The Journal of Systems and Software 149 (2019) 174–216

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

State of the art of cyber-physical systems security: An automatic control perspective

Yuriy Zacchia Lun[a], Alessandro D'Innocenzo[b], Francesco Smarra[b], Ivano Malavolta[c,*], Maria Domenica Di Benedetto[b]

[a] IMT School for Advanced Studies, Lucca, Italy
[b] Department of Information Engineering, Computer Science and Mathematics, & Center of Excellence DEWS, University of L'Aquila, Italy
[c] Vrije Universiteit Amsterdam, Amsterdam, The Netherlands

ARTICLE INFO

Article history:
Received 2 May 2017
Revised 7 August 2018
Accepted 3 December 2018
Available online 7 December 2018

Keywords:
Cyber-physical systems
Security
Systematic mapping study

ABSTRACT

Cyber-physical systems are integrations of computation, networking, and physical processes. Due to the tight cyber-physical coupling and to the potentially disrupting consequences of failures, security here is one of the primary concerns. Our systematic mapping study sheds light on how security is actually addressed when dealing with cyber-physical systems from an automatic control perspective. The provided map of 138 selected studies is defined empirically and is based on, for instance, application fields, various system components, related algorithms and models, attacks characteristics and defense strategies. It presents a powerful comparison framework for existing and future research on this hot topic, important for both industry and academia.

1. Introduction

Cyber-physical systems (CPS) are integrations of computation, networking, and physical processes (Lee and Seshia, 2015; Cárdenas et al., 2008a). The key characteristic of cyber-physical systems is their seamless integration of both hardware and software resources for computational, communication and control purposes, all of them co-designed with the physical engineered components (Poovendran, 2010).

The economic and societal potential of cyber-physical systems is astonishing, and major investments are being made worldwide to develop the technology. For instance, the December 2010 report of the U.S. President's Council of Advisors on Science and Technology (Holdren et al., 2010) called for continued investment in CPS research because of its scientific and technological importance as well as its potential impact on grand challenges in a number of sectors critical to U.S. security and competitiveness, including aerospace, automotive, chemical production, civil infrastructure, energy, healthcare, manufacturing, materials and transportation. Also, the anticipated funding to research and education projects on CPS amounts to approximately $34,000,000 each year (NSF, 2016), and the European Union has a similar vision on the importance of research on CPS (Allocca and Wavering, 2013).

Applications of CPS arguably have the potential to dwarf the 20-th century IT revolution (Lee and Seshia, 2015). Among the many applications of CPS we can find high confidence medical devices and systems, assisted living, traffic control and safety, advanced automotive systems, process control, energy conservation, environmental control, avionics, instrumentation, critical infrastructure control (electric power, water resources, and communications systems for example), distributed robotics (telepresence, telemedicine), defense, manufacturing, smart structures, etc.

It goes without saying that in this type of systems **security** is a primary concern and, because of the tight cyber-physical coupling, it is one of the main scientific challenges. Indeed, CPS security is attracting several research efforts from different and independent areas (e.g., secure control, intrusion detection in SCADA systems, etc.), each of them with specific peculiarities, features, and capabilities.

However, if on one side having many research efforts from different and independent areas on CPS security confirms its importance from a scientific point of view, on the other side it is very difficult to have a holistic view on this important domain. Under this perspective, even if the progress of research on cyber-physical systems has started more than ten years ago and the various research communities are very active, *the trends, characteristics, and the validation strategies of existing research on CPS secu-*

* Corresponding authors.
E-mail addresses: yuriy.zacchialun@imtlucca.it (Y. Zacchia Lun), i.malavolta@vu.nl (I. Malavolta).

https://doi.org/10.1016/j.jss.2018.12.006
0164-1212/

rity are still unclear. With this work we aim at filling this gap. CPS security is presently investigated in a number of scientific (e.g. in Embedded Systems and Wireless Sensor Networks) communities from different points of view. In this paper we focus on research on CPS security from the point of view of the Automatic Control scientific community. A first motivation for our choice is that most application domains where CPS security is an issue consist of/include distributed feedback-based automation systems. In addition to this, a peculiar characteristic of the Automatic Control research is the attempt to combine in a unifying mathematical framework physical components (e.g. electrical/electronic devices, vehicles, and industrial automation machineries) and cyber components (e.g. SCADA systems, communication protocols, and real-time software) of the CPS, as well as to define rigorous performance and robustness/resilience metrics on security properties based on such unifying mathematical framework.

The **goal of this work** is to identify, classify, and analyze existing research on CPS security from an automatic control perspective in order to better understand how security is actually addressed when dealing with CPS. In particular, we are interested in the works proposing methods or techniques for security enforcing or breaching in cyber-physical realm. Under this requirement, the studies that do not consider a physical phenomenon of interest, or rely only on the typical IT security practices such as classical encryption, are excluded.

In order to tackle our goal we applied a well-established methodology from the Medical and Software Engineering research communities called **systematic mapping** (Petersen et al., 2015; Kitchenham and Charters, 2007) (see Section 2.3), applying it on the peer reviewed papers which propose and validate a method or technique for CPS security enforcing or breaching. Through our systematic mapping process, we selected 138 primary studies among almost three thousand entries fitting at best three research questions we identified (see Section 3.2). Then, we defined a classification framework composed of more than 40 different parameters for comparing state-of-the-art approaches, and we applied it to all selected studies. Finally, we analyzed and discussed the obtained data for extracting emergent research challenges and implications for future research on CPS security. The main **contributions** of this study are:

- A *systematic review* of current methods and techniques in automatic control for CPS security, useful for both researchers and practitioners since it is not biased from personal experience; in particular, it considers all the studies of the field of interest, not only the known ones, searched with a validated search method, and selects those proposing technical solutions for security enforcing or breaching that are based on automatic control;
- A reusable *comparison framework* for understanding, classifying, and comparing methods or techniques for CPS security from an automatic control perspective;
- A discussion of *emerging research challenges and implications* for future research, that is based on both the empirical results of a systematic mapping within a time span of the first ten years of the field, and the examination of the trends in research on CPS security that have arisen after 2015.

To the best of our knowledge, this paper presents the first systematic investigation into the state of the art of research on CPS security from an automatic control perspective. The results of this study provide a *complete, comprehensive and replicable* picture of the state of the art of research on CPS security, helping researchers and practitioners in finding trends, characteristics, and validation strategies of current research on security-aware cyber-physical (co-)design, intrusion detection, forecast and response, and its future potential and applicability. The provided map presents several characteristics of security of cyber-physical systems that researchers from Automatic Control community care about. In addition to scientists and practitioners from the same community, this survey is useful also to researchers from the different communities also working on cyber-physical systems, since it permits to better understand the concerns that are complementary to their field of interest, opening the possibilities to find a common ground in an easier way. Thanks to the mapping of each feature to the related studies presented explicitly, an interested reader can find immediately the reference to the works of interest.

The **main findings** of our systematic analysis are discussed below:

Publication trends: in the last years there is an increasing need and scientific interest on CPS security, especially on the methods and techniques for security enforcing and breaching. The research on security in the cyber-physical domain is turning more and more into a mature field, with more foundational and comprehensive studies published in the recent years. This research area has a very multidisciplinary nature and it has been broadly considered by scientists with different research interests, such as smart grid, automatic control, communications, networked systems, parallel and distributed systems, etc.

Characteristics and focus: the bulk of the works on CPS security is focused on power grids, while somehow surprisingly, we have not found any work on the cyber-physical security of medical CPS, and only a small part of selected papers is within the application field of secure control of (unmanned) ground vehicles and aerial systems, and of heating, ventilation, and air-conditioning in large functional buildings. All the works considered in this mapping study deal with attacks, in order to either implement or to counteract them: putting together all this studies gives us the possibility to categorize the existing (cyber-physical) attack models. The defense strategies are presented in most of the studies, occupying the central spot of the research efforts on CPS security. The vast majority of the works (89.9%) is concerned with system integrity, threatened by various types of deception attacks. Regarding the considered system components, the approaches considering attacks on sensors and their protection completely dominate the scene; in fact the resilient state estimation (SE) under measurement attacks is a very active research topic within the area of CPS security. Somehow unexpectedly, very few papers consider communication aspects or imperfections and attempt to provide non-trivial mathematical models of the communication; the centralized schemes dominate both attack and defense solutions.

Validation strategies: most advanced and realistic validation methods have been exploited in the power networks application domain, but even there a benchmark is still missing. Even if the repeatability process, capturing how a third party may reproduce the validation results of the method or technique, is recognized as a good scientific practice, we found no studies providing a replication package. So, we put a particular attention on analysis and description of standard test systems and experimental testbeds used by researchers studying various aspects of CPS security.

By presenting and discussing the above mentioned results we are the first to provide a complete, comprehensive and unbiased overview of the state of the art of research in CPS security from an automatic control perspective, thus our work can certainly be useful for both researchers (either young or experienced ones) and practitioners in the field of CPS security. Finally, we use the results of the systematic part of this study for examining the last trends in the field and discussing potential implications for future research on automatic control for CPS security.

Article outline. The article is organized as follows. In Section 2 we provide background notions for setting the context of our study. Section 3 describes in details our research method-

ology in designing, conducting, and documenting the study[1], followed by a discussion of the obtained results in Sections 4, 5 and 6. We discuss the implications for future research on CPS security in Section 7, and related work in Section 8. Section 9 closes the article.

In Appendix A we discuss some additional characteristics of our primary studies, which are not related to CPS security per se, but are still useful to better understand this scientific area. Finally, Appendix B describes limitations and threats to validity of our results.

2. Background

2.1. Cyber-physical systems

The term cyber-physical systems emerged around 2006, when it was coined at the National Science Foundation (NSF) (Lee and Seshia, 2015), with the "cyber" part of the name resulting from the term "cybernetics", introduced as metaphor apt for control systems. Nowadays, CPS can be seen as a family of control systems related to the domain of embedded sensor and actuator networks (Cárdenas et al., 2008a), thus close relative of Process Control Systems (PCS) and of Supervisory Control And Data Acquisition (SCADA) systems. However, the *seamless integration* of computational, communication and control resources, *co-designed* together with physical engineered components (Allocca and Wavering, 2013) is what sets CPS discipline apart (Poovendran, 2010).

2.2. Security of CPS

Uncertainty in the environment, security attacks, and errors in physical devices make ensuring overall system security a critical challenge for CPS (Rajkumar et al., 2010). Furthermore, a cyber-physical coupling allows sophisticated adversaries to perform attacks threatening also other key attributes of the system, first and foremost safety (Koscher et al., 2010; Chen and Abu-Nimeh, 2011). This is the reason why, among several crucial requirements of CPS, today many researchers are interested in various (unique) aspects of CPS security; for example investigating on combined cyber-physical attack models (Teixeira et al., 2015b), and on attack detection and identification monitors (Pasqualetti et al., 2013).

CPS security presents a number of peculiar characteristics that distinguish it from more conventional IT systems security (Stouffer et al., 2015a). For instance, with cyber-physical systems we have real-time requirements, where response is time-critical, modest throughput is acceptable, high delay and/or jitter is not tolerable, and response to human or other emergency interaction is essential. Such systems are often resource-constrained and may not tolerate typical IT security practices. Even the usual definition of security as the combination of three primary security attributes of confidentiality, integrity and availability (Avižienis et al., 2004) assumes for the CPS a completely new meaning (Cárdenas et al., 2008b). Given that the estimation and control algorithms used in CPS are designed to satisfy certain *operational goals*, such as, closed-loop stability, safety, liveness, or the optimization of a performance function, *availability* in CPS can be viewed as the ability to maintain the operational goals by preventing or surviving denial-of-service (DoS) attacks to the information collected by the sensor networks, the commands given by the controllers, and the physical actions taken by the actuators. Similarly, CPS *integrity* aims to maintain the operational goals by preventing, detecting, or surviving deception attacks in the information sent and received by the sensors, the controllers, and the actuators. The intent of *confidentiality* in cyber-physical systems is to prevent an adversary from inferring the *state* of the physical system by eavesdropping on the communication channels between the sensors and the controller, and between the controller and the actuator or by means of side channel attacks (Tiri, 2007) on sensors, controllers and actuators.

2.3. Systematic mapping studies

A systematic mapping study (or scoping study) is a research methodology particularly intended to provide an **unbiased, objective and systematic instrument** to answer a set of research questions by finding all of the relevant research outcomes in a specific research area (CPS security in our paper) (Petersen et al., 2015). Research questions of mapping studies are designed to provide an overview of a research area by classifying and counting research contributions in relation to a set of well-defined categories such as publication type, forum, frequency, assumptions made, followed research method, etc. (Kitchenham and Charters, 2007; Petersen et al., 2008a). The mapping process involves searching and analyzing the literature in order to identify, classify, and understand existing research on a specific topic of interest.

In the recent years many researchers are conducting systematic mapping studies on a number of areas and using different guidelines or methods (e.g., on technical debt (Li et al., 2015b), search-base software engineering (Lopez-Herrejon et al., 2015), model-driven engineering for wireless sensor networks (Malavolta and Muccini, 2014)). In a recent study (Petersen et al., 2015) it emerged that at least ten different guidelines have been proposed for designing the systematic mapping process. We conducted our study by considering the two most commonly accepted and followed guidelines according to Petersen et al. (2015), specifically: the ones proposed by Kitchenham and Charters (2007) and Petersen et al. (2008a), respectively. Also, we refined our mapping process according to the results of a consolidating update on how to conduct systematic mapping studies proposed by Petersen et al. (2015). Finally, due to the various specificities of existing research on CPS (e.g., the presence of many different definitions of CPS, the intrinsic multidisciplinarity of existing research on CPS, etc.), we found it appropriate to tailor the method and classification schemes proposed in the guidelines according to our topic. The method we followed in our systematic study is detailed in Section 3.

2.4. The need for a systematic mapping study on security for CPS

As it was outlined in the introduction, there is a lack of systematic studies on CPS security. In order to ground this claim and establishing the need for performing a mapping study on security for cyber-physical systems, we searched a set of electronic data sources (i.e., those listed in Section 3.3), for systematic studies on security-aware cyber-physical co-design, self-protection and related security mechanisms specific to CPS[2] without any success. None of the retrieved publications was related to any of our research questions detailed in Section 3.2. So, we can claim that our research complements the related works described in Section 8 to investigate the state-of-research about CPS security.

3. Method

The process we followed for carrying on our study can be divided into three main phases, which are the well-accepted ones

[1] Readers mainly interested in the results of our study and future research directions may directly jump to subsequent sections and come back to this section afterwards.

[2] Search performed on January 5, 2015.

for performing a systematic study (Kitchenham and Charters, 2007; Wohlin et al., 2012): planning, conducting, and documenting. In order to mitigate potential threats to validity, some produced artifacts in each phase have been circulated to external experts for independent review. One systematic literature review (SLR) expert and two experts of CPS security reviewed our review protocol and final report independently and we refined them according to their feedback.

3.1. Main phases of systematic survey

In the following we will go through each phase of the process, highlighting its main activities and produced artifacts.

3.1.1. Planning

In this phase we identified the main research questions (see Section 3.2) and we produced a well-defined review protocol describing in details the various steps of our study. The final version of the review protocol is publicly available as part of the replication package of this study[3].

3.1.2. Conducting

In this phase we set the previously defined protocol into practice. More specifically, we performed the following activities:

- *Studies search*: we performed a combination of techniques for identifying the comprehensive set of candidate entries on automatic control for CPS security (see Section 3.3).
- *Studies selection*: we filtered candidate entries in order to obtain the final list of primary studies to be considered in later activities of the review (see Section 3.3).
- *Comparison framework definition*: we defined the set of parameters for comparing the primary studies. The main outcome of this activity is a document explaining the possible values and the meaning of each parameter (see Section 3.5).
- *Data extraction*: we went into the details of each primary study and extracted data according to the comparison framework defined in the previous activity (see Section 3.5).
- *Data synthesis*: we elaborated on the extracted data in order to address each research question of our study. This activity involved both quantitative and qualitative analysis of the extracted data (see Section 3.6).

3.1.3. Documenting

The main activities performed in this phase are: (i) a thorough elaboration on the data extracted in the previous phase with the main aim at setting the obtained results in their context, (ii) the analysis of possible threats to validity, and (iii) the writing of a set of reports describing the performed mapping study to different audiences. Produced reports have been evaluated by SLR- and CPS-experts (this article itself is an instance of produced final report).

3.2. Research questions

It is fundamental to clearly define the research questions of a systematic literature study (Brereton et al., 2007). Before going into the details of the identified research questions, we formulate the goal of this research by using the Goal-Question-Metric perspectives (i.e., purpose, issue, object, viewpoint (Basili et al., 1994)). Table 1 shows the result of the formulation mentioned above.

The goal presented above can be refined into the following main research questions. For each research question we also provide its primary objective of investigation. The research questions of this study are:

Table 1
Goal of this study.

Purpose	Analyze the
Issue	publication trends, characteristics, and validation strategies
Object	of existing methods and techniques for CPS security
Viewpoint	from a researcher's point of view.

- *RQ1 - What are the publication trends of research studies on automatic control for CPS security?*
  Objective: to classify primary studies in order to assess interest, relevant venues, and contribution types.
- *RQ2 - What are the characteristics and focus of existing research on automatic control for CPS security?*
  Objective: to analyze and classify all the existing approaches for automatic control for CPS security with respect to the specific concerns they want to address (e.g., cyber and physical security, secure control, model-based intrusion detection, or any combination of them).
- *RQ3 - What are the validation strategies of existing approaches for automatic control for CPS security?*
  Objective: to analyze and classify all the existing approaches for automatic control for CPS security with respect to the strategies used for assessing their validity (e.g., controlled experiment, industrial application, prototype-based experiment, test bed, simple examples, formal proofs).

Answer to RQ1 gives a detailed overview about publication trends, venues, and research groups active on the topic. The classification resulting from our investigation on RQ2 and RQ3 provides a solid foundation for a thorough comparison of existing and future solutions for CPS security via automatic control. These contributions are especially useful for researchers willing to further contribute this research area with new approaches to CPS security or willing to better understand or refine existing ones.

3.3. Search strategy

In order to achieve maximal coverage, our search strategy consists of three complementary methods: an automatic search, manual search, and snowballing. Fig. 1 shows the details about our search strategy, and a detailed description of our application of the aforementioned methods is described in the following.

