Kalpa Publications in Computing

Volume 4, 2018, Pages 12–20

28th International Workshop on
Principles of Diagnosis (DX'17)

Secure state estimation for Cyber-Physical Systems

Gabriella Fiore

University of L'Aquila, DISIM, Center of Excellence DEWS, L'Aquila, Italy
gabriella.fiore@univaq.it

Abstract

In Cyber-Physical Systems (CPSs), physical processes, computational resources and communication capabilities are tightly interconnected. Traditionally, the physical components of a CPS are described by means of differential or difference equations, while the cyber components are modeled by means of discrete dynamics. Therefore, hybrid systems, that are heterogeneous dynamical systems characterized by the interaction of continuous and discrete dynamics, are a powerful modeling framework to deal with CPSs. Motivated by the great importance of security issues for CPSs, we characterize the observability and diagnosability properties for hybrid systems in the general case where the available information may be corrupted by an external attacker. Then, as CPSs are found in a wide range of applications, we demonstrate how to estimate the continuous state by simulating two scenarios: the control of a Direct Current (DC) Microgrid, and the control of a network of Unmanned Aerial Vehicles (UAVs) cooperatively transporting a payload.

1 Introduction

A Cyber-Physical System (CPS) is intended to be the paradigm of a modern control system characterized by the tight interdependence of physical processes, computational resources and communication networks [17]. In particular, a CPS consists of a set of sensors and actuators, connected to controllers and other computational devices with the scope of monitoring and controlling a physical process; devices communicate by means of a (usually wireless) communication network. Traditionally, physical processes are described by means of differential or difference equations, while the computational and communication components are modeled by means of discrete systems. Therefore, due to their nature, CPSs cannot be modeled and designed by simply considering the *union* of tools belonging to the different involved domains (i.e., control of physical processes, software and communication technologies) in a separate way, but their *interaction* must be considered. Indeed, due to the coupling between continuous dynamics and discrete ones, new issues arise which do not directly belong to the above mentioned domains in an exclusive manner, and new tools to deal with them must be proposed. To properly address this heterogeneity, hybrid systems, that are dynamical systems characterized by the interaction of continuous and discrete dynamics, are a powerful modeling framework to deal with CPSs.

On the one hand, the interaction of different domains is an advantageous feature of CPSs, as it allows the modeling and control of a wide range of systems. On the other hand, the strong interconnection between the physical, computational and network layers increases the vulnerability of the entire system to failures or to malicious and intentional attacks by an external attacker. Thus, security measures protecting only the computational and communication layers are necessary but not sufficient for guaranteeing

the safe operation of the entire system against the presence of malicious attackers, and new strategies that explicitly address the strong interconnection between different domains are needed.

There exists a vast literature dealing with security for CPSs (see [1], [31], [22], [9] and references therein). Recent results inspired by the seminal work described in [7], focus on the case in which the attack is sparse, that is, it is not represented by a specific model, its intensity can be unbounded, and it is assumed to compromise only a small subset of sensors and/or actuators. As one of the most important challenges when dealing with security for CPSs is to provide countermeasures to the aim of increasing system's resilience with respect to malicious attacks, one of the main focus of current research is to investigate under which conditions the system's internal state can be correctly estimated, despite the presence of sparse attacks, and to provide efficient algorithms to perform this estimation. The problem of estimating the internal state of a system, when sensors and/or actuators can be corrupted by a malicious attacker, is called "secure state estimation" problem [7]. The secure state estimation problem in presence of sparse attacks has been investigated for two classes of systems: linear systems (both in the noiseless case [7], [8] and in the noisy scenario [20], [30], [19]), and for nonlinear differentially flat systems [28]. Instead, we provide the first contribution to the study of the secure state estimation problem for hybrid systems, due to their paramount importance when dealing with CPSs.

Observability and diagnosability properties of a hybrid system are essential in characterizing the possibility of identifying the system's hybrid state, and in particular the occurrence of some specific states that may correspond to a malfunctioning of the system due to a fault or an attack. The state can be reconstructed instantaneously or within a finite time interval. In particular, observability corresponds to the possibility of determining the current discrete state of the system as well as the continuous one, on the basis of the observed output information [6]. Diagnosability, a property that is closely related to observability but is more general, corresponds to the possibility of detecting the occurrence of particular subsets of hybrid states, for example faulty states, on the basis of the observations within a finite time interval.

