$$
$$|z_{2,i}[k]| \leq z_{2,i,\max} = 3 \ [s], \quad \forall k \in \mathbb{N}.$$

The states $\Delta P_{tie,i}[k]$ are also subject to safety constraints, since large power oscillations stress the tie line to its thermal limits and endanger the stability of the entire grid. The tie line power deviation should always respect the inequality

$$|\Delta P_{tie,i}[k]| \leq \Delta P_{tie,i,\max} = 0.5|P^{\circ}_{tie,i}|, \quad \forall k \in \mathbb{N},$$

where $P^{\circ}_{tie,i}$ denotes the nominal power exchanged between the i-th control area and the rest of the network.

The admissible power load changes on each control area are assumed to be bounded and the corresponding constraints have the generic form

$$|\Delta P_{L,i}[k]| \leq \Delta P_{L,i,\max}, \quad \forall k \in \mathbb{N}.$$

If we combine the above constraints considering all individual control areas, we can express them in terms of the convex and compact polyhedral set

$$\mathcal{X}_{net} = \left\{ x_{net} \in \mathbb{R}^{(n+1)N} : Q_{net} x_{net} \leq q_{net} \right\},$$

where $n = 4$ is the number of the state variables per control area. Accordingly, the set of the admissible values of x_{net} due to the saturation constraints imposed on the control input

of each control area can be expressed in terms of the convex and compact polyhedral set

$$\mathcal{U}_{net} = \left\{ x_{net} \in \mathbb{R}^{(n+1)N} : P_{net} x_{net} \leq p_{net} \right\}.$$

The set of the admissible disturbances can be expressed in terms of the convex and compact polyhedral set

$$\mathcal{W}_{net} = \left\{ \Delta P_{L,net} \in \mathbb{R}^{N} : R_{net} \Delta P_{L,net} \leq r_{net} \right\}.$$

The explicit representations of the sets $\mathcal{X}_{net}$, $\mathcal{U}_{net}$ and $\mathcal{W}_{net}$ can be found in full detail in [10].

Let us consider the networked system dynamics (1) in the absence of an attacker, that is when $\sigma_i[k] = 0$ for all $k \geq 0$ and $i \in \{1, 2, \ldots, N\}$. We remark that according to [10], this condition is equivalent to $B_{net} = 0$. For the design of the set-induced anomaly detector, we can first define the convex and compact polyhedral set $\mathcal{A}_{net} = \mathcal{X}_{net} \cap \mathcal{U}_{net}$ and then determine its maximal robust invariant subset

$$\mathcal{A}_{net,\infty} = \{ \, x_{net,0} \in \mathcal{A}_{net} : A_{net} x_{net}[k] + D_{net} \Delta P_{L,net}[k] \in \mathcal{A}_{net,\infty}, \ \forall \Delta P_{L,net}[k] \in \mathcal{W}_{net}, \ \forall k \in \mathbb{N} \}.$$

An efficient algorithm for the computation of maximal robust invariant subsets under asymptotically stable dynamics was proposed in [13]. However, due to the several integral control actions, the dynamics of the network are Lyapunov stable, which implies that some of the eigenvalues of A_{net} are located exactly on the boundary of the unit circle. This case has also been studied in [13], where the authors developed a method for the extraction of a finite time determined approximation of $\mathcal{A}_{net,\infty}$, namely the set $\hat{\mathcal{A}}_{net,\infty}$. The idea is to separate the system dynamics into an asymptotically stable component and a Lyapunov stable one, which is always possible through a suitable similarity transformation of the state space coordinates. Our modeling approach yields Lyapunov stable eigenvalues with unit values, which is considered by the authors in [13] as the easiest case to handle.