3.3.1. Automatic search

It refers to the execution of a search query on a set of electronic databases and indexing systems, in the literature it is the dominant method for identifying potentially relevant papers (Chen et al., 2010). The applied search string is the following:

```
((((''cyber physical'' OR ''cyber-physical'' OR cyberphysical OR ''networked control'') AND system*) OR CPS OR NCS) AND (attack* OR secur* OR protect*))
```

In the spirit of Zhang et al. (2011a), we established a *quasi-gold standard* (QGS) for creating a good search string for the automatic search. This procedure requires a manual search in a small number of venues (see Table 2) and the results of these manual searches have been treated as a QGS by cross-checking the results obtained from the automatic search. So we iteratively defined and refined the search string, and conducted automatic searches on the electronic data sources until the quasi-sensitivity was above the established threshold of 80%. When the *quasi-sensitivity* became greater than 80%, the search performance was considered acceptable and the results from the automated search have been merged with the QGS. The details of the above mentioned process are provided in the replication package of this study.

[3] Replication package of this study: http://www.cs.gssi.infn.it/CPSSecurity.

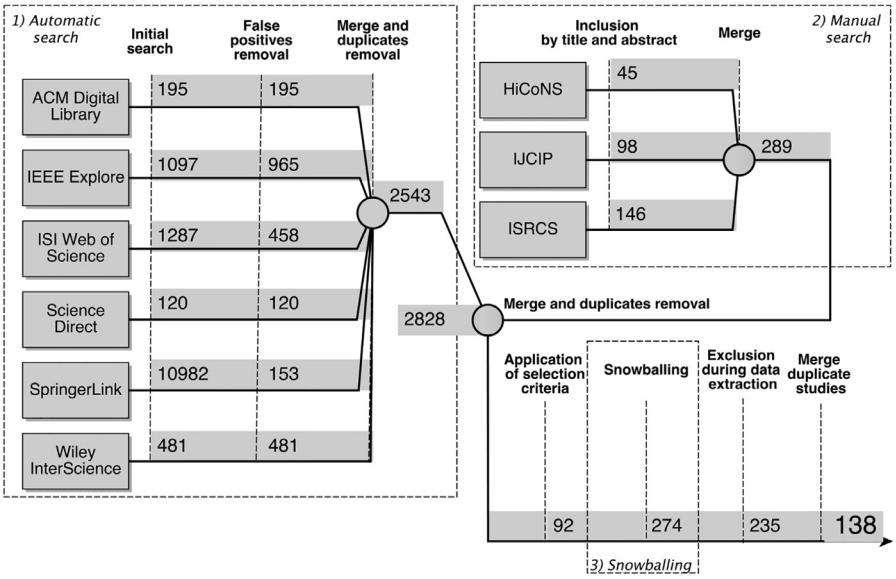


Fig. 1. Overview of the search and selection process.

Table 2
Selected venues for manual search.

Venue	Publisher
International Conference on High Confidence Networked Systems (HiCoNS)	ACM
International Journal of Critical Infrastructure Protection (IJCIP)	Elsevier
International Symposium on Resilient Control Systems (ISRCS)	IEEE

In this stage it was fundamental to select papers objectively so, following the suggestions from Wohlin et al. (2012), two researchers assessed a random sample of the studies and the inter-researcher agreement has been measured using the Cohen Kappa statistic (Cohen, 1968). Each disagreement has been discussed and resolved, with the intervention of the team administrator, if necessary, until the Cohen Kappa statistic reached a result above or equal to 0.80.

Our automatic search is performed on the largest and most complete scientific databases and indexing systems available in computer science (see the leftmost part of Fig. 1). The selection of these electronic databases and indexing systems is guided also by their high accessibility and their ability to export search results to well-defined formats.

Among the results of the automatic searches we removed a set of *false positives* in order to work on a polished set of potentially relevant studies (see Fig. 1). Examples of false positives include proceedings of conferences or workshops, tables of contents, maps, lists of program committee members, keynotes, tutorial or invited talks, and messages from (co-)chairs. As shown in Fig. 1, our automatic search resulted in 2543 potentially relevant studies.

3.3.2. Manual search

By following the quasi-gold standard procedure defined in Zhang et al. (2011a), we (i) identified a subset of important venues for the domain of cyber-physical systems security (they are shown in Table 2), and (ii) performed a *manual search* of relevant publications in those venues. The search have been performed by considering *title* and *abstract* of each publication and the considered time interval is between December 2008 and November 2014 (since the earliest of above mentioned venues dates back to December 2008). By referring to Fig. 1, we manually searched and selected 289 potentially relevant studies.

After merging all the studies and removing duplicates we obtained 2828 potentially relevant studies. In order to further restrict the number of studies to be considered during the snowballing activity, we applied the selection process depicted in Section 3.4 to the current set of studies, thus obtaining 92 potentially relevant studies. In order to handle studies selection in a cost effective way we used the adaptive reading depth, as the full-text reading of clearly excluded approaches is unnecessary. So, we considered *title, keywords* and *abstract* of each potentially relevant study and, if selection decision could not be made, other information (like *conclusion* or even *full-text*) have been exploited (Zhang et al., 2011a).

3.3.3. Snowballing

We applied the *snowballing* technique for identifying additional sources published in other journals or venues (Greenhalgh and Peacock, 2005), which may not have been considered during the automatic and manual searches. So, as recommended in Jalali and Wohlin (2012), we applied (backward and forward) snowballing on the primary studies selected by the automatic and manual searches. More specifically, we considered all the studies selected by the automatic and manual searches, and we searched all the papers referring them (i.e., forward snowballing (Wohlin, 2014)); then, we scrutinized also the references of each selected study to identify important studies that might have been missed during the initial search (i.e., backward snowballing (Wohlin, 2014)).

3.4. Selection strategy

As recommended in the guidelines for performing SLRs from Kitchenham and Charters (2007), we considered all the collected studies and filtered them according to a set of well-defined inclusion and exclusion criteria. In the following we provide the inclusion (I) and exclusion (E) criteria of our study:

- I1: Studies focusing on security of cyber-physical systems.

- I2: Studies proposing a method or technique for CPS security enforcing or breaching based on automatic control.
- I3: Studies providing some kind of validation of the proposed method or technique (e.g., via formal analysis, controlled experiment, exploitation in industry, example usage).
- E1: Studies not subject to peer review (Wohlin et al., 2012) (e.g., journal papers are considered, whereas white papers are discarded).
- E2: Studies written in any language other than English.
- E3: Studies focusing on security method or technique not specific to CPS (e.g., studies focusing on either the physical or cyber part only of the system under consideration; under this criterion the studies that do not consider a physical phenomenon of interest, sometimes called the "plant", or rely only on the typical IT security practices such as classical encryption, are excluded. See Halperin et al. (2008), Zhang et al. (2011b), and Muradore and Quaglia (2015) as examples of notable research papers excluded by this criterion).
- E4: Studies published before 2006 (since the CPS discipline has emerged in 2006).
- E5: Secondary or tertiary studies (e.g., SLRs, surveys, etc.).
- E6: Studies in the form of tutorial papers, short papers, poster papers, editorials, because they do not provide enough information.

A study was selected as a primary study if it satisfied *all* inclusion criteria, and it was discarded if it met *any* exclusion criterion. In order to reduce bias, the selection criteria of this study have been decided during the review protocol definition (thus they have been checked by three external reviewers). By following the approach proposed in Ali and Petersen (2014), two researchers classified each potentially relevant study either as *relevant, uncertain*, or *irrelevant*; studies classified as *irrelevant* have been excluded, whereas all the other approaches have been discussed with the help of a third researcher. For each potentially relevant study we firstly analysed it by considering its title, keywords, and abstract; secondly, if the analysis did not result in a clear decision, also its introduction and conclusions have been analysed; finally, we performed a comprehensive third manual step in which we read the full text of all considered studies (title, abstract, keywords, all sections and appendices, if any) in order to take a final decision.

When reading a primary study in details for extracting its information, researchers could agree that the currently analyzed study was semantically out of the scope of our research, and so it has been excluded (see the *Exclusion during Data Extraction* stage in Fig. 1), resulting in 235 potentially primary studies.

As suggested in Wohlin et al. (2012), if a primary study was published in more then one paper (e.g., if a conference paper has been extended to a journal version) then we considered only one reference paper as primary study; in those cases we considered all the related papers during the data extraction activity in order to obtain all the necessary data (Kitchenham and Charters, 2007). The final set of primary studies is composed of 138 entries after a duplicates merging step.

3.5. Data extraction

Data extraction refers to the recording of all the relevant information from the primary studies required to answer the research questions (Wohlin et al., 2012). Before analysing each primary study, we defined a *comparison framework* for classifying research studies on cyber-physical systems security from an automatic control perspective.

To help the definition of a sound and complete comparison framework, we selected and adapted suitable dimensions and properties found in existing surveys and taxonomies related to CPS security, such as those proposed in Yuan et al. (2014); Avižienis et al. (2004); Yampolskiy et al. (2013). In addition, we defined several parameters for classifying methods and techniques for CPS security; we grouped those parameters into three main dimensions: method or technique's positioning, characterization, and validation. The **Positioning** dimension characterizes the objectives and intent of existing research on CPS security (the *WHAT* aspect of each method or technique). The **Characterization** dimension concerns the classification of studies based on *HOW* CPS security is addressed in research on automatic control. Finally, the **Validation** dimension concerns the strategies researchers apply for providing evidence about the validity of proposed methods or techniques.

All the dimensions and parameters of our classification framework have been encoded in a dedicated *data extraction form*, which can be seen as the implementation of a *comparison framework*. The data extraction form is composed of a list of attributes representing the set of data items extracted from the primary studies. Our data extraction form has been designed to collect such information from each primary study; it includes both standard information (such as name of reviewer, date of data extraction, title, authors and publication details of the study) (Kitchenham and Charters, 2007) and the set of parameters to compare the primary studies according to the three dimensions described above (e.g., the used state estimation model, attack model, experimental testbed, etc.). For the sake of brevity we do not provide the description of all the parameters of our data extraction form, we will briefly elaborate on each of them while discussing the results of this study in Sections 4, 5 and 6; The interested reader can refer to our replication package for a thorough and extensive discussion of all parameters of our classification framework. As suggested in Wohlin et al. (2012), the data extraction form (and thus also the classification framework) has been independently piloted on a sample of primary studies by two researchers, and iteratively refined accordingly. Then, the data extraction activity has been conducted by two researchers.

3.6. Data synthesis

The main goal of our data synthesis activity is to understand, analyze, and classify current research on automatic control for CPS security (Kitchenham and Charters, 2007, § 6.5). Depending on the parameters of the classification framework (see Section 3.5), in this research we applied both quantitative and qualitative synthesis methods.

For each parameter of the classification framework we divided our *quantitative* analysis on two main steps: (i) we counted the number of primary studies falling in relevant categories in the context of the specific parameter and (ii) we aggregated and visualized the extracted information to better clarify similarities and differences between the primary studies.

For what concerns the analysis of *qualitative* data, we used the *keywording method* for identifying also the possible values of each parameter of the classification framework, and then we analysed and summarized the trends and collected information in a quantitative manner. Keywording aims at reducing the time needed in clustering qualitative data into meaningful cateogires and ensures that it takes the considered studies into account (Petersen et al., 2008b). Keywording is done in two steps:

1. *Collect keywords*: we collect keywords by reading the fragment of primary study related to each qualitative parameter. When all fragments have been analysed, all keywords are combined together. The output of this stage is the set of keywords as they have been used in each primary study.
2. *Cluster keywords and form categories*: when keywords have been collected, then a clustering operation is performed on them

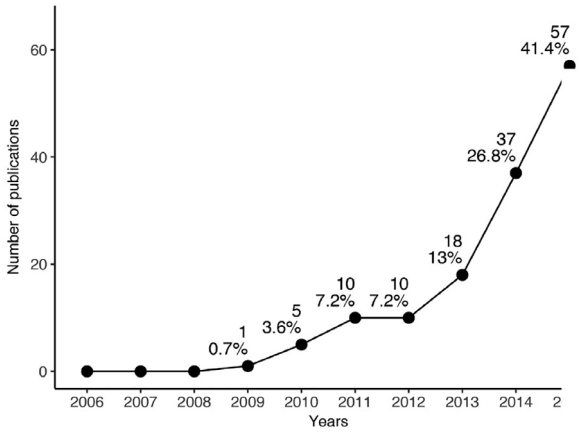


Fig. 2. Distribution by year.

in order to have a set of representative clusters of keywords. We identify the clusters by applying the open card sorting technique (Spencer, 2009) to categorize keywords into relevant groups. More specifically, we consider all the identified keywords and iteratively grouped them together until a saturation of all the concepts is achieved and all primary studies are analyzed. The output of this stage is the set of possible values that each qualitative parameter can have according to the identified clusters of keywords.

Finally, we carried out a narrative synthesis of the results obtained both quantitatively and qualitatively. Narrative synthesis refers to a commonly used method to synthesize research in the context of systematic reviews where a textual narrative summary is adopted to explain the characteristics of primary studies (Popay et al., 2006), usually in conjunction with some form of statistical analysis (PETTICREW et al., 2009; Cruzes and Dybå, 2011). In the context of our study, for each parameter of our classification framework we firstly summarized it from a quantitative perspective (i.e., statistical summary) and then we complemented such quantitative analysis by applying the general framework for narrative synthesis proposed in Popay et al. (2006), namely: (i) we developed a theory about the specific values of the parameter by tabulating the results and iteratively performing content analysis sessions, (ii) we realized a preliminary synthesis of findings based on the quantitative analysis, (iii) we explored potential relationships in the data (i.e., horizontal analysis), (iv) we assessed the robustness of the synthesis by critically reflecting on the synthesis process and checking the obtained synthesis with authors of primary studies (Popay et al., 2006).

In the following sections we present the results of our analysis of the extracted data. In total 138 publications have been selected and analyzed as the subjects of our study. For the sake of clarity we organized the results of the analysis according to our research questions (see Section 3.2).

4. Results - publication trends (RQ1)

In order to assess the publication trends on CPS security, we identified a set of variables focusing on the publication and bibliographic data of each primary study. In the following we describe the main facts emerging from our analysis.

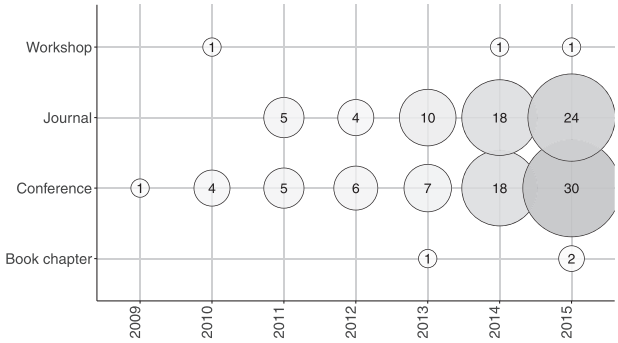


Fig. 3. Types of publications over the years.

4.1. Publication timeline

Fig. 2 presents the distribution of the selected publications[4] on security for cyber-physical systems over the time period from 2006 to 2015. The first interesting result is the growth of the number of those publications in the last years. From the collected data, we can offer the following observations:

- There are no selected studies until 2009, the year in which the famous false data injection attack [S001] has been introduced;
- Starting from 2012, there is a sharp increase in the number of selected studies; we can trace this observation to the fact that (i) in the last years methods and techniques for CPS security are gaining increasing interest and attention from a scientific point of view and (ii) methods and techniques for CPS security are getting urgently needed to produce industry-ready systems with the required levels of security and reliability;
- Finally, we can notice that 112 (81.2%) out of the 138 studies were published during the last three years; this can be seen as an indication that CPS security is a relatively new area, which is gaining more and more traction from a scientific point of view; this observation is further strengthened by the fact that 41.3% of the studies was published in 2015 alone.

Fig. 3 shows the distribution of targeted types of venues over the years. The most common publication types are journal and conference, with 61 (44.2%) and 69 (50.0%) of primary studies, respectively. Such a high number of journal and conference papers may indicate that CPS security is becoming more and more a mature research theme, despite its relative young age (the first publication on CPS security from an automatic control perspective was in 2009).

5. Results - characteristics and focus of research (RQ2)

As already introduced in Section 3.5, we identified a set of variables describing positioning and characterization of methods and techniques for CPS security breaching and/or enforcing. With the purpose of evaluating what aspects of system are attacked or protected by an approach, in the following we indicate which application fields, points of view, security attributes, system components, plant models, SE and anomaly detection algorithms, controllers, communication aspects and network-induced imperfections are considered by each primary study. Furthermore, we give an account of attacks and their characteristics, attack and defense schemes, plant models used by an attacker and defense strategies, in order to understand how these methods and techniques are characterized.

[4] See Section 3.4 for details on selection strategy, which, of course, determined the results presented here.

Table 3
Application field.