Reconstructing the discrete mode corresponds to understanding which continuous dynamical system is evolving. This can be done by using either only the discrete output information (in this case, hybrid discrete state observability corresponds to purely discrete state observability), or by using only the continuous output information (in this case, the reconstruction of the discrete part of the hybrid state corresponds to the possibility of distinguishing between any two continuous dynamical systems), or by using mixed information, both discrete and continuous. In this work, we do not consider the first case. A comprehensive survey of recent results on diagnosis methods for purely discrete event systems can be found in [34], [26], and references therein. Instead, we investigate the second and the third scenarios.

As already mentioned, when only the continuous output information is accessible and the discrete output is not available, the reconstruction of the discrete mode of the hybrid system corresponds to understanding which continuous dynamical system is evolving, in a set of known ones. In other words, this means that, given a pair of continuous dynamical systems, we have to investigate the possibility of *distinguishing* which one of the two systems is active, based on the continuous output and input information. The current discrete mode of the hybrid system can be reconstructed if and only if each pair of dynamical systems can be distinguished. In the nominal case, i.e., if the continuous input and output information can be fully trusted (sensors and actuators are not attacked), different distinguishability notions have been proposed, based on the role of the input function and of the continuous initial state (see [5] for an exhaustive analysis). This problem has been extensively addressed in the literature for hybrid and switching systems when the continuous input and output information is not corrupted by failures or malicious attacks (see [6] and references therein for a complete review of existing results on this topic). In [2] the authors investigate the problem of identifying the current location of a switching system when the continuous measurement signal is corrupted by noise. This disturbance is assumed to have bounded magnitude and therefore the results in [2] do not apply to the case in which the additive

signal is not a measurement noise but an attack performed by a malicious attacker, the magnitude of which can be unbounded. Making use of the formalism introduced in [5] and further developed in [6], where the authors address the problem of discrete state reconstruction for ideal autonomous and controlled hybrid systems, we investigate the scenario in which the continuous input and output signals may be corrupted by additive malicious attacks. In particular, we introduce the *secure distinguishability* property when sensors and/or actuators are corrupted by sparse malicious attacks, and we investigate under which conditions this property holds.

We also consider the more general case in which the current discrete mode is reconstructed by using both the discrete and the continuous output information, when the continuous output can be corrupted by sparse attacks. We propose a formal definition of observability and diagnosability for hybrid systems, and we characterize these properties in the case where the available information may be corrupted by an external attacker. We also propose an abstracting procedure that can be used to determine if a hybrid system is observable and diagnosable. More specifically, this procedure combines the available (corrupted) continuous and discrete information of the hybrid system and obtains an abstracted Finite State Machine (FSM) $\mathcal{M}$. Then, by checking the observability (diagnosability) of the abstracted FSM $\mathcal{M}$ it is possible to infer the observability (diagnosability) of the original hybrid system. To the best of our knowledge, this is the first contribution to the study of the secure state estimation problem for hybrid systems.

In this paper, I provide a brief description of the research activity carried out during my PhD program at the University of L'Aquila, advised by Prof. M.D. Di Benedetto and Prof. E. De Santis. All the details can be found in [9]. Section 2 deals with the first part of the dissertation, that is, the methodological contribution concerning of observability and diagnosability of hybrid systems.

The second part of the dissertation is dedicated to two important case studies, and it is illustrated in Section 3. Motivated by the fact that CPSs are found in a wide range of applications, we demonstrate how to estimate the continuous state (once the discrete state has been recovered) by simulating two scenarios: the control of a Direct Current (DC) microgrid, and the control of a network of Unmanned Aerial Vehicles (UAVs) cooperatively transporting a payload.