The method used to compute the set $\hat{\mathcal{A}}_{net,\infty}$ is sketched as follows. If the initial set $\mathcal{A}_{net}$ is augmented in terms of properly selected extra state constraints, then it can be shown that the algorithm used in the case of asymptotically stable dynamics converges, allowing us to extract the finite time determined approximation $\hat{\mathcal{A}}_{net,\infty}$. The process used to augment the set $\mathcal{A}_{net}$ is based on the nature of the Lyapunov stable eigenvalues and it is not always the same. After we extract the set $\hat{\mathcal{A}}_{net,\infty}$, we can introduce the alarm signal driving the anomaly detection mechanism as

$$\rho(x_{net}) = \begin{cases} 0 & \text{if} \quad x_{net} \in \hat{\mathcal{A}}_{net,\infty} \\ 1 & \text{otherwise} \end{cases}$$

and we assume that the state vector $x_{net}[k]$ is available to the control center at any given time instant k, in order to decide whether or not an alarm should be triggered.

It is important to highlight that the Lyapunov stable dynamics of the networked model (1) do not allow us to extract robust invariant sets for each control area in a decentralized manner. Therefore, our approach is centralized but it is still valid if we consider the case of an islanded power network operating isolated from the rest of the grid [10].

IV. Simulation Studies

We study the benchmark two-area power network when an adversary attacks the first control area with an intermittent bias injected signal α_1. The parameters used in the simulations are provided in TABLE I. For completeness, we provide

Parameter	Symbol	Area 1 Value	Area 2 Value	Units
Power Base	$P_{B,i}$	2000	1500	MW
Load Dependency Factor	D_i	16.66	10.5	MW/Hz
Speed Droop	R_i	1.2×10^{-3}	1.33×10^{-3}	Hz/MW
Generator Inertia Constant	H_i	5	4	s
Turbine Static Gain	$K_{T,i}$	1	1	MW/MW
Turbine Time Constant	$T_{T,i}$	0.3	0.25	s
Area Static Gain	$K_{p,i}$	0.06	0.095	Hz/MW
Area Time Constant	$T_{p,i}$	24	22.85	s
Controller Static Gain	$K_{I,i}$	0.5	0.45	$1/s$
Control Input Bound	$u_{i,\max}$	600	450	MW
Power Load Bound	$\Delta P_{L,i,\max}$	20	15	MW

TABLE I: Parameter values for the two-area power plant *Source:* [12].

the formulas associated with the static gains $K_{p,i}$ and the time constants $T_{p,i}$ as

$$K_{p,i} = \frac{1}{D_i}, \quad T_{p,i} = \frac{2 H_i P_{B,i}}{f^{\circ} D_i}.$$

The simulations start with $k = 0$, the initial condition is $x_{net}[0] = 0$ and the duration is the time interval $t \in [0, 40]$. Considering a global sampling frequency $f_s = 100 \ [Hz]$ we have $k \in [0, 4 \times 10^3]$. The efficiency of the proposed anomaly detection mechanism has to be assessed when the networked system evolves in the presence of unknown disturbances. To this end, we assume that the two-area power plant is subject to the following power load changes

$$\Delta P_{L,1}(t) = 20 \ [MW], \quad t \geq 0 \ [s]$$

$$\Delta P_{L,2}(t) = \begin{cases} 0 \ [MW], & 0 \leq t < 20 \ [s] \\ -5 \ [MW], & t \geq 20 \ [s] \end{cases}.$$

The nominal electrical frequency of the power network is $f^{\circ} = 50 \ [Hz]$, the tie line is assumed to be lossless, the nominal exchanged power is $P^{\circ}_{tie,1} = -P^{\circ}_{tie,2} = 1000 \ [MW]$ and the synchronization coefficients of the tie line are given as $T_{12} = T_{21} = 175 \ [MW/rad]$. For the polyhedral operations we used the MPT Toolbox 3.0 [14].