Application field	Studies
Building automation	D'Innocenzo et al. (2015)
Irrigation and water supply	Pasqualetti et al. (2013); Amin et al. (2010); Smith (2015); Teixeira et al. (2015b, 2012)
Linear dynamical systems	Li et al. (2015b); Pasqualetti et al. (2013); Yang et al. (2016); Manandhar et al. (2014); Amin et al. (2009); Mo et al. (2015); Mo and Sinopoli (2012); Gupta et al. (2010); Sundaram et al. (2010); Cáardenas et al. (2011); Befekadu et al. (2015); Zhu and Martínez (2014); Smith (2015); Fawzi et al. (2014); Zhu and Başar (2015); Teixeira et al. (2015b); Kwon et al. (2014); Teixeira et al. (2012) Foroush and Martínez (2013); Zhu et al. (2018); Shoukry et al. (2013); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Rhouma et al. (2015); Barreto et al. (2013); Kwon and Hwang (2013b); Miao and Zhu (2014); Chen et al. (2015a); Mo and Sinopoli (2015); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Djouadi et al. (2015); Bai et al. (2015); Weimer et al. (2014); De Persis and Tesi (2015); Zhang et al. (2014); Liu et al. (2014c); Bezzo et al. (2014); Li et al. (2015c); Park et al. (2014); Miao et al. (2014); Mishra et al. (2014); Shoukry and Tabuada (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014); Bezzo et al. (2015); Sajjad et al. (2015); Mishra et al. (2015b); Shoukry et al. (2015b); Qi et al. (2015); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Yuan and Mo (2015); Cetinkaya et al. (2015); Xu and Zhu (2015); Chen et al. (2015b); Tang et al. (2015); Do et al. (2015); Kontouras et al. (2015); Lee et al. (2015)
Nonlinear dynamical systems	Yang et al. (2016); Smith (2015); Zhu and Başar (2015); Mo and Sinopoli (2015); Tiwari et al. (2014); Jones et al. (2014); Bezzo et al. (2015); Sajjad et al. (2015); Shoukry et al. (2015b,a)
Power grid: generation	Vrakopoulou et al. (2015); Pasqualetti et al. (2013); Hammad et al. (2015b); Mishra et al. (2014); Liu et al. (2014b); Wei and Kundur (2015); Mishra et al. (2015a); Amini et al. (2015); Nudell et al. (Sept. 2015); Fawzi et al. (2014); Djouadi et al. (2015)
Power grid: transmission	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Teixeira et al. (2010); Huang et al. (2010); Yuan et al. (2012); Liu et al. (2014c); Bezzo et al. (2014); Li et al. (2015c); Park et al. (2014); Hammad et al. (2015b); Liu et al. (2014b); Weerakkody and Sinopoli (2015); Jones et al. (2014); Bezzo et al. (2015); Bi and Zhang (2014); Davis et al. (2012); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012) Ozay et al. (2013); Zonouz et al. (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Mishra et al. (2015a); Wang et al. (2014); Valenzuela et al. (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016); Qin et al. (2013); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b); Liang et al. (2014); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Manandhar et al. (2014); Tan et al. (2014); Amini et al. (2015); Kim et al. (2015); Yu and Chin (2015); Soltan et al. (2015); Liu et al. (2015a); Rawat and Bajracharya (2015); Chakhchoukh and Ishii (2015); Gu et al. (2015); Nudell et al. (Sept. 2015); Li et al. (2015a); Fawzi et al. (2014); Zhang and Sankar (2015)
Power grid: distribution	Pasqualetti et al. (2013); Mohsenian-Rad and Leon-Garcia (2011); Mishra et al. (2015a); Lo and Ansari (2013); Amini et al. (2015); Anwar et al. (2015); Teixeira et al. (2015a)
Power grid: electricity market	Kosut et al. (2011); Kim and Tong (2013); Wang et al. (2014); Tan et al. (2014); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Ma et al. (2015); Tan et al. (2015); Sanjab and Saad (2015)
(Unmanned) aerial systems	Kwon et al. (2014); Kwon and Hwang (2013a,b); Park et al. (2014); Bezzo et al. (2015); Shoukry et al. (2015b); Xu and Zhu (2015)
(Unmanned) ground vehicles	Xue et al. (2014); Tiwari et al. (2014); Pajic et al. (2015); Bezzo et al. (2014); Shoukry and Tabuada (2014); Sajjad et al. (2015)

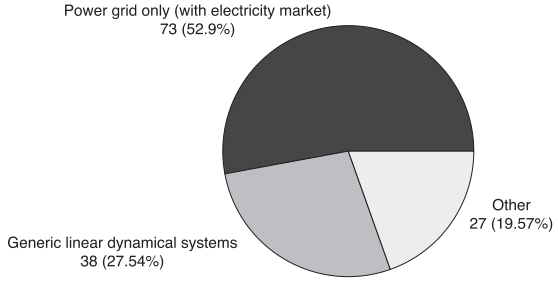


Fig. 4. Distribution by application area.

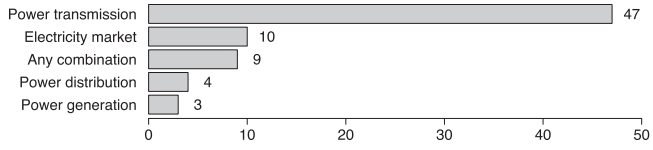


Fig. 5. Distribution in power grids.

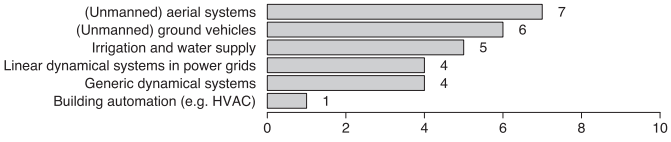


Fig. 6. Distribution of other applications.

5.1. CPS application field

The mapping of individual studies to application fields is reported in Table 3, while the distribution of studies by application area is outlined by Figs. 4,5,6.

As we can see from Fig. 4, 73 (52.9%) out of 138 primary studies are focused exclusively on power grids. Among those, as shown in Fig. 5, 47 papers (i.e. 39.8% of all the selected studies) deal exclusively with power transmission, 10 studies address the security aspects of the electricity market, 4 works are focused on power distribution, 3 papers on power generation, and the remaining 9 on any combination of the previous ones.

The second largest group of publications in Fig. 4 counts 38 works, that is 27.5% of the whole set of primary studies of our research. All these research papers study the security of generic linear dynamical systems, so the proposed approaches can be used in any suitable application. However, these works do not provide examples of a particular application.

The last group of the remaining 27 studies is detailed in Fig. 6. These works are almost uniformly distributed among the following applications: (unmanned) aerial systems (e.g. unmanned aerial vehicles, air traffic management systems) and (unmanned) ground vehicles (UGV) accounting for 7 and 6 of primary studies, respec-

tively; hydro-systems relying on automatic control considered in 5 papers; generic (linear and non linear) dynamical systems and linear dynamical systems with applications to power grids, both found in 4 studies. It is worth noting that UGV-based systems deal with the navigation and control of teleoperated and autonomous ground vehicles, together with their supervisory control and vehicle platooning. Finally, the security of building automation applications is investigated in one primary study. From the collected data, we can offer the following observations:

- The bulk of the selected works on security for cyber-physical systems is focused on power grids; this is not surprising, and may be due to the fact that smart grids are recognized as a driver for sustained economic prosperity, quality of life, and global competitiveness of a nation, attracting big research efforts to this area as a whole; also, the models used in this domain are well-known and the famous false data injection attack [S001] has been introduced in the context of power networks, giving traction to this kind of research applications. Moreover, the impressive market growth in renewable energy devices posed novel challenging problems in the design and management of power grids: as a consequence, the interest of energy providers on novel methods and technologies for optimizing network management with guaranteed performance, safety, and security provided a tremendous boost to academic research on these topics;
- Only a small part of the selected papers presents the applications to the secure control of (unmanned) ground vehicles and aerial systems, and of heating, ventilation, and air-conditioning (HVAC), as well as lighting and shading, in large functional buildings; this application fields are relatively new for the approaches to the cyber-physical security, with the first studies appearing only in 2012; this result can be seen as indication of a potentially interesting direction for future research on CPS security;
- Somehow surprisingly, from the automatic control perspective we have not found any work focused on the cyber-physical security of medical CPS (Lee and Sokolsky, 2010) (since all the works on security we found in this domain still rely only on the typical IT security practices and do not consider the dynamics of physical phenomena of interest, and thus were excluded by exclusion criteria E3, described in Section 3.4). We suppose that the topics of physiological close-loop control and patient modeling are seen as not mature enough to consider the security aspects specific to this important application field from the control-theoretic point of view. In any case, we expect that these topics will be considered and addressed in the near future.

5.2. Point of view

As reported in Fig. 7[5], we distinguish primary studies based on whether they treat approaches for security breaching (i.e. *attack*) or enforcing via some kind of countermeasures (i.e. *defense*), or both. From our analysis it emerged that 68 studies over 138 focus exclusively on the various countermeasures that a CPS may put in place in response to an attack, whereas 35 studies focus exclusively on vulnerability analysis by proposing or improving an attack scheme using an adversary's point of view. They do not study the topic of the risk treatment, which is peculiar to the designer's or operator's perspective. The remaining 35 works treat both attack and defense strategies.

[5] We use area-proportional set diagrams (Micallef and Rodgers, 2014) for visualizing the distribution over parameters with multiple values in which the discussion of their intersections is relevant for this study.

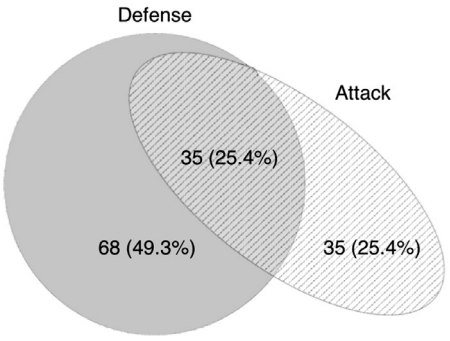


Fig. 7. Distribution by point of view.

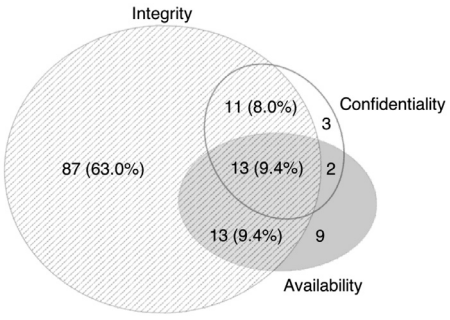


Fig. 8. Distribution by security attributes.

From this result we can observe that the defense strategies are presented in most (103, i.e. 74.6%) of the selected studies, occupying the central spot of the research efforts on CPS security. A more detailed discussion of the various defense strategies proposed in research is provided in Section 5.16, while the mapping of primary studies by the adopted point of view is detailed in Table 4.

5.3. Considered security attributes

Security can be seen as a composition of three main attributes, namely confidentiality, integrity and availability (Avižienis et al., 2004). Therefore, we have identified the security attributes considered by each primary study in order to understand how those attributes have been investigated by researchers on CPS security. Fig. 8 shows the distribution of the primary studies across confidentiality, integrity, and availability, whilst Table 5 provides the map of the main security attributes to the primary studies.

The first thing that strikes the eye is that 124, i.e. 89,9%, of the works are concerned with CPS *integrity*, threatened by various types of deception attacks. Some of these works consider also the availability and/or confidentiality, together with integrity. On the contrary, only two studies, Ma et al. (2015) and Liu et al. (2014c), focus on the combination of solely *availability and confidentiality*; those papers apply game theory to the design of countermeasures to intelligent jamming attacks, which have been published between the fall 2014 and 2015. For further discussion of security attributes, see Section 5.12.

5.4. System components

Each approach to security breaching or enforcing considers a particular set of system components to be compromised or protected. In our analysis we identified five main categories for describing the main system components to be compromised or protected, that are: sensors, actuators, network, controllers, plant. As an example, false data injection mainly targets a set of *sensors*,

Table 4
Point of view.

Point of view	Primary studies
Attack	Liu et al. (2011); Vrakopoulou et al. (2015); Teixeira et al. (2010); Yuan et al. (2012); Esmalifalak et al. (2011); Hammad et al. (2015b); Hug and Giampapa (2012); Mishra et al. (2015a); Kim et al. (2014a); Deka et al. (2015a,b); Liu et al. (2015b); Liang et al. (2014); Yamaguchi et al. (2014), Amini et al. (2015); Kim et al. (2015); Yu and Chin (2015); Chakhchoukh and Ishii (2015); Xie et al. (2011); Esmalifalak et al. (2012); Bi and Zhang (2013); Kim et al. (2014b); Mo and Sinopoli (2012); Smith (2015); Teixeira et al. (2015b); Kwon et al. (2014); Chen et al. (2015a); Djouadi et al. (2015), Zhang et al. (2014); Qi et al. (2015); Zhang and Sankar (2015); Kontouras et al. (2015); Teixeira et al. (2015a); Tan et al. (2015)
Defense	Bobba et al. (2010); Hendrickx et al. (2014); Huang et al. (2010); Pasqualetti et al. (2011); Hammad et al. (2015a); Tajer et al. (2011); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Wei and Kundur (2015); Zonouz et al. (2012); Valenzuela et al. (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016), Li (2014); Sanandaji et al. (2014); Rahman et al. (2014); Manandhar et al. (2014); Soltan et al. (2015); Liu et al. (2015a); Rawat and Bajracharya (2015); Anwar et al. (2015); Gu et al. (2015); Nudell et al. (Sept. 2015); Li et al. (2015a); Amin et al. (2009); Mo et al. (2015); Sundaram et al. (2010); Befekadu et al. (2015); Zhu and Martínez (2014), Fawzi et al. (2014); Zhu and Başar (2015); Teixeira et al. (2012); Xue et al. (2014); Foroush and Martínez (2013); Zhu et al. (2018); Shoukry et al. (2013); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Rhouma et al. (2015); Kwon and Hwang (2013b); Miao and Zhu (2014); Mo and Sinopoli (2015); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Weimer et al. (2014); De Persis and Tesi (2015); Bezzo et al. (2014); Li et al. (2015c); Park et al. (2014); Miao et al. (2014); Mishra et al. (2014); Shoukry and Tabuada (2014); Jones et al. (2014), Bezzo et al. (2015); Mishra et al. (2015b); Shoukry et al. (2015b); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Cetinkaya et al. (2015); Xu and Zhu (2015); Tang et al. (2015); Do et al. (2015); Shoukry et al. (2015a); Lee et al. (2015)
Both	Kosut et al. (2011); Li et al. (2015b); Kim and Poor (2011); Pasqualetti et al. (2013); Liu et al. (2014b); Giani et al. (2013); Bezzo et al. (2015); Sajjad et al. (2015); Mishra et al. (2015b); Davis et al. (2012); Ozay et al. (2013); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Wang et al. (2014); Lo and Ansari (2013); Qin et al. (2013), Deka et al. (2014); Wang and Ren (2014); Hao et al. (2015); Tan et al. (2014); Jia et al. (2014); Choi and Xie (2013); Esmalifalak et al. (2013); Ma et al. (2015); Amin et al. (2010); Gupta et al. (2010); Cárdenas et al. (2011); Barreto et al. (2013); Bai et al. (2015), Liu et al. (2014c); Weerakkody and Sinopoli (2015); Sajjad et al. (2015); Yuan and Mo (2015); Chen et al. (2015b); Sanjab and Saad (2015)

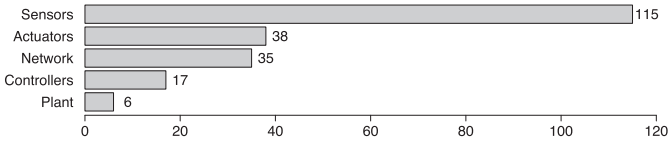


Fig. 9. Distribution of primary studies by system components.

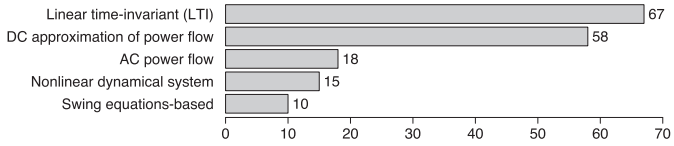


Fig. 10. Distribution of studies by plant model.

while load altering can attack a set of *actuators*. As for all deception and some disruption attacks, we should *"note that from a practical point of view, an attack on a sensor could either be interpreted as an attack on the node itself (making it transmit an incorrect signal), or it could also be interpreted as an attack on the communication link between the sensor and the receiver device; similarly an attack on an actuator could either be interpreted as an attack on the actuator itself, or on the communication link from the controller to the actuator"* (Fawzi et al., 2014). Thus, we say that an approach considers a *network* either when it does it implicitly by considering a denial-of-service (DoS) attack on communication links, or explicitly, by exploiting transmission scheduling, routing or some network-induced imperfections. By the same line of reasoning, we say that the work takes into account a *controller* when it proposes a novel one, whereas the *plant* category comes into play with attacks at the physical layer and with eavesdropping.

Fig. 9 presents how system components have been considered among the primary studies, while the Table 6 reports the related mapping, showing that sensors were taken into account 115 (83.3%) times, 69 (50.0%) times alone and 32 (23,2%) times together with actuators. The actuators themselves were considered 38 (27.5%) times, while network was taken into account in 35 (25.4%) studies. This data suggests that the approaches considering attacks on sensors and their protection completely dominate the scene. All the other system components have received much less attention, with a slight predominance of actuators and network.

5.5. Plant model

We have seen in Section 5.1 that the application domain of research on CPS security is mainly divided between power grids and all the others. This result is reflected also in the choice of the mathematical models used to describe the physical domain.

In particular, power transmission is traditionally studied via a power flow model, which is a set of equations that depict the energy flow on each transmission line of a power grid. An AC power flow model considers both real and reactive power and is formulated by nonlinear equations, where the state variables are voltage magnitudes and phase angles of the buses (Abur and Exposito, 2004; Wood and Wollenberg, 1996). However, SE using an AC power flow model can be computationally expensive and does not always converge to a solution. Thus, power system engineers sometimes use a linearized power flow model, DC power flow model, to approximate the AC power flow model [S001]. In DC power flow model the reactive power is completely neglected and state variables only consist of voltage phase angles of the buses. As of power generation, the model based on equations describing the electromechanical swing dynamics of the synchronous generators (Kundur, 1994) is usually applied. In other application domains more general linear time invariant (LTI) or nonlinear dynamical models are used.

Fig. 10 shows how the above mentioned models have been used within the set of primary studies, whilst Table 7 provides the re-

Table 5
Security attributes.