2 Secure state estimation of hybrid systems

Hybrid systems provide a powerful modeling framework to deal with a great variety of applications, such as smart grids, automotive and air traffic management systems, unmanned vehicles, and many others. All the above mentioned applications are safety critical, in the sense that their failure can cause irreparable damage to the physical systems being controlled and to the people who depend on it [3], [4]. Even when the disruption of these complex systems is not life threatening for people, it could have a large impact on society, by causing large direct and indirect economic losses. For these reasons, the study of security issues for hybrid systems is presently one of the most significant challenges. In this respect, the observability and diagnosability properties of a hybrid system play an important role. In fact, they are essential in characterizing the possibility of identifying the system's hybrid state, and in particular the occurrence of some specific states that may correspond to a malfunctioning of the system due to a fault or an attack.

One of the most important challenges when dealing with security for hybrid systems is to provide countermeasures to the aim of increasing the resilience of the system with respect to malicious attacks. For this reason, the main focus of our research activity is in investigating under which conditions the system's internal state can be correctly estimated, despite the presence of attacks, and to provide efficient algorithms to perform this estimation.

We suppose that the attack is not represented by a specific model, but it is assumed to be unbounded and influencing only a small subset of sensors and/or actuators, that is, the attack intensity could be

unbounded but it is sparse. More precisely, when the attacker has the ability to compromise $\overline{s}$ nodes on a set of p devices, we define it as a $\overline{s}-$sparse attack. We assume that the actual number of nodes under attack is unknown, but an upper bound is known, that is, $\overline{s} \leq s \ll p$. This assumption is motivated by the fact that it is reasonable to consider that, in a real system, the attacker cannot reach the whole set of monitoring devices. We also assume that the set of attacked nodes is unknown, but fixed over time. This is compatible with the assumption that the attacker does not have arbitrary access to the whole set of devices. Formally, given a vector $x \in \mathbb{R}^n$, $\mathrm{supp}(x)$ is its support, that is the set of indexes of the non-zero elements of x; $\|x\|_0$ is the cardinality of $\mathrm{supp}(x)$, that is the number of non-zero elements of x. The vector $x \in \mathbb{R}^n$ is said to be s-sparse if $\|x\|_0 \leq s$, and $\mathbb{S}_s^n$ indicates the set containing all the s-sparse vectors $x_i \in \mathbb{R}^n$ such that $\|x_i\|_0 \leq s$.

We consider linear hybrid systems as defined in the following.

Definition 1. *A linear hybrid dynamical system (LH-system) is a tuple*

$$\mathcal{H} = (\Xi, \Xi_0, Y, h, S, E, G, R, \delta, \Delta) \tag{1}$$

in which:

- $\Xi = Q \times \mathbb{R}^n$ *is the hybrid state space, where the finite set* $Q = \{1, \ldots, N\}$ *is the discrete state space,* $\mathbb{R}^n$ *is the continuous state space. The hybrid state is* $\xi = (q, x)$ *with* $q \in Q$ *the discrete state (also called mode or location), and* $x \in \mathbb{R}^n$ *the continuous state.*
- $\Xi_0 = Q_0 \times \mathbb{R}^n \subset \Xi$ *is the set of initial hybrid states,* Q_0 *is the set of initial discrete states.*
- $Y = Y_d \times \mathbb{R}^p$ *is the hybrid output space, where the finite set* Y_d *is the discrete output space,* $\mathbb{R}^p$ *is the continuous output space.*
- $h : Q \to Y_d$ *is the discrete output function.*
- S *is a function which associate a linear dynamical system* $S(q)$ *to each discrete state* $q \in Q$*.* $S(q)$ *(also indicated as* S_q*) is described by the following equations:*

$$\begin{aligned} x(t+1) &= A_q x(t) + B_q[u(t) + v(t)] \\ y(t) &= C_q x(t) + w(t) \end{aligned} \tag{2}$$