In Figs. 2, 3, we present the time evolution of the various state variables considering two distinct attack scenarios. The graphs of $z_{1,i}$ are similar to those of $z_{2,i}$ and are omitted for brevity. The first scenario is presented in Figs. 2, 4 and involves the attack signals $\alpha_1 = 4.5 \ [Hz]$ and $\alpha_2 = 0 \ [Hz]$, whereas the second scenario is presented in Figs. 3, 4 and involves the attack signals $\alpha_1 = 2.0 \ [Hz]$ and $\alpha_2 = 0 \ [Hz]$. In both cases, the switching bounds of $\sigma_1[k]$ were selected as $\alpha_{1,\min} = 0.01 \ [Hz]$ and $\alpha_{1,\max} = 0.1 \ [Hz]$, while the tolerance is $\delta = 10^{-3}$. We remark that the value of $\alpha_{1,\min}$ is meaningful only if it is reasonably larger than the frequency sensor measurement error ($\sim 10^{-3}$).

We highlight that, on both occasions, the adversary is activated only during brief intervals, but he is able to inflict considerable damage. In fact, during an approximately 5 $[s]$ oscillation, the intermittent pattern $\sigma_1[k]$ causes the attacker

to remain active only for approximately 0.5 $[s]$. Furthermore, the switching signal causes the variables Δf_i to oscillate. Although these oscillations have not a significant amplitude, they cause in turn large persistent and non-decaying oscillations of $\Delta P_{tie,i}$. We remark that the oscillations of $\Delta P_{tie,i}$ are generally undesirable, since they stress the tie line and may cause the coupled generators to desynchronize. We also emphasize on the fact that the impact of the attack on the variables $z_{1,i}$ and $z_{2,i}$ is critical, since the accumulated time errors are forced to diverge linearly towards infinity for as long as the adversary is active [10].

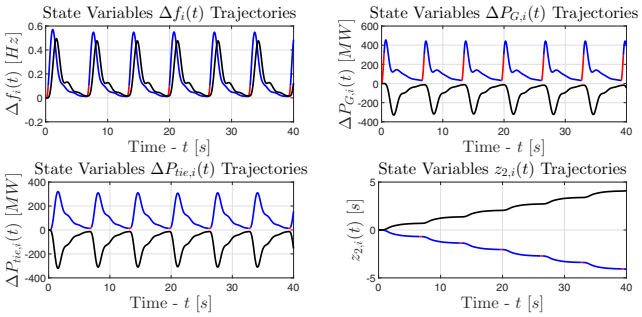

Fig. 2: State variable trajectories for $\alpha_1 = 4.5$ $[Hz]$ and $\alpha_2 = 0$. The variables of area 1 are printed in blue (●), while the variables of area 2 are printed in black (●). An active attacker is indicated with red (●).

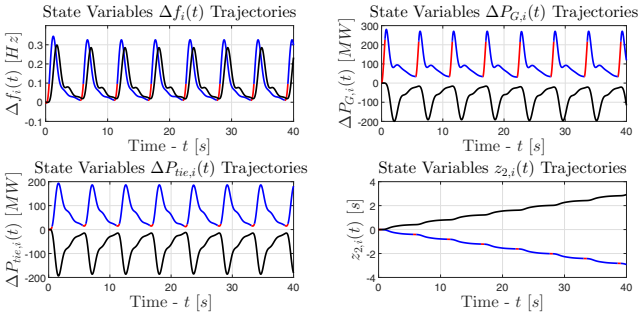

Fig. 3: State variable trajectories for $\alpha_1 = 2.0$ $[Hz]$ and $\alpha_2 = 0$.

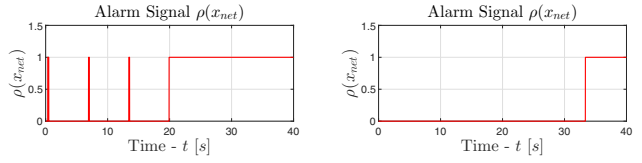

Fig. 4: Alarm signal over time for an attack with $\alpha_1 = 4.5$ $[Hz]$ and $\alpha_2 = 0$ *(left)* and for an attack with $\alpha_1 = 2.0$ $[Hz]$ and $\alpha_2 = 0$ *(right)*.