Security attribute	Primary studies
Availability	Li et al. (2015b); Hammad et al. (2015b,a); Liu et al. (2014b); Mohsenian-Rad and Leon-Garcia (2011); Vuković and Dán (2014); Mishra et al. (2015a); Soltan et al. (2015); Rawat and Bajracharya (2015); Nudell et al. (Sept. 2015); Kim et al. (2014b); Ma et al. (2015); Amin et al. (2009); Gupta et al. (2010), Cárdenas et al. (2011); Befekadu et al. (2015); Zhu and Martínez (2014); Smith (2015); Zhu and Başar (2015); Teixeira et al. (2015b); Foroush and Martínez (2013); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Barreto et al. (2013); Chen et al. (2015a); Eyisi and Koutsoukos (2014); Djouadi et al. (2015), De Persis and Tesi (2015); Zhang et al. (2014); Liu et al. (2014c); Li et al. (2015c); Park et al. (2014); Sajjad et al. (2015); Qi et al. (2015); Cetinkaya et al. (2015); Xu and Zhu (2015); Shoukry et al. (2015a)
Integrity	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Vrakopoulou et al. (2015); Teixeira et al. (2010); Huang et al. (2010); Li et al. (2015b); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2013, 2011); Esmalifalak et al. (2011); Liu et al. (2014b); Tajer et al. (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Mohsenian-Rad and Leon-Garcia (2011); Davis et al. (2012); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012); Wei and Kundur (2015); Ozay et al. (2013); Zonouz et al. (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Mishra et al. (2015a); Wang et al. (2014); Valenzuela et al. (2013); Lo and Ansari (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016); Qin et al. (2013); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b); Liang et al. (2014); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Manandhar et al. (2014); Tan et al. (2014); Amini et al. (2015); Kim et al. (2015); Yu and Chin (2015); Liu et al. (2015a); Rawat and Bajracharya (2015); Anwar et al. (2015); Chakhchoukh and Ishii (2015); Gu et al. (2015); Nudell et al. (Sept. 2015); Li et al. (2015a); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Mo et al. (2015); Mo and Sinopoli (2012); Amin et al. (2010); Gupta et al. (2010); Sundaram et al. (2010); Cárdenas et al. (2011); Zhu and Martínez (2014); Smith (2015); Fawzi et al. (2014); Zhu and Başar (2015); Teixeira et al. (2015b); Kwon et al. (2014); Teixeira et al. (2012), Zhu et al. (2018); Shoukry et al. (2013); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Rhouma et al. (2015); Barreto et al. (2013); Kwon and Hwang (2013b); Miao and Zhu (2014); Mo and Sinopoli (2015); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Djouadi et al. (2015); Bai et al. (2015); Weimer et al. (2014); Zhang et al. (2014); Bezzo et al. (2014); Park et al. (2014, 2014); Miao et al. (2014); Mishra et al. (2014); Shoukry and Tabuada (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014); Bezzo et al. (2015); Sajjad et al. (2015); Mishra et al. (2015b); Shoukry et al. (2015b); Qi et al. (2015); Naghnaeian et al. (2015); Xu and Zhu (2015); Zhang and Sankar (2015); Chen et al. (2015b); Tang et al. (2015); Do et al. (2015); Kontouras et al. (2015); Shoukry et al. (2015a); Teixeira et al. (2015a); Tan et al. (2015); Lee et al. (2015); Sanjab and Saad (2015)
Confidentiality	Vrakopoulou et al. (2015); Li et al. (2015b); Pasqualetti et al. (2013); Esmalifalak et al. (2011); Liu et al. (2014b); Amini et al. (2015); Gu et al. (2015); Ma et al. (2015); Mo et al. (2015); Zhu and Martínez (2014); Smith (2015); Zhu and Başar (2015); Teixeira et al. (2015b), Xue et al. (2014); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Zhang et al. (2014); Liu et al. (2014c); Mishra et al. (2014); Shoukry and Tabuada (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014); Bezzo et al. (2015); Sajjad et al. (2015); Qi et al. (2015); Kogiso and Fujita (2015); Yuan and Mo (2015); Xu and Zhu (2015); Shoukry et al. (2015a)

lated mapping. The *DC power flow* model has been used in 58 works (42.0% of whole set), while the more complicated and realistic *AC power flow model* (which is capable to capture more subtleties) has been studied 18 (13.0%) times. In 8 (5.8%) studies both the AC power flow model and its linear DC approximation have been used. Other *LTI models* were applied in 67 (48.6%) primary studies. *Nonlinear dynamic* and *swing equation-based models* were applied 15 (10.9%) and 10 (7.2%) times, respectively.

5.6. Process noise

To capture any deviation in the plant model from the real dynamics of the controlled physical system, the process noise is used. From the primary studies it emerged that it can be categorized into three main classes: *Gaussian*, *bounded (non-stochastic)*, and *noiseless*.

The mapping of individual studies to process noise is shown in Table 8, while the distribution of primary studies by process noise is reported in Fig. 11, where the studies considering the measurement model only (70, accounting for 50.7% of the whole set of selected papers) were not included, since for them the facet of process noise is not applicable. We can see that the noiseless and Gaussian process noise models are the most used ones (accounted 36 and 30 times, respectively). As shown in Fig. 12, the bounded non-stochastic model (used 9 times) is starting to receive a growing attention in the very last years.

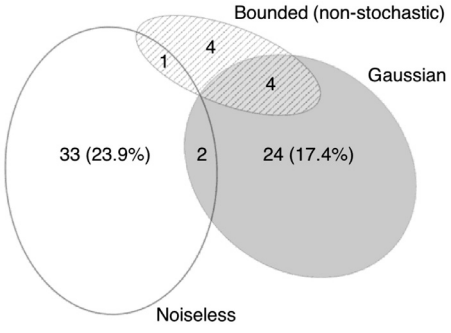


Fig. 11. Distribution by process noise.

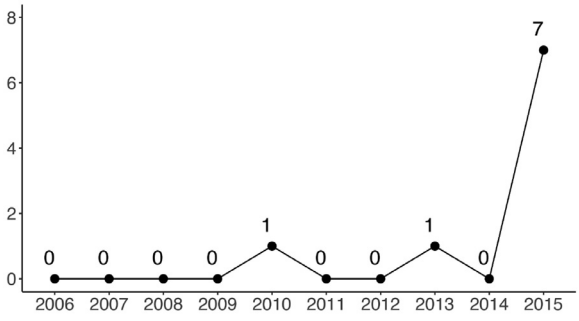


Fig. 12. Number of studies with bounded process noise year by year.

Table 6
System components.

System component	Primary studies
Plant	Soltan et al. (2015); Teixeira et al. (2015b); Xue et al. (2014); Zhu et al. (2018); Weerakkody and Sinopoli (2015); Sajjad et al. (2015)
Sensors	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Teixeira et al. (2010); Huang et al. (2010); Li et al. (2015b); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2013, 2011); Esmalifalak et al. (2011); Tajer et al. (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Davis et al. (2012); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012); Wei and Kundur (2015); Ozay et al. (2013); Zonouz et al. (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Mishra et al. (2015a); Wang et al. (2014); Valenzuela et al. (2013); Lo and Ansari (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016); Qin et al. (2013); Kim et al. (2014a); Deka et al. (2014, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b); Liang et al. (2014); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Manandhar et al. (2014); Tan et al. (2014) Kim et al. (2015); Yu and Chin (2015); Liu et al. (2015a); Rawat and Bajracharya (2015); Anwar et al. (2015); Chakhchoukh and Ishii (2015); Gu et al. (2015); Nudell et al. (Sept. 2015); Li et al. (2015a); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Mo et al. (2015); Mo and Sinopoli (2012); Amin et al. (2010); Sundaram et al. (2010); Cáardenas et al. (2011); Zhu and Martínez (2014); Smith (2015); Fawzi et al. (2014); Zhu and Başar (2015); Teixeira et al. (2015b); Kwon et al. (2014); Teixeira et al. (2012); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Rhouma et al. (2015); Barreto et al. (2013); Kwon and Hwang (2013b); Miao and Zhu (2014); Mo and Sinopoli (2015); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Djouadi et al. (2015); Bai et al. (2015); Weimer et al. (2014); Zhang et al. (2014); Bezzo et al. (2014); Li et al. (2015c); Park et al. (2014); Miao et al. (2014); Mishra et al. (2014); Shoukry and Tabuada (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014); Bezzo et al. (2015) Mishra et al. (2015b); Shoukry et al. (2015b); Qi et al. (2015); Naghnaeian et al. (2015); Zhang and Sankar (2015); Chen et al. (2015b); Tang et al. (2015); Do et al. (2015); Shoukry et al. (2015a); Tan et al. (2015); Lee et al. (2015); Sanjab and Saad (2015)
Controllers	Hammad et al. (2015a); Wei and Kundur (2015); Ozay et al. (2013); Amin et al. (2009); Gupta et al. (2010); Befekadu et al. (2015); Zhu and Martínez (2014); Zhu and Başar (2015); Zhu et al. (2018); Kwon and Hwang (2013b); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Yuan and Mo (2015); Cetinkaya et al. (2015); Xu and Zhu (2015) Kontouras et al. (2015); Teixeira et al. (2015a)
Actuators	Vrakopoulou et al. (2015); Pasqualetti et al. (2013); Hammad et al. (2015b); Liu et al. (2014b); Mohsenian-Rad and Leon-Garcia (2011); Kim and Tong (2013); Deka et al. (2015a); Rahman et al. (2014); Amini et al. (2015); Amin et al. (2009); Mo et al. (2015); Mo and Sinopoli (2012); Amin et al. (2010) Zhu and Martínez (2014); Smith (2015); Fawzi et al. (2014); Zhu and Başar (2015); Teixeira et al. (2015b); Kwon et al. (2014); Teixeira et al. (2012); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Rhouma et al. (2015); Barreto et al. (2013); Miao and Zhu (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Djouadi et al. (2015); Bai et al. (2015); Li et al. (2015c); Mishra et al. (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014) Naghnaeian et al. (2015); Zhang and Sankar (2015); Tang et al. (2015); Shoukry et al. (2015a)
Network	Li et al. (2015b); Hammad et al. (2015a); Vuković et al. (2012); Vuković and Dán (2014); Deka et al. (2015a); Manandhar et al. (2014); Soltan et al. (2015); Rawat and Bajracharya (2015); Li et al. (2015a); Ma et al. (2015); Amin et al. (2009); Gupta et al. (2010) Sundaram et al. (2010); Befekadu et al. (2015); Zhu and Martínez (2014); Zhu and Başar (2015); Teixeira et al. (2015b); Foroush and Martínez (2013); Shoukry et al. (2013); D'Innocenzo et al. (2015); Rhouma et al. (2015); Barreto et al. (2013); Miao and Zhu (2014); Chen et al. (2015a) Eyisi and Koutsoukos (2014); Pajic et al. (2015); Djouadi et al. (2015); De Persis and Tesi (2015); Zhang et al. (2014); Liu et al. (2014c); Li et al. (2015c); Park et al. (2014); Jones et al. (2014); Cetinkaya et al. (2015); Xu and Zhu (2015)

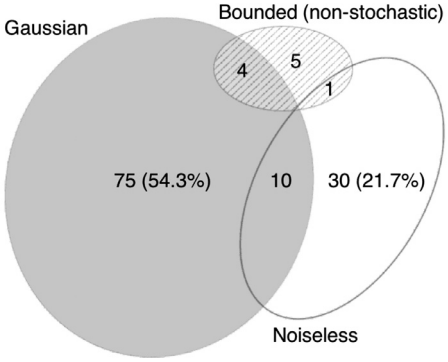


Fig. 13. Distribution by measurement noise.

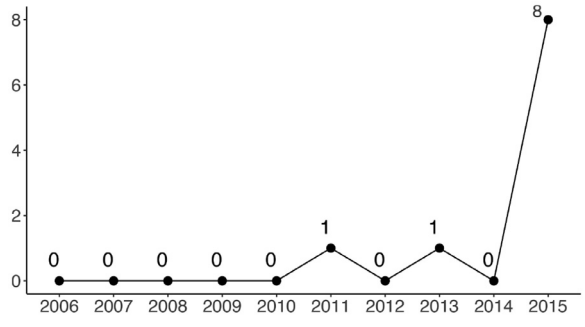


Fig. 14. Number of studies with bounded measurement noise year by year.

5.7. Measurement noise

Depending on the assumptions on the noise, sensor measurement models can be broadly categorized into three classes: *Gaussian, bounded (non-stochastic)* and *noiseless* Mishra et al. (2015b). As shown in Fig. 13, the majority of primary studies (89, i.e. 64.5%) uses Gaussian measurement noise model; while 41 (29.7% of all) works assume noiseless measurements. Only 10 works have used bounded (non-stochastic) assumptions. Similarly for the bounded process noise, the bounded measurement noise has started to gain attention only recently in the CPS security domain, as we can see from Fig. 14.

The mapping of individual studies to measurement noise is reported in Table 9. If a study does not consider the measurement

Table 7
Plant models.

Plant model	Primary studies
AC power flow	Teixeira et al. (2010); Davis et al. (2012); Sou et al. (2014); Hug and Giampapa (2012); Zonouz et al. (2012); Kim and Tong (2013); Wang et al. (2014); Valenzuela et al. (2013); Qin et al. (2013); Kim et al. (2014a); Liang et al. (2014) Manandhar et al. (2014); Kim et al. (2015); Liu et al. (2015a); Anwar et al. (2015); Chakhchoukh and Ishii (2015); Gu et al. (2015); Zhang and Sankar (2015)
DC power flow	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Teixeira et al. (2010); Huang et al. (2010); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2013, 2011); Esmalifalak et al. (2011); Tajer et al. (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Mohsenian-Rad and Leon-Garcia (2011); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012) Ozay et al. (2013); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Mishra et al. (2015a); Wang et al. (2014); Lo and Ansari (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Deka et al. (2014, 2015a, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014) Tan et al. (2014); Amini et al. (2015); Kim et al. (2015); Yu and Chin (2015); Soltan et al. (2015); Rawat and Bajracharya (2015); Anwar et al. (2015); Chakhchoukh and Ishii (2015); Li et al. (2015a); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Ma et al. (2015); Tan et al. (2015); Sanjab and Saad (2015)
Linear time-invariant (LTI)	Li et al. (2015b); Pasqualetti et al. (2013); Hammad et al. (2015b,a); Liu et al. (2014b); Yang et al. (2016); Manandhar et al. (2014); Amin et al. (2009, 2009); Gupta et al. (2010); Befekadu et al. (2015); Zhu and Martínez (2014); Zhu and Başar (2015); Zhu et al. (2018); Shoukry et al. (2013); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Rhouma et al. (2015); Barreto et al. (2013); Kwon and Hwang (2013b); Miao and Zhu (2014); Chen et al. (2015a); Mo and Sinopoli (2015); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Djouadi et al. (2015); Bai et al. (2015); Weimer et al. (2014); De Persis and Tesi (2015); Zhang et al. (2014); Liu et al. (2014c); Bezzo et al. (2014); Li et al. (2015c); Park et al. (2014); Miao et al. (2014); Mishra et al. (2014); Shoukry and Tabuada (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014); Sajjad et al. (2015); Mishra et al. (2015b); Shoukry et al. (2015b); Qi et al. (2015); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Yuan and Mo (2015); Cetinkaya et al. (2015); Xu and Zhu (2015) Chen et al. (2015b); Tang et al. (2015); Do et al. (2015); Kontouras et al. (2015); Teixeira et al. (2015a); Lee et al. (2015)
Nonlinear dynamical system	Vrakopoulou et al. (2015); Hammad et al. (2015b); Liu et al. (2014b); Yang et al. (2016); Manandhar et al. (2014); Smith (2015); Zhu and Başar (2015); Teixeira et al. (2012); Mo and Sinopoli (2015); Park et al. (2014) Jones et al. (2014); Bezzo et al. (2015); Sajjad et al. (2015); Shoukry et al. (2015b,a)
Swing equations-based	Pasqualetti et al. (2013); Hammad et al. (2015b,a); Liu et al. (2014b); Wei and Kundur (2015); Amini et al. (2015); Nudell et al. (Sept. 2015); Fawzi et al. (2014); Zhu and Başar (2015); Djouadi et al. (2015)

Table 8
Process noise

Process noise	Primary studies
Gaussian	Li et al. (2015b); Yang et al. (2016); Manandhar et al. (2014); Rawat and Bajracharya (2015); Amin et al. (2009, 2009); Mo and Sinopoli (2012); Gupta et al. (2010); Befekadu et al. (2015); Smith (2015); Zhu and Başar (2015); Teixeira et al. (2015b); Kwon et al. (2014) Rhouma et al. (2015); Miao and Zhu (2014); Chen et al. (2015a); Bai et al. (2015); Weimer et al. (2014); Zhang et al. (2014); Bezzo et al. (2014); Li et al. (2015c); Park et al. (2014); Miao et al. (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014); Mishra et al. (2015b) Qi et al. (2015); Yuan and Mo (2015); Tang et al. (2015); Do et al. (2015)
Bounded (non-stochastic)	Gupta et al. (2010); Zhu and Başar (2015); Teixeira et al. (2015b); Shoukry et al. (2013); Pajic et al. (2015); De Persis and Tesi (2015); Li et al. (2015c); Xu and Zhu (2015); Lee et al. (2015)
Noiseless	Vrakopoulou et al. (2015); Pasqualetti et al. (2013); Hammad et al. (2015b,b); Liu et al. (2014b); Amini et al. (2015); Amin et al. (2010); Sundaram et al. (2010); Cáardenas et al. (2011); Zhu and Martínez (2014); Smith (2015); Fawzi et al. (2014) Teixeira et al. (2012); Xue et al. (2014); Foroush and Martínez (2013); Zhu et al. (2018); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Barreto et al. (2013); Kwon and Hwang (2013b); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Djouadi et al. (2015); De Persis and Tesi (2015) Liu et al. (2014c); Mishra et al. (2014); Shoukry and Tabuada (2014); Bezzo et al. (2015); Sajjad et al. (2015); Mishra et al. (2015b); Shoukry et al. (2015b); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Cetinkaya et al. (2015); Teixeira et al. (2015a)

model (e.g., when the work is not related to the secure state estimation against sensor attacks), we say that the measurement noise is not applicable. Among the selected primary studies there were 13 such studies.

5.8. State estimation

For many situations, it may be unrealistic or unfeasible to assume that all the states of the system are measured. In fact, 99 studies were using some kind of state estimation, which corresponds to 71.7% of all the primary studies (see Fig. 15). The most used SE method is *weighted least squares* (WLS), found in 59 (42.8% of all) works (interestingly, all 59 studies were related to power grids). The WLS method for power system SE is optimal under Gaussian measurement noise Chakhchoukh and Ishii (2015) and, in case of DC approximation of power flow, leads to an estimator identical to the one obtained with maximum likelihood or with minimum variance methods [S001]. The (extended) *Kalman filter* was used in 25 studies (18.1% of all primary studies), while the (extended) *Luenberger observer* was used in 13 studies (9.4%), the H_∞

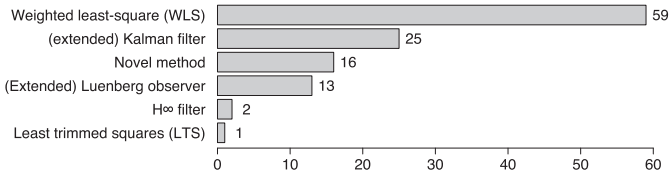


Fig. 15. Distribution of primary studies by state estimation.