  where $t \in \mathbb{Z}$*,* $x(t) \in \mathbb{R}^n$ *is the (continuous) state of the system,* $y(t) \in \mathbb{R}^p$ *is the (continuous) output signal,* $u(t) \in \mathbb{R}^m$ *is the (continuous) input signal,* $w(t) \in \mathbb{S}_s^p$ *is the* s*-sparse attack vector on sensor measurements,* $v(t) \in \mathbb{S}_r^m$ *is the* r*-sparse attack vector on actuator signals,* $A_q \in \mathbb{R}^{n \times n}$*,* $B_q \in \mathbb{R}^{n \times m}$*,* $C_q \in \mathbb{R}^{p \times n}$*, for all* $q \in Q$*.*
- $E \subset Q \times Q$ *is the set of admissible discrete transitions. A transition (also called switching) from the discrete state* $i \in Q$ *to* $j \in Q$ *is indicated by the pair* (i, j)*.*
- $G : E \to 2^{\mathbb{R}^n}$ *is the function which associates to the transition* $e \in E$ *a linear subspace* $G(e) \subseteq \mathbb{R}^n$*, called guard set.*
- $R : E \times \mathbb{R}^n \to \mathbb{R}^n$ *is the linear reset function.* $R(e, x) = R_e x$*, with* $R_e \in \mathbb{R}^{n \times n}$*.*
- $\delta : Q \to \mathbb{R}^+$ *is the function which associates to* $q \in Q$ *the minimum dwell time* $\delta(q)$*.*
- $\Delta : Q \to \mathbb{R}^+ \cup \{\infty\}$ *is the function which associates to* $q \in Q$ *the maximum dwell time* $\Delta(q)$*.*

In the following, we describe the property of distinguishing between any two discrete states of the hybrid system, on the basis of the continuous output information only. Then, we focus our attention on observability and diagnosability properties and we outline an abstracting procedure that allows to infer these properties, in the more general case where the output information can be corrupted by an adversarial attacker.

2.1 Secure mode distinguishability

Reconstructing the discrete mode of an LH-system corresponds to understanding which continuous dynamical system is evolving. When the discrete information is not sufficient to identify the discrete state, the possibility of distinguishing between two continuous dynamical systems on the basis of the continuous output information is needed. Thus, in the first part of the dissertation we consider the scenario in which the discrete output is not available and only the continuous input and output signals are accessible, but they can be corrupted by sparse attacks. We provide a formal characterization of the secure distinguishability property both for autonomous systems and for controlled systems, when sensor measurements and actuator signals may be corrupted by sparse attacks. In this case, we provide a geometric characterization of the distinguishability property for all possible initial states, for all sparse attacks on sensors, and for generic corrupted inputs. We also provide bounds on the maximum number of sensors and/or actuators which could be corrupted. Lastly, we provide conditions to detect the occurrence of a transition between two discrete modes of the LH-system, by using only the corrupted continuous output information. These results are described in detail in [13].

2.2 Secure diagnosability and observability of hybrid systems

This section outline the secure diagnosability and observability properties of hybrid system, the results are described in [11]. The main theoretical contribution of the research activity is the formal characterization of the observability and diagnosability properties in the scenario in which both discrete and continuous information is used to reconstruct the system's hybrid state. We consider the more general situation in which the continuous output information can be corrupted by malicious sparse attacks (this is the reason why we define *secure* observability and *secure* diagnosability).

Diagnosability has been extensively studied for Finite State Machines (FSMs) in the last two decades, with different approaches depending on the model, on the available output information, and on the objective for which state reconstruction is needed (see [18], [14], [25], [33], [21], [23], [24], [32] to name a few). Due to the lack of a common formalism, in [26] the authors propose a unifying framework where observability and diagnosability are defined and characterized with respect to a subset of the state space for finite state systems. For this class of systems, time flow is not taken into consideration, so that the results obtained for FSMs cannot, in general, be applied directly to hybrid systems where the discrete evolution interacts with the continuous one. Therefore we propose a formal definition of diagnosability and observability for LH-systems by extending the one provided in [26] for FSMs. We also provide an abstracting procedure that can be used to determine if a hybrid system is observable and/or diagnosable. The abstracting procedure that we propose combines the available continuous and discrete information of the LH-system to obtain an abstracted Finite State Machine. More specifically, we define a partition of the set of discrete states induced by the secure distinguishability relation (between the dynamical systems associated to each discrete mode), and we associate a symbol to each discrete state depending on the equivalence class to which it belongs. Then, we associate an additional binary output to each discrete transition, based on the possibility to detect the transition from the continuous or discrete output information. Finally, we prove that the observability (diagnosability) of the abstracted FSM with purely discrete output corresponds to the observability (diagnosability) of the original hybrid system.