Finally, from Fig. 4, we observe that in both scenarios the set-induced anomaly detector successfully triggers an alarm. We should also mention that no matter how small the value of the attack signal becomes, the convex and compact set used in the implementation of the anomaly detector along with the gradual increase of $z_{1,i}$ and $z_{2,i}$, ensure that the adversary will always be disclosed, as long as his attacks are restricted to only one area. However, smaller values of the attack signal may allow the adversary to remain undetected for a significantly longer time interval. The second attack scenario clearly demonstrates such a case.

V. Conclusions

This article concerns the study of a bias injection cyber-attack on the automatic generation control unit of a generic networked power system. An intermittent attack pattern is developed using a hysteresis-based switching signal. It is shown that such an attack incites large frequency and power oscillations on the network jeopardizing the stability of the grid. A set-induced anomaly detector is designed based on a robust invariant set. The ability of the proposed detector to disclose an attack in the presence of disturbances is demonstrated through simulation studies considering a benchmark two-area power plant.

Acknowledgments

The third author wishes to acknowledge financial support from the Special Account for Research of ASPETE through the funding program “Strengthening Research of ASPETE Faculty Members”.

References

[1] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor and V. Vittal, Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance, IEEE Transactions on Power Systems, vol. 20, no. 4, 2005, pp. 1922-1928.

[2] A. Teixeira, H. Sandberg and K. H. Johansson, Networked Control Systems under Cyber Attacks with Applications to Power Networks, American Control Conference, Baltimore, MD, USA, 2010, pp. 3690-3696.

[3] G. Franzé, F. Tedesco and A. Casavola, A leader-follower architecture for Load Frequency Control purposes against cyber attacks in power grids - Parts I and II, IEEE 55th Conference on Decision and Control, Las Vegas, USA, 2016, pp. 5128-5133 and pp. 5134-5139.

[4] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros and G. Andersson, Cyber Attack in a Two-Area Power System: Impact Identification using Reachability, American Control Conference, 2010, pp. 962-967.

[5] F. Pasqualetti, F. Dörfler, and F. Bullo, Attack Detection and Identification in Cyber-Physical Systems, IEEE Transactions on Automatic Control, 58(11), 2013, pp. 2715-2729.

[6] F. Pasqualetti, F. Dörfler and F. Bullo, Cyber-Physical Attacks in Power Networks: Models, Fundamental Limitations and Monitor Design, IEEE Conference on Decision and Control and European Control Conference, Orlando, FL, USA, 2011, pp. 2195-2201.

[7] A. Teixeira, D. Pérez, H. Sandberg and K. H. Johansson, Attack Models and Scenarios for Networked Control Systems, Proceedings of the 1st International Conference on High Confidence Networked Systems, Beijing, China, 2012, pp. 55-64.

[8] E. Kontouras, A. Tzes and L. Dritsas, Cyber-Attack on a Power Plant using Bias Injected Measurements, American Control Conference, Seattle, WA, USA, 2017, pp. 5507-5512.

[9] E. Kontouras, A. Tzes and L. Dritsas, Impact Analysis of a Bias Injection Cyber-Attack on a Power Plant, 20th World Congress of the International Federation of Automatic Control, Toulouse, France, 2017, pp. 11586-11591.

[10] E. Kontouras, A. Tzes and L. Dritsas, Set-Theoretic Detection of Bias Injection Cyber-Attacks on Networked Power Systems, American Control Conference, Milwaukee, WI, USA, 2018 *(in print)*.

[11] D. Liberzon, Switching in Systems and Control, Systems & Control: Foundations & Applications, Birkhäuser, 2003.

[12] O. I. Elgerd, Electric Energy Systems Theory: An Introduction, McGraw-Hill, 2nd edition, 1982.

[13] I. Kolmanovsky and E. G. Gilbert, Theory and Computation of Disturbance Invariant Sets for Discrete-Time Linear Systems, Mathematical Problems in Egineering, vol (4), 1998, pp. 317-367.

[14] M. Herceg, M. Kvasnica, C. N. Jones, and M. Morari, Multi-Parametric Toolbox 3.0, In Proceedings of the European Control Conference, Zurich, Switzerland, July 17-19, 2013, pp. 502-510.