Table 9
Measurement noise.

Measurement noise	Primary studies
Gaussian	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Teixeira et al. (2010); Huang et al. (2010); Li et al. (2015b); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2011); Esmalifalak et al. (2011); Tajer et al. (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012) Ozay et al. (2013); Zonouz et al. (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Mishra et al. (2015a); Wang et al. (2014); Lo and Ansari (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016); Qin et al. (2013); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b); Liang et al. (2014); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Manandhar et al. (2014); Tan et al. (2014); Kim et al. (2015); Yu and Chin (2015); Liu et al. (2015a); Rawat and Bajracharya (2015); Anwar et al. (2015); Chakhchoukh and Ishii (2015); Gu et al. (2015); Li et al. (2015a); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Ma et al. (2015) Mo et al. (2015); Mo and Sinopoli (2012); Befekadu et al. (2015); Smith (2015); Teixeira et al. (2015b); Kwon et al. (2014); Xue et al. (2014); Rhouma et al. (2015); Miao and Zhu (2014); Chen et al. (2015a); Mo and Sinopoli (2015) Bai et al. (2015); Weimer et al. (2014); Zhang et al. (2014); Bezzo et al. (2014); Li et al. (2015c); Park et al. (2014); Miao et al. (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014); Mishra et al. (2015b); Qi et al. (2015); Yuan and Mo (2015); Zhang and Sankar (2015) Tang et al. (2015); Do et al. (2015); Shoukry et al. (2015a); Sanjab and Saad (2015)
Bounded (non-stochastic)	Tajer et al. (2011); Wei and Kundur (2015); Teixeira et al. (2015b); Shoukry et al. (2013); Mo and Sinopoli (2015); Pajic et al. (2015); De Persis and Tesi (2015); Li et al. (2015c); Bezzo et al. (2015); Lee et al. (2015)
Noiseless	Pasqualetti et al. (2013); Hammad et al. (2015b); Liu et al. (2014b); Giani et al. (2013); Mohsenian-Rad and Leon-Garcia (2011); Davis et al. (2012); Sou et al. (2014); Talebi et al. (2010); Kim and Tong (2013); Deka et al. (2015a); Liu et al. (2015b); Liang et al. (2014); Amini et al. (2015) Nudell et al. (Sept. 2015); Amin et al. (2009, 2010); Sundaram et al. (2010); Cáardenas et al. (2011); Smith (2015); Fawzi et al. (2014); Zhu and Başar (2015); Teixeira et al. (2012); Foroush and Martínez (2013); Zhu et al. (2018) D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Barreto et al. (2013); Kwon and Hwang (2013b); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Djouadi et al. (2015); De Persis and Tesi (2015); Liu et al. (2014c); Mishra et al. (2014); Shoukry and Tabuada (2014) Sajjad et al. (2015); Mishra et al. (2015b); Shoukry et al. (2015b); Chen et al. (2015b)

filter in 2 studies and the *least trimmed squares* estimator in only one study. Novel solutions for the SE were proposed in 16 (11.6%) studies. The mapping of individual primary studies to SE methods is reported in Table 10.

Novel methods range from application-specific solutions (Wei and Kundur, 2015; Amin et al., 2010) and distributed state estimation techniques for power networks (Pasqualetti et al., 2011; Tajer et al., 2011; Ozay et al., 2013) to generic attack-resilient solutions inspired by Kalman filter (Bezzo et al., 2014; Mishra et al., 2015b).

Within the domain of power grids, Giani et al. (2013) proposed SE based countermeasures to coordinated sparse attacks on power meter readings, that take advantage of graph-theoretic construct of *observable islands*, which are disjoint subsets of buses sharing the same perceived change of state [voltage phase] under the attack. As a countermeasure to leverage point attacks against WLS SE in smart grid, Tan et al. (2014) introduced a modified robust Schweppe-Huber Generalized-M estimator. The WLS estimation method for power networks has been extended by Liu et al. (2015a) by merging cyber impact factor matrix into the state estimation as a reasonable adjustment of the weight values, in order to create the abnormal traffic-indexed SE.

Regarding generic CPS, to estimate the state of the plant despite attacks on sensors and actuators, (Fawzi et al., 2014) proposed an efficient state reconstructor inspired from techniques used in compressed sensing and error correction over the real numbers. Pajic et al. (2014) showed that implementation issues such as jitter, latency and synchronization errors can be mapped into parameters of the SE procedure that describe modeling errors, and provides a bound on the SE error caused by modeling errors. The same research line is extended in [S104] to prove that for linear dynamical systems with bounded process and measurement noise, the worst-case error is linear with the size of the noise, meaning that an attacker cannot exploit noise and modeling errors to introduce unbounded SE errors in the proposed state estimator based on ℓ_0 and ℓ_1 norms.

Mo and Sinopoli (2015) constructed an optimal estimator of a scalar state that minimizes the "worst-case" expected cost against all possible manipulations of measurements by the attacker, while Weimer et al. (2014) introduced a minimum mean-squared error resilient (MMSE-R) estimator for stochastic systems, whose conditional mean squared error from the state remains finitely bounded and is independent of additive measurement attacks.

Finally, for linear dynamical systems under sensor attacks, Shoukry and Tabuada (2014) presented an efficient event-triggered projected Luenberger observer for systems under sparse attacks, and Shoukry et al. (2015), Shoukry et al. (2015b) developed an efficient algorithm that uses a Satisfiability Modulo Theory (SMT) approach to isolate the compromised sensors and estimate the system state despite the presence of the attack.

Together, these results are an indication that the resilient SE under measurement attacks is a very active research topic within the area of CPS security, making us reasonably confident about its future development and potential.

5.9. Anomaly detector

Current state estimation algorithms use bad data detection (BDD) schemes to detect random outliers in the measurement data [S006]. Two of the most used BDD hypothesis tests are the *performance index test* (also known in power system's community as $J(\hat{x})$-*test* or χ^2-*test*) and the *largest normalized residual test* (often referred as r^N_{max}-*test*) (Abur and Exposito, 2004). As shown in Fig. 16, among our primary studies there are 62 approaches considering performance index test, 23 approaches dealing with normalized residual test, and 14 considering both aforementioned hypothesis tests. The mapping of primary studies by the adopted state estimation algorithms is detailed in Table 11, which shows that 9 studies consider an arbitrary anomaly detector implemented by the controller and deployed to detect possible deviations from the nominal behavior, while 43 (31.2%) primary studies do not deal at all with anomaly detection.

Table 10
State estimation.

State estimators	Primary studies
(Extended) Kalman filter	Li et al. (2015b); Pasqualetti et al. (2013); Yang et al. (2016); Manandhar et al. (2014); Rawat and Bajracharya (2015); Amin et al. (2009); Mo et al. (2015); Mo and Sinopoli (2012); Teixeira et al. (2015b); Kwon et al. (2014); Rhouma et al. (2015) Kwon and Hwang (2013b); Miao and Zhu (2014); Chen et al. (2015a); Bai et al. (2015); Zhang et al. (2014); Bezzo et al. (2014); Park et al. (2014); Miao et al. (2014); Weerakkody and Sinopoli (2015); Bezzo et al. (2015); Mishra et al. (2015b) Qi et al. (2015); Yuan and Mo (2015); Do et al. (2015)
(Extended) Luenberger observer	Pasqualetti et al. (2013); Liu et al. (2014b); Zhu and Başar (2015); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Eyisi and Koutsoukos (2014); Djouadi et al. (2015); Mishra et al. (2014); Shoukry and Tabuada (2014); Cetinkaya et al. (2015) Tang et al. (2015); Lee et al. (2015)
H_∞ filter	Shoukry et al. (2013); Kwon and Hwang (2013b)
Least trimmed squares (LTS)	Chakhchoukh and Ishii (2015)
Maximum likelihood	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Huang et al. (2010); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2011); Esmalifalak et al. (2011); Giani et al. (2013); Kosut et al. (2011); Bobba et al. (2010); Bi and Zhang (2014); Talebi et al. (2010) Vuković et al. (2012); Ozay et al. (2013); Rahman and Mohsenian-Rad (2012); Kosut et al. (2011); Bobba et al. (2010); Mishra et al. (2015a); Lo and Ansari (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Deka et al. (2014, 2015a, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b) Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Tan et al. (2014); Yu and Chin (2015); Li et al. (2015a); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Ma et al. (2015); Sanjab and Saad (2015)
Minimum variance	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Huang et al. (2010); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2011); Esmalifalak et al. (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Talebi et al. (2010) Vuković et al. (2012); Ozay et al. (2013); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Mishra et al. (2015a); Lo and Ansari (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Deka et al. (2014, 2015a, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b) Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Tan et al. (2014); Yu and Chin (2015); Li et al. (2015a); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Ma et al. (2015); Weimer et al. (2014); Sanjab and Saad (2015)
Weighted least-square (WLS)	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Teixeira et al. (2010); Huang et al. (2010); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2011); Esmalifalak et al. (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014) Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012); Ozay et al. (2013); Zonouz et al. (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Mishra et al. (2015a); Wang et al. (2014); Lo and Ansari (2013, 2013); Sedghi and Jonckheere (2015); Qin et al. (2013); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b); Liang et al. (2014); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Tan et al. (2014) Kim et al. (2015); Yu and Chin (2015); Liu et al. (2015a); Anwar et al. (2015); Chakhchoukh and Ishii (2015); Gu et al. (2015); Nudell et al. (Sept. 2015); Li et al. (2015a); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Ma et al. (2015); Zhang and Sankar (2015); Sanjab and Saad (2015)
Novel	Pasqualetti et al. (2011); Tajer et al. (2011); Giani et al. (2013); Wei and Kundur (2015); Ozay et al. (2013); Tan et al. (2014); Liu et al. (2015a); Amin et al. (2010); Fawzi et al. (2014); Mo and Sinopoli (2015) Pajic et al. (2015); Weimer et al. (2014); Bezzo et al. (2014); Shoukry and Tabuada (2014); Mishra et al. (2015b); Shoukry et al. (2015b)

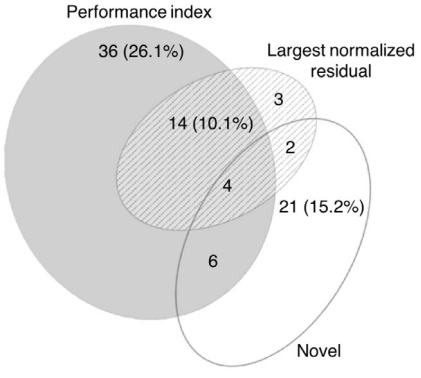


Fig. 16. Distribution of primary studies by anomaly detection.

In an effort to minimize the detection delay, the change detection can be formulated as a quickest detection problem. Page's cumulative sum (CUSUM) algorithm is the best-known technique to tackle this type of problem. There are 6 selected primary studies, that propose or use a CUSUM-based attack detection schemes (Huang et al., 2010; Yang et al., 2014; 2016; Li et al., 2015a; Cárdenas et al., 2011; Do et al., 2015). There are also 28 (20.3%) studies that propose other novel anomaly detection approaches, some of which are considered together with the performance index test and/or normalized residual test. The novel solutions for bad data detection cover the topics of distributed monitoring Pasqualetti et al. (2013, 2011); Tajer et al. (2011); Vuković and Dán (2014) and application-specific anomaly detection for multi-agent distributed flocking formation control (Wei and Kundur, 2015), automated cascade canal irrigation systems Amin et al. (2010), wireless control networks, *"where the network itself acts as the controller, instead of having a specially designated node performing this task"* Sundaram et al. (2010), multi-hop control networks, *"where the communication between sensors, actuators and computational units is supported by a (wireless) multi-hop communication network and data flow is performed using scheduling, routing and network coding of sensing and actuation data"* D'Innocenzo et al. (2015), air transportation systems Park et al. (2014), and vehicle platooning Sajjad et al. (2015).

Table 11
Bad data detection.

Anomaly detector	Primary studies
Arbitrary	Giani et al. (2013); Nudell et al. (Sept. 2015); Teixeira et al. (2015b); Rhouma et al. (2015); Bai et al. (2015); Naghnaeian et al. (2015); Chen et al. (2015b); Lee et al. (2015); Sanjab and Saad (2015)
Largest normalized residual test	Kosut et al. (2011); Hendrickx et al. (2014); Teixeira et al. (2010); Yang et al. (2014); Davis et al. (2012); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012); Ozay et al. (2013); Vuković and Dán (2014); Kim et al. (2014a); Li (2014) Wang and Ren (2014); Hao et al. (2015); Yu and Chin (2015); Chakhchoukh and Ishii (2015); Li et al. (2015a); Esmalifalak et al. (2012); Ma et al. (2015); Teixeira et al. (2015b); Weerakkody and Sinopoli (2015); Shoukry et al. (2015b)
Novel	Kosut et al. (2011); Huang et al. (2010); Pasqualetti et al. (2013, 2011); Tajer et al. (2011); Sou et al. (2014); Wei and Kundur (2015); Zonouz et al. (2012); Vuković and Dán (2014); Valenzuela et al. (2013) Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016); Li (2014); Sanandaji et al. (2014); Manandhar et al. (2014); Rawat and Bajracharya (2015); Gu et al. (2015); Li et al. (2015a); Mo et al. (2015); Amin et al. (2010) Sundaram et al. (2010); Cáardenas et al. (2011); D'Innocenzo et al. (2015); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Li et al. (2015c); Park et al. (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014); Sajjad et al. (2015) Tang et al. (2015); Do et al. (2015)
Performance index test	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Teixeira et al. (2010); Yuan et al. (2012); Kim and Poor (2011); Esmalifalak et al. (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Davis et al. (2012); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012) Ozay et al. (2013); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Wang et al. (2014); Lo and Ansari (2013); Liu et al. (2014a); Qin et al. (2013); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b); Liang et al. (2014); Yamaguchi et al. (2014); Rahman et al. (2014); Manandhar et al. (2014); Tan et al. (2014) Kim et al. (2015); Liu et al. (2015a); Rawat and Bajracharya (2015); Anwar et al. (2015); Chakhchoukh and Ishii (2015); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Ma et al. (2015); Mo et al. (2015); Mo and Sinopoli (2012); Teixeira et al. (2015b); Kwon et al. (2014); Teixeira et al. (2012); Rhouma et al. (2015) Miao and Zhu (2014); Weimer et al. (2014); Park et al. (2014); Miao et al. (2014); Weerakkody and Sinopoli (2015); Zhang and Sankar (2015); Shoukry et al. (2015a)

In the power system domain, Kosut et al. (2011) proposes a generalized likelihood ratio detector, that incorporates historical data and does not compute explicitly the residue error, while Gu et al. (2015) introduces a new method to detect false data injection attacks against AC state estimation by tracking the dynamics of measurement variations: the Kullback–Leibler distance (KL divergence, known also as relative entropy) is used to calculate the distance between two probability distributions derived from measurement variations.

The KL divergence is adopted also by Mo et al. (2015), Weerakkody et al. (2014)[6] in designing the optimal watermark signal in the class of stationary Gaussian processes, which is used to derive the optimal Neyman–Pearson detector of reply and covert attacks, respectively.

Valenzuela et al. (2013) use principal component analysis (PCA) to separate power flow variability into regular and irregular subspaces, with the analysis of the information in the irregular subspace determining whether the power system data has been compromised. Also Liu Liu et al. (2014a) views false data detection as matrix separation problem and, differently from the case of the PCA, proposes algorithms that exploit *"the low rank structure of the anomaly-free measurement matrix, and the fact that malicious attacks are quite sparse."*

Tiwari et al. (2014) propose an approach inspired by PCA, that uses an invariant *"– an over-approximation of the reachable states – of the system under normal conditions as the classifier";* this set is called the safety envelope. An alarm is raised whenever the system state falls outside the safety envelope.

Security-oriented cyber-physical state estimation (SCPSE) for power grid, proposed in Zonouz et al. (2012), uses stochastic information fusion algorithms on *"information provided by alerts from intrusion detection systems that monitor the cyber infrastructure for malicious or abnormal activity, in conjunction with knowledge about the communication network topology and the output of a traditional state estimator"*, in order to detect intrusions and malicious data, and to assess the cyber-physical system state.

Other novel anomaly detection methods in power grid comprise a detector implementing the Euclidean distance metric (Manandhar et al., 2014), and a cosine similarity matching based approach (Rawat and Bajracharya, 2015). It is worth noting that the second one requires the usage of the Kalman filter as a source of estimated/expected data.

To contrast false data injection attacks, Sedghi and Jonckheere (2015) presented a decentralized detection and isolation scheme based on the Markov graph of the bus phase angles, obtained via conditional mutual information threshold (CMIT) test, while Sou et al. (2014) introduced a scheme, that considers potentially compromised information from both the active and the reactive power measurements on transmission lines. In this second scheme, based on the novel reactive power measurement residual, *"the component of the proposed residual on any particular line depends only locally on the component of the data attack on the same line"*. Li and Wang (Li, 2014) presented the state summation detection using state variables' distributions, which tests hypothesis on true measurement square sum S_x (assumed to follow normal distribution, given a large number of state variables) together with test on $J(\hat{x})$. Sanandaji et al. (2014) introduced a heuristic for detecting abrupt changes in the system outputs based on the singular value decomposition of a history matrix built from system observations. To detect the presence of a replay attack without injecting authentication noise to the control signal in networked control systems (NCS) involving additive white Gaussian noise channels, Tang et al. (2015) presented a hypothesis test based on spectral estimation techniques. For dissipative or passive CPS, Eyisi and Koutsoukos (2014) proposed energy-based attack detection monitor. To contrast stochastic cyber-attacks, Li et al. (2015c) presented an algebraic detection scheme based on the frequency-

[6] This work was extended by [S117].

Table 12
Controllers.