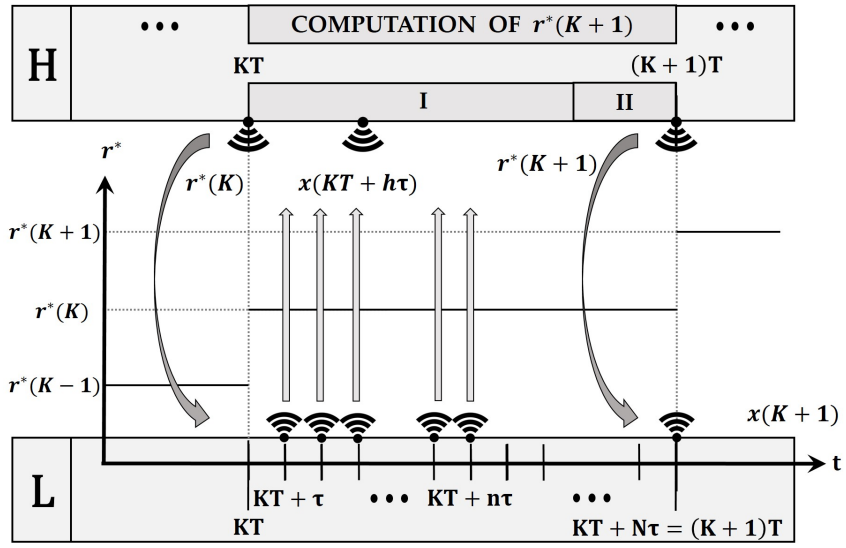

Figure 1: The time scales of the control algorithm. H stands for HL controller, while L for LL controllers. During phase I data acquisition is performed by the HL controller, the state estimation is also performed in order to ensure that the optimization taking place in phase II is based on the system's true state.

Hence, we obtain sufficient conditions for the observability/diagnosability of the given LH-system in the more general scenario in which the continuous output information can be compromised by a malicious attacker.

3 Case studies

In this section we describe two important case studies. Motivated by the fact that CPSs are found in a wide range of applications, we demonstrate how to estimate the continuous state (once the discrete state has been recovered) by simulating two scenarios: the control of a DC microgrid, and the control of a network of UAVs cooperatively transporting a payload.

3.1 Secure state estimation for DC microgrids control

The case study of this section is concerned with the secure state estimation of a DC microgrid, and it is described in [12].

We consider a DC microgrid operating in islanded mode, made up of a photovoltaic array, storage systems in different time scales (e.g., batteries and supercapacitors), and loads (e.g., electric vehicles). The control strategy is implemented with a hierarchical structure, with the objective of ensuring voltage stability of the whole DC microgrid, while properly feeding the load. We take into account the presence of low level controllers (LL controllers), regulating the operating points of the different devices, and a higher level controller (HL controller), sending the optimal reference values to the LL controllers. To the aim of computing the optimal reference values, the HL controller receives sensor measurements sent by the LL controllers, as shown in Fig. 1. This information is assumed to be exchanged through a wireless communication network, which can be compromised by sparse malicious attacks. With the purpose

of guaranteeing the resilience of the DC microgrid despite the presence of the malicious attacker, we simulate a scenario in which the HL controller performs a secure state estimation of the true state of the system, before performing the optimization in phase II. In particular, the HL controller performs the secure estimation algorithm proposed in [29] and further developed in [27] where, thanks to the results in [8] and [29], the authors propose a sound and complete secure state estimation algorithm based on a Satisfiability-Modulo-Theory (SMT) approach [15]. Thanks to this secure state estimation, the hierarchical control strategy proposed in [16] is demonstrated to be robust against the presence of a malicious attacker compromising the communication between the LL controllers and the HL one. The work [12] is the first step in providing a robust solution for a DC microgrid having variable loads and renewable sources, which have to be properly coordinated to ensure stability of the overall system. The microgrid could also be modeled as a hybrid system, with different modes of operation based on the load's typology and on the nature of the employed renewable sources. As the primary concern is to provide service continuity, the security of the overall system must be carefully handled. We leave this extension for future research.