Controller	Primary studies
Event-triggered and self-triggered	Foroush and Martínez (2013); De Persis and Tesi (2015); Shoukry and Tabuada (2014); Cetinkaya et al. (2015); Xu and Zhu (2015)
Linear-quadratic regulator	Mo et al. (2015); Mo and Sinopoli (2012); Teixeira et al. (2015b); Rhouma et al. (2015); Barreto et al. (2013); Kwon and Hwang (2013b); Miao and Zhu (2014); Chen et al. (2015a); Djouadi et al. (2015); De Persis and Tesi (2015); Liu et al. (2014c); Weerakkody and Sinopoli (2015); Yuan and Mo (2015)
Linear time-invariant feedback	Smith (2015); Fawzi et al. (2014); Teixeira et al. (2015b); Xue et al. (2014); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Barreto et al. (2013); Miao and Zhu (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015) De Persis and Tesi (2015); Liu et al. (2014c); Mishra et al. (2014); Weerakkody and Sinopoli (2015); Tang et al. (2015); Kontouras et al. (2015)
H_∞ (minimax)	Smith (2015); Zhu and Başar (2015); Shoukry et al. (2013); Kwon and Hwang (2013b); Xu and Zhu (2015)
Novel	Hammad et al. (2015a); Wei and Kundur (2015); Amin et al. (2009); Gupta et al. (2010); Befekadu et al. (2015); Zhu and Martínez (2014); Zhu et al. (2018); Kwon and Hwang (2013b); Kogiso and Fujita (2015); Yuan and Mo (2015) Cetinkaya et al. (2015); Kontouras et al. (2015)
Other	Naghnaeian et al. (2015); Xu and Zhu (2015); Teixeira et al. (2015a)
Proportional-integral-derivative	Vrakopoulou et al. (2015); Amini et al. (2015); Amin et al. (2010); Cáardenas et al. (2011); Eyisi and Koutsoukos (2014); Bezzo et al. (2015); Sajjad et al. (2015)
Sliding mode	Hammad et al. (2015b); Liu et al. (2014b); Sajjad et al. (2015)

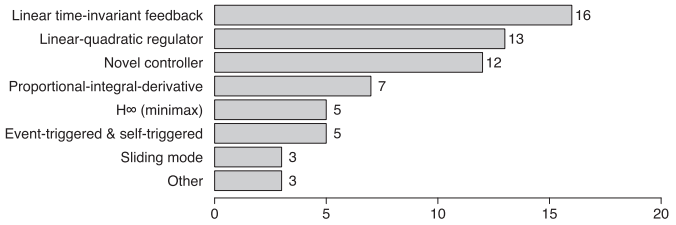


Fig. 17. Distribution of primary studies by controller.

domain transformation technique and linear algebra theory, together with sufficient and necessary conditions guaranteeing the detectability of such attacks. Finally, Jones et al. (2014) presents an automated anomaly detection mechanism based on inference via formal methods to develop an unsupervised learning algorithm, which constructs from data a signal temporal logic (STL) formula that describes normal system behavior. Trajectories that do not satisfy the learned formula are flagged as anomalous.

As a general comment, the literature described in this section appears quite fragmented, and a systematic high level view is still missing even within a specific application domain. The different results and methodologies are very difficult to relate each other and validate since both a comparison metric and a benchmark, neither academic nor industrial, have not been agreed and defined yet.

5.10. Controller

Considering the used controller, the first fact emerging from our analysis is that studies focusing on state estimation usually do not examine at all the controller. So in 91 (65.9% of 138 selected) studies the controller is not available. In the remainder of this section we will focus on the remaining 47 studies, some of which consider more than one controller at once.

As shown in Fig. 17, the most considered controllers are generic state feedback or output feedback controllers with a control law restricted to be linear time invariant, found in 16 (i.e. 11.6% of all) studies, together with linear quadratic regulators (LQR) and novel controllers, seen in 13 and 12 works, respectively. Variations of proportional-integral-derivative (PID) controller are found in 7 primary studies, while both the event-triggered and self-triggered controllers, and the H_∞ (minimax) controllers are considered by 5 works, whilst sliding mode and other types of controllers are deployed in 3 papers. Table 12 provides the related mapping.

The "other" control schemes not listed explicitly in Table 12 were used in cloud-enabled NCS and in interconnected microgrids, as well as in more generic CPS. Specifically, Xu and Zhu [S128] proposed a control design for cloud-enabled NCS, where the controller encrypts data via a randomized transformation, prior to the computation of the contro law in the cloud, and verifies the solutions from the cloud. The presented controller has three operational modes, with the switching mechanism between event-triggered model predictive controller, buffer mode and H_∞ controller. Teixeira et al. (2015a) instead studied the impact of adversarial actions on voltage control schemes in interconnected microgrids. It presented two attack scenarios where the adversary corrupts measurement data and reference signals received by the voltage droop controllers. Considering sampled-data nature of controlled CPS consisting of the continuous physical dynamics and the digital controllers, Naghnaeian et al. (2015) showed that dual rate control is sufficient to remove all the vulnerabilities to stealthy actuator attacks, and that if a single measurement output remains secure, and if the modes of the system are observable from this output, then dual rate systems always provide the ability to detect combined sensor-actuator attacks.

For what concerns the novel controllers, inspired by the analogy to flocking behavior, Wei and Kundur (2015) developed distributed hierarchical *"control methodologies that leverage cooperation between distributed energy resources and traditional synchronous machines to maintain transient stability in the face of severe disturbances"*. For a class of DoS attack models, Amin et al. (2009) presented an optimal minimax causal feedback control law, subject to the power, safety and security constraints. Then, Gupta et al. (2010) studied a similar problem of optimal minimax control in the presence of an intelligent jammer with limited actions as dynamic zero-sum game between the jammer and the controller. Befekadu et al. (2015) introduced instead the *"measure transformation technique under which the observation and state variables become mutually independent along the sample-path (or path-estimation) of the DoS attack sequences in the system"*, thanks to which it derived the optimal control policy for the risk-sensitive control problem, under a Markov modulated DoS attack model. Zhu and Martínez (2014) proposed a variation of the receding-horizon control law to deal with the replay attacks, Zhu et al. (2018) provided a set of coupled Riccati differential equations characterizing feedback Nash equilibrium as the solution concept for the distributed control in the multi-agent system environment subject to cyber attacks and malicious behaviors of physical agents. Kwon and Hwang (2013b) proposed *"a hybrid robust control scheme that considers multiple sub-controllers, each*

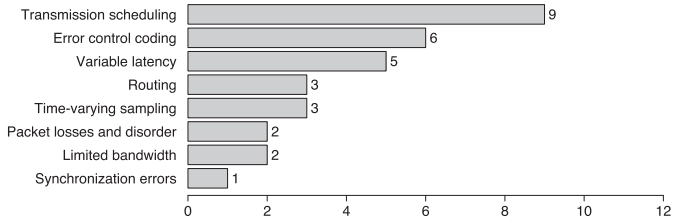


Fig. 18. Distribution by communication aspects and network-induced imperfections.

matched to a specific type of cyber attacks", together with a method for designing the corresponding secure switching logic. For an efficient transient frequency and phase stabilization in the power grid, Hammad et al. (2015a) proposed the combined centralized-decentralized parametric feedback linearization controller which is resilient to large communication delays and denial-of-service (DoS) attacks. Cetinkaya et al. (2015) instead presented a numerical method for designing an event-triggered state-feedback control that guarantees almost sure asymptotic stabilization of NCS subject to (simultaneous) malicious jamming attacks and random packet-losses modeled by a binary-valued time-inhomogeneous Markov chain. Yuan and Mo (2015) provided necessary and a sufficient conditions under which an adversary can successfully identify the system model by using only its disclosure resources (presenting also the similarities with the known-plaintext attack from the information security literature) and designed a countermeasure by using a low-rank controller design strategy while trading off the linear quadratic Gaussian control performance. In order to conceal several informations (such as controller and plant model parameters, measurements and control commands) processed inside the controller device, Kogiso and Fujita [S124] proposed a concept of encrypting a linear controller using the homomorphic encryptions, in a way that the encrypted controller need not to keep any private keys for calculating the control input, which means that the decryption process is not required inside the controller. Lastly, Kontouras et al. (2015) examined a constrained multivariable dynamical system, where a contractive controller and a covert attacker take turns in affecting the control input. It presented an adversary control scheme based on an expanding controller that steers and keeps the state vector outside the desired operation domain, while always respecting the alarm constraints. The proposed control scheme allows the attacker relinquish its authority over the control input according to a switching logic, in order to achieve the main task with a limited use of the available disruption resources.

As a general comment, the literature described in this section derives interesting theoretical results, but there is still a lot of work to do for addressing the practical challenges in CPS security.

5.11. Communication aspects and network-induced imperfections

The introduction of the communication network in a control loop modifies the external signals of the plant and the controller due to the network-induced imperfections (Levine, 2010), which in turn depend on some communication aspects, such as transmission scheduling and routing.

When analyzing the primary studies on the basis of this facet we got a surprise: 119 studies (i.e. 86.2%) do not explicitly consider any communication aspect or imperfection, while only 7 studies (i.e. 5.1%) address more than one aspect. The total number of times each communication aspect was addressed within the set of the primary studies is shown in Fig. 18, whilst the related mapping is reported in Table 13.

Synchronization errors are considered only by Pajic et al. (2014) (which is part of the research line of Pajic et al. (2015)), where also variable latency and time-varying sampling are mapped into parameters of the state estimation procedure that describe modeling errors. Time-varying sampling is taken into account also by Li et al. (2015a) and, together with transmission scheduling, by De Persis and Tesi (2015). Limited bandwidth is considered together with error control coding by Gupta et al. (2011) (which is related to Gupta et al. (2010)), and by Sundaram et al. (2010), in which *"nodes in a network transmit linear combinations of incoming packets rather than simply routing them"*. Packet losses and disorder were taken into consideration only together with transmission scheduling, by Cetinkaya et al. (2015) and by Shoukry et al. (2013). Noticeably, Shoukry et al. (2013) took into account also the variable latency. Only the variable latency was considered by Miao and Zhu (2014) and by Jones et al. (2014). Routing by itself is examined by Vuković et al. (2012), and together with error control coding, transmission scheduling and variable latency, by D'Innocenzo et al. (2015). The error control coding and transmission scheduling by themselves were taken into account in 3 (Fawzi et al. (2014); Miao et al. (2014); Mishra et al. (2014)) and 5 works (Li et al. (2015b); Foroush and Martínez (2013); Chen et al. (2015a); Zhang et al. (2014); Qi et al. (2015)), respectively.

Surprisingly, very few papers (attempt to) provide non-trivial mathematical models of the communication protocol, which indeed is a fundamental actor of almost any CPS. In particular, only in D'Innocenzo et al. (2015) a specific standard for communication, i.e. WirelessHART and ISA-100, is explicitly considered in the CPS mathematical model.

5.12. Attacks and their characteristics

Regardless of the adopted point of view (see Section 5.2), every study on CPS security deals with attacks in order to either implement or to counteract them. Each attack threats one or more primary security attributes (see Section 5.3). More specifically, the best known attack on availability is the *denial of service* (DoS) attack, that renders inaccessible some or all the components of a control system by preventing transmissions of sensor or/and control data over the network. *"To launch a DoS an adversary can jam the communication channels, compromise devices and prevent them from sending data, attack the routing protocols, flood with network traffic some devices, etc."* Amin et al. (2009). Attacks on data integrity are known as *deception* attacks and represent the largest class of attacks on cyber-physical systems, including false data injection attacks. The attacks on confidentiality alone are often referred to as *disclosure* attacks, i.e. *eavesdropping*, which is discussed only in six studies, as reported in Table 14.

Fig. 19 shows the distribution of attacks within the set of our primary studies. The false data injection, together with generic deception and DoS, with 58, 41 and 23 occurrences respectively, are considered in 108 (78.3%) primary studies, while the bias injection, the packet scheduling, and the variable structure switching attacks are considered only once and twice, respectively.

Characterization of the attacks. Generally speaking, an attack on control systems can be characterized by the amount of available resources and knowledge Teixeira et al. (2015b). The resources of an adversary can be split in *disclosure* resources, which enable her to obtain sensitive information about the system during the attack by violating data confidentiality, and *disruption* resources, that affect the system operation by compromising the integrity and/or availability. The amount of a priori *knowledge* regarding the control system is another core component of the adversary model, as it may be used, for instance, to render the attack undetectable. In the rest of Section 5.12 we describe the characteristics of each type of attack individually.

Table 13
Communication aspects and network-induced imperfections.

Feature	Primary studies
Error control coding	Gupta et al. (2010); Sundaram et al. (2010); Fawzi et al. (2014); D'Innocenzo et al. (2015); Miao et al. (2014); Mishra et al. (2014)
Limited bandwidth	Gupta et al. (2010); Sundaram et al. (2010)
Packet losses and disorder	Shoukry et al. (2013); Cetinkaya et al. (2015)
Routing	Vuković et al. (2012); Sundaram et al. (2010); D'Innocenzo et al. (2015)
Synchronisation errors	Pajic et al. (2015)
Time-varying sampling	Li et al. (2015a); Pajic et al. (2015); De Persis and Tesi (2015)
Transmission Scheduling	Li et al. (2015b); Foroush and Martínez (2013); Shoukry et al. (2013); D'Innocenzo et al. (2015); Chen et al. (2015a); De Persis and Tesi (2015); Zhang et al. (2014); Qi et al. (2015); Cetinkaya et al. (2015)
Variable Latency	Shoukry et al. (2013); D'Innocenzo et al. (2015); Miao and Zhu (2014); Pajic et al. (2015); Jones et al. (2014)

Table 14
Attacks.

Attack name	Primary studies
Attack at physical layer	Soltan et al. (2015); Zhu et al. (2018); Sajjad et al. (2015); Shoukry et al. (2015a)
Bias injection	Teixeira et al. (2015b)
Covert attack	Pasqualetti et al. (2013); Smith (2015); Teixeira et al. (2015b); Bopardikar and Speranzon (2013); Weerakkody and Sinopoli (2015); Do et al. (2015); Kontouras et al. (2015); Lee et al. (2015)
Data framing attack	Kim et al. (2014a); Deka et al. (2015b); Kim et al. (2015)
Denial of service (DoS)	Li et al. (2015b); Hammad et al. (2015a); Manandhar et al. (2014); Soltan et al. (2015); Rawat and Bajracharya (2015); Ma et al. (2015); Amin et al. (2009); Gupta et al. (2010); Befekadu et al. (2015); Zhu and Martínez (2014); Zhu and Başar (2015) Teixeira et al. (2015b); Foroush and Martínez (2013); Barreto et al. (2013); Chen et al. (2015a); Eyisi and Koutsoukos (2014); Djouadi et al. (2015); De Persis and Tesi (2015); Liu et al. (2014c); Li et al. (2015c); Park et al. (2014); Cetinkaya et al. (2015); Xu and Zhu (2015)
Eavesdropping	Teixeira et al. (2015b); Xue et al. (2014); Kogiso and Fujita (2015); Yuan and Mo (2015); Xu and Zhu (2015); Shoukry et al. (2015a)
False data injection	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Teixeira et al. (2010); Huang et al. (2010); Kim and Poor (2011); Pasqualetti et al. (2013, 2011); Esmalifalak et al. (2011); Tajer et al. (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Davis et al. (2012); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012) Ozay et al. (2013); Zonouz et al. (2012); Rahman and Mohsenian-Rad (2012); Wang et al. (2014); Lo and Ansari (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016); Qin et al. (2013); Deka et al. (2014); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liang et al. (2014); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Manandhar et al. (2014) Kim et al. (2015); Yu and Chin (2015); Liu et al. (2015a); Rawat and Bajracharya (2015); Anwar et al. (2015); Gu et al. (2015); Li et al. (2015a); Xie et al. (2011); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Kim et al. (2014b); Mo and Sinopoli (2012) Teixeira et al. (2015b); Mo and Sinopoli (2015); Bai et al. (2015); Weimer et al. (2014); Miao et al. (2014); Mishra et al. (2015b); Shoukry et al. (2015b); Sanjab and Saad (2015)
Generic deception	Vrakopoulou et al. (2015); Li et al. (2015b); Pasqualetti et al. (2013); Wei and Kundur (2015); Vuković and Dán (2014); Mishra et al. (2015a); Valenzuela et al. (2013); Nudell et al. (Sept. 2015); Jia et al. (2014); Mo and Sinopoli (2012); Amin et al. (2010); Gupta et al. (2010); Sundaram et al. (2010); Cáardenas et al. (2011) Fawzi et al. (2014); Kwon et al. (2014); D'Innocenzo et al. (2015); Kwon and Hwang (2013a); Barreto et al. (2013); Kwon and Hwang (2013b); Miao and Zhu (2014); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Djouadi et al. (2015); Bai et al. (2015); Zhang et al. (2014); Bezzo et al. (2014); Li et al. (2015c); Park et al. (2014) Mishra et al. (2014); Shoukry and Tabuada (2014); Jones et al. (2014); Bezzo et al. (2015); Qi et al. (2015); Naghnaeian et al. (2015); Xu and Zhu (2015); Chen et al. (2015b); Do et al. (2015); Teixeira et al. (2015a); Tan et al. (2015)
Leverage point attack	Tan et al. (2014); Chakhchoukh and Ishii (2015)
Load altering attack	Pasqualetti et al. (2013); Mohsenian-Rad and Leon-Garcia (2011); Amini et al. (2015)
Load redistribution attack	Yuan et al. (2012); Liu et al. (2015b); Bi and Zhang (2013)
Packet scheduling attack	Shoukry et al. (2013)
Reply attack	Pasqualetti et al. (2013); Gu et al. (2015); Mo et al. (2015); Zhu and Martínez (2014); Teixeira et al. (2015b); Miao and Zhu (2014); Shoukry and Tabuada (2014); Tang et al. (2015)
Switching attack	Hammad et al. (2015b); Liu et al. (2014b)
Topology poisoning	Giani et al. (2013); Kim and Tong (2013); Deka et al. (2015a); Rahman et al. (2014); Zhang and Sankar (2015)
Zero dynamics	Teixeira et al. (2015b, 2012); Rhouma et al. (2015); Li et al. (2015c); Naghnaeian et al. (2015)

In the **bias injection** attack, considered only by Teixeira et al. (2015b), the adversary's goal is to inject a constant bias in the system without being detected. *No disclosure* capabilities are required for this attack, since the attack policy is open-loop. The data corruptions may be added to both the actuator and sensor data, and the amount of disruption resources should be *above the threshold of undetectability*[7]. Furthermore, the open-loop attack policy requires an extensive knowledge of the parameters of the considered closed-loop system and anomaly detector.