3.2 Secure state estimation for collaborative UAVs payload transportation

In this section we briefly describe the secure state estimation for the control of a network of UAVs transporting a payload [10]. We assume that the communication between the UAVs and a central controller can be compromised by malicious attacks. However, contrary to what has been done in the rest of the dissertation, we do not assume that the attacker influences only a fixed subset of devices. Instead, we consider a different notion of sparsity, which could be defined as "sparsity in time", assuming that the set of attacked nodes can change over time. Then, over a given observation interval, the attacker can compromise only a subset of output information. We also assume that the attacker causes malicious packet drops. However, due to its intentional and adversarial nature, the missing information is not assumed to follow any probabilistic model, we only give bounds on the maximum number of information packet that could be maliciously dropped in a certain interval. Hence, a new detection and estimation method is proposed. Our results show that the proposed strategy allows a perfect recovery of the actual state of the system. Future works include the implementation of a real testbed to validate the proposed method and the extension of the results to the decentralized case, to overcome the limitations imposed by the presence of a central controller.

4 Conclusions

As hybrid systems constitute a powerful modeling framework to deal with CPSs, in [9] we provide the first contribution to the study of security issues for hybrid systems, when the continuous input and output information can be compromised by sparse attacks. In this scenario, we provide a formal characterization of modes distinguishability, observability, and diagnosability. We also propose a procedure to obtain an abstracted FSM from the original hybrid system, by combining the available continuous and discrete information. Sufficient conditions for the observability/diagnosability of the given LH-system cn then be obtained on the basis of observability/diagnosability conditions for the abstracted FSM. Once the discrete state of the hybrid system has been identified, the continuous state can be also recovered. Therefore, in the second part of [9], we demonstrate the continuous state estimation by simulating the control of a DC microgrid and the control of a network of UAVs cooperatively transporting a payload.

5 Acknowledgments

I would like to express my deep gratitude to my advisors Prof. Maria Domenica Di Benedetto and Prof. Elena De Santis for their guidance, encouragement, kindness, and support in developing the results contained in my dissertation, they gave me the right amount of independence while guiding me and encouraging my research activity. It has been a privilege to work with them.

References

[1] S. Amin, A. A. Cárdenas, and S. S. Sastry. Safe and secure networked control systems under denial-of-service attacks. In *Hybrid Systems: Computation and Control*, pages 31–45. Springer, 2009.

[2] M. Baglietto, G. Battistelli, and P. Tesi. Mode-observability degree in discrete-time switching linear systems. *Systems & Control Letters*, 70:69–76, 2014.

[3] A. A. Cárdenas, S. Amin, and S. Sastry. Secure control: Towards survivable Cyber-Physical Systems. In *2008 The 28th International Conference on Distributed Computing Systems Workshops*, pages 495–500, June 2008.

[4] A. A. Cárdenas, S. Amin, and S. S. Sastry. Research challenges for the security of control systems. In *Proceedings of the 3rd Conference on Hot Topics in Security*, HOTSEC'08, pages 6:1–6:6, Berkeley, CA, USA, 2008. USENIX Association.

[5] E. De Santis. On location observability notions for switching systems. *Systems & Control Letters*, 60(10):807–814, 2011.

[6] E. De Santis and M. D. Di Benedetto. Observability of hybrid dynamical systems. *Foundations and Trends in Systems and Control*, 3(4):363–540, 2016.

[7] H. Fawzi, P. Tabuada, and S. Diggavi. Secure state-estimation for dynamical systems under active adversaries. In *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 337–344, Sept 2011.

[8] H. Fawzi, P. Tabuada, and S. Diggavi. Secure estimation and control for Cyber-Physical Systems under adversarial attacks. *Automatic Control, IEEE Transactions on*, 59(6):1454–1467, 2014.

[9] G. Fiore. *Secure State Estimation for Cyber-Physical Systems*. PhD thesis, University of L'Aquila, Department of Information Engineering, Computer Science and Mathematics, 2017.

[10] G. Fiore, Y. H. Chang, Q. Hu, M. D. Di Benedetto, and C. J. Tomlin. Secure state estimation for cyber physical systems with sparse malicious packet drops. In *2017 American Control Conference (ACC)*, pages 1898–1903, May 2017.

[11] G. Fiore, E. De Santis, and M. D. Di Benedetto. Secure diagnosability of hybrid dynamical systems. In *Diagnosability, Security and Safety of Hybrid Dynamic and Cyber-Physical Systems (To appear)*, 2018.