In the coordinated **variable structure switching** attack and its extension to multi-switch and resonance attack, considered in the works of Liu et al. (2014b) and in the work of Hammad et al. (2015b), an opponent controls multiple circuit

[7] In other words, the attacker should have enough resources to construct an unobservable attack; a good example of the amount of disruption resources above the threshold of undetectability in the context of power transmission networks is given by the security index (Sandberg et al., 2010), defined as minimum number of measurements an attacker needs to compromise, in order to attack measurement k without being detected.

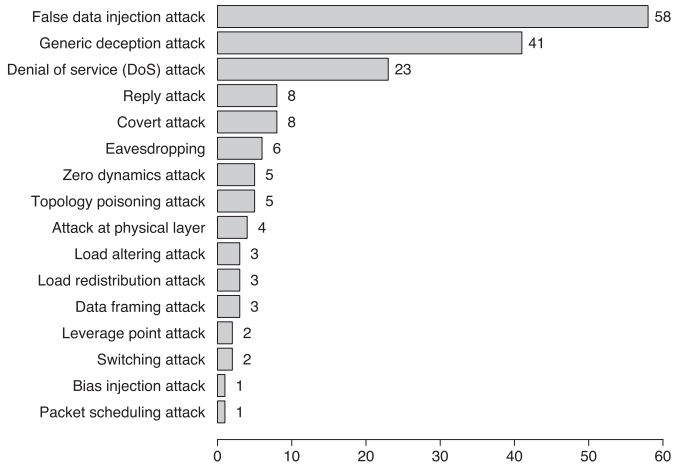


Fig. 19. Distribution of attacks considered by primary studies.

breakers within a power system, and employs a local model of the system and local state information (i.e. some knowledge of the target generator states, which are rotor angle and frequency) to design a state-dependent breaker switching sequence, that destabilizes target synchronous generators.

The attack on the **scheduling** algorithm influences the temporal characteristics of the network, as *"it results in time-varying delays and data packets possibly received out-of-order"* Shoukry et al. (2013). To remain stealthy, the attacker is not able to delay the packets beyond a maximum allowable delay consistent with the network protocol in place. On the system level, this attack does not require any a priori knowledge of the system model, nor any disclosure resources.

The **false data injection** is a specific deception attack on state estimation, introduced in the context of electric power grids by Liu et al. (2011). This attack on cyber-physical systems is the most studied one. To perform it, an adversary with some knowledge of the system topological information manipulates sensor measurements in order to change the state variables, while bypassing existing bad data detection schemes. This attack is based on the open-loop policy and does not require any disclosure resources. To construct the attack vectors, a common assumption in most works on false data injection attacks on power system state estimation is that the attacker has complete knowledge about the power grid topology and transmission-line admittances. This information is abstracted in the Jacobian matrix **H** (Huang et al., 2012; Abur and Exposito, 2004), known also as measurement or (power network) topology matrix. By contrast, Teixeira et al. (2010) assumes the attacker only possesses a perturbed model of the power system, *"such a model may correspond to a partial model of the true system, or even an out-dated model"* [S006]. In this way it quantifies a trade-off between the accuracy of the model known by adversary and possible attack impact for different BDD schemes, showing that *"the more accurate model the attacker has access to, the larger deception attack he can perform undetected"* [S006]. Similarly, Rahman and Mohsenian-Rad (2012) argues that *"a realistic false data injection attack is essentially an attack with incomplete information due to the attackers lack of real-time knowledge with respect to various grid parameters and attributes such as the position of circuit breaker switches and transformer tap changers and also because of the attacker's limited physical access to most grid facilities"*, and presents a vulnerability measure for topologies of power grids subject to attacks based on incomplete information. On the same line, Bi and Zhang (2014) derives a necessary and sufficient condition to perform undetectable false data injection attack with partial topological information and develops a min-cut method to design the optimal attack, which requires the minimum knowledge of system topology.

Finally, the problem of constructing a *blind* false data injection attacks without explicit prior knowledge of the power grid topology is studied by Esmalifalak et al. (2011), Kim et al. (2015), and Yu and Chin (2015). In Esmalifalak et al. (2011) attackers try to make inferences through phasor observations applying linear independent component analysis (ICA) technique. However, such technique requires that loads are statistically independent and non-Gaussian, and the technique need full sensor observations (Kim et al., 2015). Kim et al. (2015) instead proposes subspace methods, which requires no system parameter information. In this case the attack can be launched with only partial sensor observations. Yu and Chin (2015) proposes to use principal component analysis (PCA) approximation method without the assumption regarding the distribution of state variables, to perform the same task of making inferences from the correlations of the line measurements, in order to construct the blind false data injection attack.

Differently from the works on undetectable false data injection attacks on power grids summarized up to here, Qin et al. (2013) presents an *unidentifiable* version of this attack, in which the control center can detect that there are bad or malicious measurements, but it cannot identify which meters have been compromised.

A special type of false data injection attack on electric power grid is the **load redistribution** attack, in which only load bus power injection and line power flow measurements are attackable (Yuan et al., 2012). It consists in increasing load at some buses and reducing loads at other buses, while maintaining the total load unchanged, in order to hide the attack from bad data detection. The construction of load redistribution attack relies on topological information of the network, that can be derived from the Jacobin matrix **H**. Considering the practical issue that an attacker can only obtain the parameter information of a limited number of lines, Liu et al. (2015b) present a strategy to determine optimal local attacking region, that requires the minimum network parameter information. The undetectability is obtained by *"making sure that the variations of phase angles of all boundary buses connected to the same island of the nonattacking region are the same"* (Liu et al., 2015b). A practical cost-aware "neighbourhood" version of such attack compromising only limited measurements around the targeted bus can be found in Bi and Zhang [S071].

The **data framing** attack is a deception attack on power system state estimation that exploits current bad data detection and removal mechanisms. It purposely triggers the bad data detection mechanism and frames some normally operating meters as sources of bad data such that their data will be removed. After such data removal, although the remaining data appear to be consistent with the system model, the resulting state estimate may have an arbitrarily large error (Kim et al., 2014a). Also this attack does not require any disclosure resources, since the attack policy is open-loop. By applying the subspace methods presented in 2015 by Kim et al. (2015) to learn the system operating subspace from measurements, the data framing can be performed without knowledge of the Jacobian matrix **H**. A limited a priori knowledge required consists of a basis matrix **U** of a subspace of all possible noiseless measurements $\mathcal{R}$ of **H**. Deka et al. (2015b) showed that a generalization of this "detectable" attack model produces feasible attacks in operating regimes where no "hidden" attacks are possible, and also considered the impact of adding measurement jamming to the adversary's arsenal on the design of the optimal data attacks.

The **leverage point** attack is a deception attack which creates leverage points within the factor space of the (power system) state estimation regression model Tan et al. (2014). The residual of the measurement corresponded with the leverage point is very

small even when it is contaminated with a very large error. Thus the adversary can freely introduce arbitrary errors into the meter measurements without being detected. This attack is based on an open-loop policy and thus does not require disclosure resources. However, to be fully effective, it requires a complete knowledge of the Jacobian matrix **H** and amount of disruption resources above the threshold of undetectability (Chakhchoukh and Ishii, 2015).

The **load altering** attack against power grid's demand response and demand side management programs can bring down the grid or cause significant damage to the power transmission and user equipment. It consists in an attempt to control and change (usually increase) certain load types in order to damage the grid through circuit overflow or disturbing the balance between power supply and demand (Mohsenian-Rad and Leon-Garcia, 2011). The *static* load altering is mainly concerned in changing the volume of the load. Here the attacker without any prior knowledge of the plant model uses some historical data to impose a pre-programmed trajectory to the victim load (an open-loop policy). In the more advanced *dynamic* load altering attack, presented in 2015 by Amini et al. (2015), the adversary *"constantly monitors the grid conditions through the attacker's installed sensors so that it can adjust the attack trajectory based on the current conditions in the power grid"* (Amini et al., 2015). With this closed-loop policy, the attacker having a complete knowledge of the plant's model controls the victim load based on a feedback from the power system frequency and can make the power system unstable, without the need for increasing the scope or volume of the attack, compared to a static scenario.

The attacks at **physical layer** range from attacks that affect both the physical infrastructure and the control network (of power grids) Soltan et al. (2015) to attacks through physical layer interactions, such as an attack on vehicle platoon traveling at a constant speed, presented by Sajjad et al. (2015). The attack studied by Soltan et al. (2015) physically disconnects some power lines within the attacked zone (which is defined as a set of buses, power lines, phasor measurement units (PMUs) and an associated phasor data concentrator (PDC) (Huang et al., 2012)) and disallows the information from the PMUs within the zone to reach the control center. This attack does not require any knowledge of the plant model, nor disclosure resources. The attack on vehicle platoons (Sajjad et al., 2015) is carried out by a maliciously controlled vehicle, who attempts to destabilize or take control of the platoon by combining changes to the gains of the associated law with the appropriate vehicle movements. This closed-loop attack *"bears some resemblance to an insider version of the replay attack of Pasqualetti et al. (2013), in that the attacker is part of the CPS and is therefore able inject control inputs legitimately"*.

In **topology poisoning** attack an adversary covertly alters data from certain meters, network switches and line breakers to mislead the control center with an incorrect network topology. Kim and Tong (2013) shows that under certain conditions even in a local information regime, where the attacker has only local information from those meters it has gained control, undetectable topology poisoning attacks exist and can be implemented easily based on simple heuristics. Deka et al. (2015a) proves that grids completely protected by secure measurements are also vulnerable to hidden topology poisoning attacks, if the adversary armed only with generic information regarding the grid structure can corrupt the breaker statuses on transmission lines and jam the communication of flow measurements on the attacked lines. Then, Zhang and Sankar [S129] develops an algorithm based on breadth-first search to determine the minimum subset of topology data and measurements required to launch successful unobservable state-preserving line-maintaining topology attacks.

The **zero dynamics** attack, first considered in Sundaram and Hadjicostis (2011); Pasqualetti et al. (2012a), is one in which an adversary constructs an open-loop policy such that the attack signal produces no output. In other words, *"these attacks are decoupled from the plant output y_k, thus being stealthy with respect to arbitrary anomaly detectors"* (Teixeira et al., 2015b). For an attacker with limited disruption resources, zero dynamics attacks are based on the perfect (local) knowledge of the plant dynamics. In this setting, Teixeira et al. (2012) shows that zero-dynamics attacks may not be completely stealthy since they require the system to be at a non-zero initial condition; however for the subset of attacks exciting unstable zero-dynamics, the effect of initial condition mismatch in terms of the resulting increase in the output energy can be made arbitrarily small while still affecting the system performance. We should notice that an adversary capable of changing all the measurements can, of course, force the system's output to zero without any knowledge of the model, initial state and nominal input. Furthermore, for a linear not left-invertible system, the knowledge of the initial state is not required, because an attacker can exploit the kernel of the transfer matrix and the linearity of the system.

With the covert attack, also known as a **covert misappropriation** of the plant (Smith, 2015), an adversary can gain control of the plant in a manner that cannot be detected by the controller. This attack requires high levels of system knowledge and the ability of attacker to both read and replace communicated signals within the control loop, indeed *"the covert agent is assumed to have the resources to read and add to both the control actuation commands and the output measurements. In practice, this could also be accomplished by augmenting the physical actuators or modifying the sensors. Examples of such modifications include installing a controlled-flow bypass around a sluice gate in an irrigation system and connecting a controlled voltage source between a voltage measuring device and its intended connection point in an electrical network. Another potential mode of attack would involve corrupting the PLCs used by the nominal controller to implement the control and sensing operations"* (Smith, 2015). Pasqualetti et al. (2013) observe that the covert attack can be seen as a feedback version of the replay attack, while Smith (2015) examines also the effects of lower levels of system knowledge and nonlinear plants on the ability to detect a covert misappropriation of the plant.

The **replay** attack is a deception attack (possibly combined with a physical attack), in which an adversary first gathers sequences of measurement and/or control data, and then replays the recorded data while injecting an exogenous signal into the system (Teixeira et al., 2015b). The adversary requires no knowledge of the system model to generate stealthy outputs. However, the attacker needs to have *"enough knowledge of the system model to design an input that may achieve its malicious objective, such as physically damaging the plant"* (Mo et al., 2015). The model of this attack is inspired by the Stuxnet (Chen and Abu-Nimeh, 2011).

A **generic deception** attack is an attack on data integrity, where an adversary sends false information from (one or more) sensors or/and controllers in order to deceive a compromised system's component into believing that a received false data is valid or true (Mo and Sinopoli, 2012). Usually it is modeled as an arbitrary additive signal injected to override the original data. Since generic deception attacks can be used to represent also other, more specialized deception attacks, they are considered mostly in the studies adopting the defender's point of view, presented in Section 5.2.

There are 26 (18.8% of all) studies using a generic deception attack model only to develop some defense strategy, whilst the false-data injection into the communication network supporting the control system examined by Sanjab and Saad (2015) was already mentioned in Section 5.10. The remaining 14 primary studies present (generic) deception attacks, that are different from any other attack considered above. Vrakopoulou et al. (2015) deals with a cyber-attack on the automatic generation control (AGC) sig-

nal in multi-area power system as a controller synthesis problem, where the objective is to drive the system outside the safety margins. It investigates two cases according to whether the attacker has perfect model knowledge or not, and provides different alternatives for attack synthesis, ranging from *"open loop approaches, based on Markov Chain Monte Carlo (MCMC) optimization, to close loop schemes based on feedback linearization and gain scheduling"* [S005]. Always within power grids' application domain, Vuković and Dán (2014) consider a sophisticated adversary, that knows the system model and aims to disable the state-of-the-art distributed state estimation by preventing it from converging. To this end, he or she compromises the communication infrastructure of a single control center in an interconnected power system, in order to manipulate the exchanged data (i.e. state variables) used as an input to the state estimator. The stealthy cyber attacks that maximize the error in unmanned aerial systems' state estimation are studied in Kwon et al. (2014). To consider the worst-case security problem, this study assumes the attacker has the perfect knowledge on the system model and can compromise sensors and/or actuators. The attacks on both sensors and actuators by the adversary with a perfect knowledge of the static parameters of a CPS (modeled as a discrete LTI system equipped with a Kalman filter, LQR and χ^2 failure detector) are considered also by Mo and Sinopoli (2012), where the adversary's strategy is formulated as a constrained control problem. Djouadi et al. (2015) instead present optimal sensor signal attacks for the observer-based finite and infinite horizon linear quadratic (LQ) control in terms of maximizing the corresponding cost functions. Also this study assumes full-information, i.e. the system parameters are known to the adversary. Zhang et al. (2014) studies stealthy deception attacks on remote state estimation with communication rate constraints. Here the deception attacker intrudes the sensor, learns its online transmission strategy, and then modifies the event-based sensor transmission schedule in order to degrade the estimation quality. Li et al. (2015a) observes that sensors adopt an acknowledgement (ACK)-based online power schedule to improve the remote state estimation performance under limited resources, and that an attacker can modify the ACKs from the remote estimator and convey fake information to the sensor, thereby misleading the sensor with subsequent performance degradation. Li et al. (2015a) is a part of the research line represented by Li et al. (2015b). Lastly, Qi et al. (2015) designs an event-based (online) attack strategy to degrade the real-time state estimation quality with arbitrary communication rate constraint; this deception attack can be implemented by compromising a sensor in order to learn and modify the transmission decisions, eavesdropping the measurements and injecting false feedback information into the sensor. For the domain of electricity market, Tan et al. (2015) studies the impact of two common and broad classes of simple integrity attacks on real-time pricing, where either the prices advertised to consumers are compromised by a scaling factor or timing information of prices is corrupted, and provides the conditions under which the system is at risk of being destabilized. Jia et al. (2014) studies the average relative perturbation of the real-time locational marginal price as an optimization problem; the adversary is assumed to have not only the perfect knowledge of the system model, but also the possibility to access the measurement values in real-time, in order to inject bad data that is state independent, partially adaptive, or even fully adaptive. Targeting power consumption sector, Mishra et al. (2015a) introduces the price modification attack (under the name of rate alteration attack) which induces changes in load profiles of individual users through fabrication of price messages and eventually causes major alteration in the load profile of the entire power network. A stealthy deception scheme capable of compromising the performance of the automated cascade canal irrigation systems is presented by Amin et al. (2010). This attack scheme is based on approximate knowledge of canal hydrodynamics and is implemented via switching the linearized shallow water partial differential equation parameters and proportional boundary control actions, to withdraw water from the pools through offtakes. Similarly, the stealthy deception attacks on process control systems performed by a very powerful adversary with knowledge of the exact linear model of the plant, the parameters of anomaly detector and control command signals, are presented by Cárdenas et al. (2011). In the most sophisticated attack considered in this study, adversaries *"try to shift the behavior of the system very discretely at the beginning of the attack and then maximize the damage after the system has been moved to a more vulnerable state"* (Cárdenas et al., 2011). Finally, for a single-input single-output plant, Bai et al. (2015) analytically characterizes an optimal stealthy attack strategy, that maximizes the estimation error of the Kalman filter by tampering with the control input, as a function of the system parameters, noise statistics and information available to the attacker.

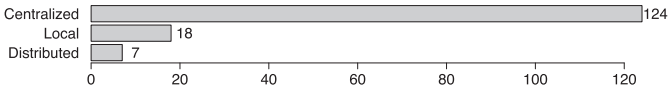


Fig. 20. Distribution of studies by attack scheme.

From such literature a systematic characterization of "types" of attack is emerging, even if the "generic deception attack" and "false data injection attack" have been primarily addressed.

5.13. Attack scheme

In this section we distinguish the selected studies based on whether they consider centralized, distributed or local attack strategies. The mapping between the considered attack schemes and the primary studies is reported in Table 15, whilst the distribution of studies based on this facet is summarized in Fig. 20.

The overwhelming majority of primary studies (117, i.e. 84.8% of all selected works) considers only near omniscient adversary, capable of compromising several system components in a centralized fashion, whereas there are only 7 works that study distributed attacks, and 18 (i.e. 13.0%) studies dealing with local attacks. It is clear from this data that local and especially distributed solutions require more attention.