[12] G. Fiore, A. Iovine, E. De Santis, and M. D. Di Benedetto. Secure state estimation for DC microgrids control. In *IEEE International Conference on Automation Science and Engineering (CASE)*, August 2017.

[13] G. Fiore, E. De Santis, and M. D. Di Benedetto. Secure mode distinguishability for switching systems subject to sparse attacks. *IFAC-PapersOnLine*, 50(1):9361 – 9366, 2017. 20th IFAC World Congress.

[14] P. M. Frank. Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy. *Automatica*, 26(3):459 – 474, 1990.

[15] Imhotep-SMT. Imhotep-SMT, a novel SMT-based solver for secure state estimation. http://nesl.github.io/Imhotep-smt/.

[16] A. Iovine, S. B. Siad, G. Damm, E. De Santis, and M. D. Di Benedetto. Nonlinear control of an AC-connected DC MicroGrid. In *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, pages 4193–4198, Oct 2016.

[17] E. A. Lee and S. A. Seshia. *Introduction to embedded systems: A Cyber-Physical Systems approach*. Lee & Seshia, 2011.

[18] F. Lin. Diagnosability of discrete event systems and its applications. *Discrete Event Dynamic Systems*, 4(2):197–212, 1994.

[19] S. Mishra, Y. Shoukry, N. Karamchandani, S. Diggavi, and P. Tabuada. Secure state estimation against sensor attacks in the presence of noise. *IEEE Transactions on Control of Network Systems*, PP(99):1–1, 2016.

[20] M. Pajic, I. Lee, and G. J Pappas. Attack-resilient state estimation for noisy dynamical systems. *IEEE Transactions on Control of Network Systems*, 2016.

[21] A. Paoli and S. Lafortune. Safe diagnosability for fault-tolerant supervision of discrete-event systems. *Automatica*, 41(8):1335 – 1347, 2005.

[22] F. Pasqualetti, F. Dorfler, and F. Bullo. Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems. *IEEE Control Systems*, 35(1):110–127, Feb 2015.

[23] Y. Pencolé. Diagnosability analysis of distributed discrete event systems. In *Proceedings of the 16th European Conference on Artificial Intelligence*, ECAI'04, pages 38–42, Amsterdam, The Netherlands, The Netherlands, 2004. IOS Press.

[24] W. Qiu and R. Kumar. Decentralized failure diagnosis of discrete event systems. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 36(2):384–395, March 2006.

[25] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 40(9):1555–1575, Sep 1995.

[26] E. De Santis and M.D. Di Benedetto. Observability and diagnosability of finite state systems: A unifying framework. *Automatica*, 81:115 – 122, 2017.

[27] Y. Shoukry, M. Chong, M. Wakaiki, P. Nuzzo, A. L. Sangiovanni-Vincentelli, S. A. Seshia, J. P. Hespanha, and P. Tabuada. SMT-based observer design for cyber-physical systems under sensor attacks. In *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*, pages 1–10, April 2016.

[28] Y. Shoukry, P. Nuzzo, N. Bezzo, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada. Secure state reconstruction in differentially flat systems under sensor attacks using satisfiability modulo theory solving. In *2015 54th IEEE Conference on Decision and Control (CDC)*, pages 3804–3809, Dec 2015.

[29] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada. Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach. *IEEE Transactions on Automatic Control*, 62(10):4917–4932, Oct 2017.

[30] Y. Shoukry and P. Tabuada. Event-triggered state observers for sparse sensor noise/attacks. *IEEE Transactions on Automatic Control*, 61(8):2079–2091, Aug 2016.

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

[32] L. Ye and P. Dague. An optimized algorithm of general distributed diagnosability analysis for modular structures. *IEEE Transactions on Automatic Control*, 62(4):1768–1780, April 2017.

[33] T.-S. Yoo and S. Lafortune. Polynomial-time verification of diagnosability of partially observed discrete-event systems. *IEEE Transactions on Automatic Control*, 47(9):1491–1495, Sep 2002.

[34] J. Zaytoon and S. Lafortune. Overview of fault diagnosis methods for discrete event systems. *Annual Reviews in Control*, 37(2):308 – 320, 2013.