As a side note, we observe that some works are considering the vulnerability of the system on both global and local scales, with attacks following a specific coordination model. As an example, in Kim and Tong [S031] both centralized and distributed attacks relying only on local measurements observed in the clusters are constructed, while in Davis et al. (2012) the adversary needs only local information to achieve the attack, but the work builds on a previous article from the same authors where a typical centralized attack was considered.

5.14. Plant model used by the attacker

This facet characterizes a modeling framework[8] used by an adversary to design an attack on a CPS. Since attacker's knowledge of the control system and plant model can be limited or absent, an adversary may rely on a model of plant that is different from the actual model used by a system operator. Here our focus is on such cases. Fig. 21 shows the distribution of the primary studies by plant model used by an attacker.

In 114 studies (82.6%) it is assumed that the attacker uses the same model of the plant as the system operator, while in 21 stud-

[8] See Section 5.5 for the analysis of the considered plant models.

Table 15
Attack schemas.

Scheme	Primary studies
Centralized	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Teixeira et al. (2010); Huang et al. (2010); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2013, 2011); Esmalifalak et al. (2011); Hammad et al. (2015a); Tajer et al. (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Mohsenian-Rad and Leon-Garcia (2011); Davis et al. (2012); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012); Ozay et al. (2013); Zonouz et al. (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013) Mishra et al. (2015a); Wang et al. (2014); Valenzuela et al. (2013); Lo and Ansari (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016); Qin et al. (2013); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Manandhar et al. (2014); Tan et al. (2014); Amini et al. (2015); Kim et al. (2015); Yu and Chin (2015); Liu et al. (2015a); Rawat and Bajracharya (2015); Anwar et al. (2015); Chakhchoukh and Ishii (2015); Gu et al. (2015); Nudell et al. (Sept. 2015); Li et al. (2015a); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Ma et al. (2015); Amin et al. (2009); Mo et al. (2015); Mo and Sinopoli (2012); Amin et al. (2010); Gupta et al. (2010); Sundaram et al. (2010); Cáardenas et al. (2011); Befekadu et al. (2015); Zhu and Martínez (2014); Smith (2015); Fawzi et al. (2014); Zhu and Başar (2015); Teixeira et al. (2015b); Kwon et al. (2014); Teixeira et al. (2012); Foroush and Martínez (2013); Zhu et al. (2018); Shoukry et al. (2013); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Rhouma et al. (2015); Barreto et al. (2013); Kwon and Hwang (2013b); Miao and Zhu (2014); Chen et al. (2015a); Mo and Sinopoli (2015); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Djouadi et al. (2015); Bai et al. (2015); Weimer et al. (2014); De Persis and Tesi (2015); Liu et al. (2014c); Bezzo et al. (2014); Li et al. (2015c); Park et al. (2014); Miao et al. (2014); Mishra et al. (2014); Shoukry and Tabuada (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014); Bezzo et al. (2015); Mishra et al. (2015b); Shoukry et al. (2015b); Naghnaeian et al. (2015); Yuan and Mo (2015); Cetinkaya et al. (2015); Xu and Zhu (2015) Chen et al. (2015b); Tang et al. (2015); Do et al. (2015); Kontouras et al. (2015); Shoukry et al. (2015a); Teixeira et al. (2015a); Tan et al. (2015); Lee et al. (2015); Sanjab and Saad (2015)
Distributed	Pasqualetti et al. (2013); Hammad et al. (2015b); Liu et al. (2014b); Tajer et al. (2011); Wei and Kundur (2015); Ozay et al. (2013); Zhu et al. (2018)
Local	Vrakopoulou et al. (2015); Li et al. (2015b); Hammad et al. (2015b); Liu et al. (2014b); Davis et al. (2012); Ozay et al. (2013); Kim and Tong (2013); Vuković and Dán (2014); Liu et al. (2015b); Liang et al. (2014); Sundaram et al. (2010); Xue et al. (2014); Zhu et al. (2018) Zhang et al. (2014); Sajjad et al. (2015); Qi et al. (2015); Kogiso and Fujita (2015); Zhang and Sankar (2015)

Table 16
Plant model used by an attacker.

Plant model	Primary studies
Absent	Hammad et al. (2015a); Mohsenian-Rad and Leon-Garcia (2011); Valenzuela et al. (2013); Soltan et al. (2015); Amin et al. (2009); Mo et al. (2015); Gupta et al. (2010); Befekadu et al. (2015); Zhu and Martínez (2014); Foroush and Martínez (2013); Shoukry et al. (2013); Chen et al. (2015a); De Persis and Tesi (2015) Liu et al. (2014c); Shoukry and Tabuada (2014); Kogiso and Fujita (2015); Yuan and Mo (2015); Cetinkaya et al. (2015); Do et al. (2015); Shoukry et al. (2015a); Tan et al. (2015)
Different	Kim et al. (2014a); Liang et al. (2014); Kim et al. (2015)

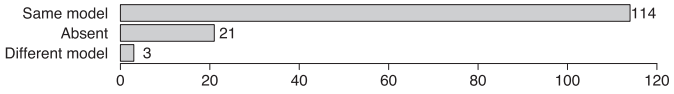


Fig. 21. Distribution of primary studies by plant model used by an attacker.

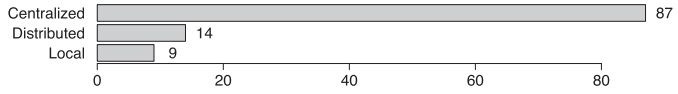


Fig. 22. Distribution of studies by defense scheme.

ies (15.2%) the adversary does not use any model of plant. In the remaining 3 works, listed in Table 16, the attacker uses a model of plant that is simpler than the one used by operator. In particular, in the works of Kim et al. (2014a), S056 data framing attacks on power transmission system are designed using a linearized system. It is shown that such attacks can successfully perturb a nonlinear *"state estimate, and the attacker is able to control the degree of perturbation as desired"* (Kim et al., 2014a). This is an answer on the question on *"whether attacks constructed from a linear model is effective in a nonlinear system"* (Kim et al., 2015). Liang et al. (2014) studies both DC and AC attack models to construct the false data injection in AC state estimation, showing that the DC attack is detectable when the injected values are too large, while the AC attack model permits to *"hide the attack completely"* (Liang et al., 2014).

5.15. Defense scheme

Similarly to attack schemes, we differentiate the studies also based on whether the proposed approach to defend a CPS focuses on the local or global scale of the system. In case of the global scale, this dimension also specifies whether a defense mechanism uses centralized or distributed coordination model.

We recall from Section 5.2 that there are 35 primary studies adopting only an adversary's point of view and not concerned with countermeasures against attacks. We say that for them the defense schemes are not available. The distribution of remaining (103, i.e. 74.6%) primary studies by defense scheme is shown in Fig. 22, while the related mapping is reported in Table 17.

Most of the studies (82) on defense mechanisms uses only centralized scheme, while the local scale is considered only in 9 works ((Pasqualetti et al. (2012b) and Liu et al. (2012), related to Pasqualetti et al. (2013) and Liu et al. (2014b), respectively, Li et al. (2015b); Liu et al. (2014c); Kogiso and Fu-

Table 17
Defense schemes.

Defense scheme	Primary studies
Centralized	Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Huang et al. (2010); Kim and Poor (2011); Pasqualetti et al. (2013); Hammad et al. (2015a); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Mohsenian-Rad and Leon-Garcia (2011); Davis et al. (2012); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Ozay et al. (2013); Zonouz et al. (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Wang et al. (2014); Valenzuela et al. (2013); Lo and Ansari (2013); Liu et al. (2014a) Yang et al. (2016); Qin et al. (2013); Deka et al. (2014); Li (2014, 2014); Wang and Ren (2014); Hao et al. (2015); Rahman et al. (2014); Manandhar et al. (2014); Tan et al. (2014); Soltan et al. (2015, 2015); Liu et al. (2015a); Rawat and Bajracharya (2015); Anwar et al. (2015); Gu et al. (2015); Nudell et al. (Sept. 2015); Li et al. (2015a); Jia et al. (2014) Esmalifalak et al. (2013); Ma et al. (2015); Amin et al. (2009); Mo et al. (2015); Amin et al. (2010); Gupta et al. (2010); Sundaram et al. (2010); Cáardenas et al. (2011); Befekadu et al. (2015); Zhu and Martínez (2014); Fawzi et al. (2014); Zhu and Başar (2015); Teixeira et al. (2012); Foroush and Martínez (2013); Shoukry et al. (2013); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Rhouma et al. (2015); Barreto et al. (2013); Kwon and Hwang (2013b); Miao and Zhu (2014) Mo and Sinopoli (2015); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Bai et al. (2015); Weimer et al. (2014); De Persis and Tesi (2015); Bezzo et al. (2014); Li et al. (2015c); Miao et al. (2014); Shoukry and Tabuada (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014); Bezzo et al. (2015); Mishra et al. (2015b); Shoukry et al. (2015b); Cetinkaya et al. (2015) Xu and Zhu (2015); Chen et al. (2015b); Tang et al. (2015); Do et al. (2015); Shoukry et al. (2015a); Lee et al. (2015); Sanjab and Saad (2015)
Distributed	Pasqualetti et al. (2013, 2011); Hammad et al. (2015a); Tajer et al. (2011); Wei and Kundur (2015); Ozay et al. (2013); Vuković and Dán (2014); Sedghi and Jonckheere (2015); Li et al. (2015a); Xue et al. (2014); Zhu et al. (2018); Park et al. (2014); Mishra et al. (2014) Sajjad et al. (2015)
Local	Li et al. (2015b); Pasqualetti et al. (2013); Liu et al. (2014b); Sou et al. (2014); Liu et al. (2014c); Sajjad et al. (2015); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Yuan and Mo (2015)

jita (2015); Naghnaeian et al. (2015); Yuan and Mo (2015), together with Sou et al. (2014), where the centralized scheme with some relevant local dependencies is taken into account, and Sajjad et al. (2015), where a sliding mode control using only local sensor information and a decentralized attack detector is considered). Distributed approaches are examined in 14 works (alone in Pasqualetti et al. (2011); Tajer et al. (2011); Wei and Kundur (2015); Vuković and Dán (2014); Sedghi and Jonckheere (2015); Xue et al. (2014); Zhu et al. (2018); Park et al. (2014); Mishra et al. (2014) and alongside centralized ones in Pasqualetti et al. (2013); Hammad et al. (2015a); Ozay et al. (2013); Li et al. (2015a)). We must point out that according to our selection strategy we do not consider the studies focused on the typical distributed problem of reaching consensus in the presence of malicious agents (Pasqualetti et al., 2012a; Sundaram and Hadjicostis, 2011); this is because in these works the dynamics is part of the consensus algorithm and can be specifically designed, rather than being given as in a physical system (Gu et al., 2015).

This data suggests that distributed and local defense solutions require more attention and surely present a promising direction in research on security of CPS from automatic control point of view.

5.16. Defense strategy

We have already anticipated in Section 5.2 that countermeasures against attacks, i.e. actions minimizing the risk of threats, are presented in more than three-fourth of primary studies, and occupy the central spot of the research efforts. The defense strategies can be classified as prevention, detection, and mitigation (Teixeira et al., 2015); following the line of the fault diagnosis literature (Hwang et al., 2010), we advocate isolation as a further defense strategy extending detection approaches.

Prevention aims at decreasing the likelihood of attacks by reducing the vulnerability of the system (Teixeira et al., 2015). It brings together all the actions performed **offline**, before the system is perturbed or attacked. There are 45 studies (32.6%) studying exclusively prevention mechanisms. These studies range from security metrics for the vulnerability analysis of systems or their

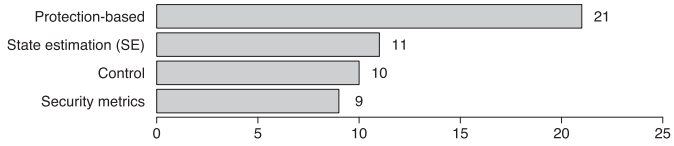


Fig. 23. Distribution of primary studies by prevention approach.

critical components to design and analysis of resilient state estimators and controllers capable to withstand some attacks, and protection-based approaches aiming to identify and secure some strategic distributed components. Fig. 23 shows the distribution of the primary studies focussing on prevention, whilst Table 18 provides the related mapping and Table 19 reports the mapping of individual studies to each defense strategy.

Twenty one studies present **protection-based** approaches. Among them, there are 7 studies discussing the *secure sensor allocation* against undetectable false data injection attacks in power transmission networks. More specifically, Bobba et al. (2010) show that it is necessary and sufficient to protect a set of basic measurements (in number equal to number of all the unknown state variables in the state estimation problem) to ensure that no such attack can be launched, while Giani et al. (2013) proof that placing $p+1$ secure phasor measurement units (PMUs) at carefully chosen buses are sufficient to neutralize any collection of p sparse attacks, and Kim and Tong (2013) present a so-called cover-up protection that identifies the set of meters that need to be secured so an undetectable attack does not exist for any target topology. Also Yang et al. (2014) identifies the critical meters to protect and observes that the meters measuring bus injection powers play a more important role than the ones measuring the transmission line power flows, since they are essential in determining a specific state variable, while the measurements of line power flows are redundant to improve the accuracy of state estimation. As finding the minimum number of protected sensors such that an adversary cannot inject false data without being detected is NP-hard[9]

[9] since this problem is reducible to the *hitting set problem*.

Table 18
Prevention-based approaches to defense.

Prevention approach	Primary studies
Control	Hammad et al. (2015a); Amin et al. (2009); Gupta et al. (2010); Befekadu et al. (2015); Zhu and Martínez (2014); Shoukry et al. (2013); Bezzo et al. (2015); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Yuan and Mo (2015); Cetinkaya et al. (2015)
Protection-based	Bobba et al. (2010); Kim and Poor (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Mohsenian-Rad and Leon-Garcia (2011); Talebi et al. (2010); Kim and Tong (2013); Wang et al. (2014); Lo and Ansari (2013); Deka et al. (2014); Wang and Ren (2014); Hao et al. (2015) Rahman et al. (2014); Soltan et al. (2015); Anwar et al. (2015); Esmalifalak et al. (2013); Ma et al. (2015); Teixeira et al. (2012); Bopardikar and Speranzon (2013); Miao et al. (2014)
Security metrics	Kosut et al. (2011); Hendrickx et al. (2014); Vuković et al. (2012); Rahman and Mohsenian-Rad (2012); Jia et al. (2014); Xue et al. (2014); Kwon and Hwang (2013a); Bai et al. (2015); Chen et al. (2015b)
State estimation	Giani et al. (2013); Tan et al. (2014); Liu et al. (2015a); Shoukry et al. (2013); Mo and Sinopoli (2015); Pajic et al. (2015); Weimer et al. (2014); Mishra et al. (2014); Shoukry and Tabuada (2014); Mishra et al. (2015b)

Table 19
Defense strategies.

Defense strategy	Primary studies
Prevention	Kosut et al. (2011, 2011); Hendrickx et al. (2014); Kim and Poor (2011); Hammad et al. (2015a); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Mohsenian-Rad and Leon-Garcia (2011); Talebi et al. (2010); Vuković et al. (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Wang et al. (2014); Lo and Ansari (2013) Deka et al. (2014); Wang and Ren (2014); Hao et al. (2015); Rahman et al. (2014); Tan et al. (2014); Soltan et al. (2015); Liu et al. (2015a); Anwar et al. (2015); Jia et al. (2014); Esmalifalak et al. (2013); Ma et al. (2015); Amin et al. (2009); Gupta et al. (2010) Befekadu et al. (2015); Zhu and Martínez (2014); Teixeira et al. (2012); Xue et al. (2014); Shoukry et al. (2013); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Mo and Sinopoli (2015); Pajic et al. (2015); Bai et al. (2015); Weimer et al. (2014); Miao et al. (2014); Mishra et al. (2014); Shoukry and Tabuada (2014) Bezzo et al. (2015); Mishra et al. (2015b); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Yuan and Mo (2015); Cetinkaya et al. (2015); Chen et al. (2015b)
Detection	Kosut et al. (2011); Huang et al. (2010); Pasqualetti et al. (2013, 2011); Tajer et al. (2011); Yang et al. (2014); Davis et al. (2012); Sou et al. (2014); Wei and Kundur (2015); Ozay et al. (2013); Zonouz et al. (2012); Vuković and Dán (2014); Valenzuela et al. (2013) Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016); Li (2014); Sanandaji et al. (2014); Hao et al. (2015); Manandhar et al. (2014); Soltan et al. (2015); Rawat and Bajracharya (2015); Gu et al. (2015); Nudell et al. (Sept. 2015); Li et al. (2015a); Mo et al. (2015); Amin et al. (2010) Sundaram et al. (2010); Cáardenas et al. (2011); D'Innocenzo et al. (2015); Rhouma et al. (2015); Miao and Zhu (2014); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Bezzo et al. (2014); Miao et al. (2014); Park et al. (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014); Sajjad et al. (2015) Shoukry et al. (2015b); Tang et al. (2015); Do et al. (2015); Shoukry et al. (2015a)
Isolation	Kosut et al. (2011); Pasqualetti et al. (2013); Tajer et al. (2011); Davis et al. (2012); Sou et al. (2014); Wei and Kundur (2015, 2015); Zonouz et al. (2012); Vuković and Dán (2014); Valenzuela et al. (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016); Qin et al. (2013); Hao et al. (2015) Soltan et al. (2015); Nudell et al. (Sept. 2015); Amin et al. (2010); Sundaram et al. (2010); Cáardenas et al. (2011); Foroush and Martínez (2013); D'Innocenzo et al. (2015); Tiwari et al. (2014); Bezzo et al. (2014); Park et al. (2014); Jones et al. (2014); Shoukry et al. (2015b); Do et al. (2015)
Mitigation	Li et al. (2015b); Liu et al. (2014b); Tajer et al. (2011); Wei and Kundur (2015); Vuković and Dán (2014); Qin et al. (2013); Soltan et al. (2015); Sundaram et al. (2010); Cáardenas et al. (2011); Fawzi et al. (2014); Zhu and Başar (2015); Foroush and Martínez (2013); Zhu et al. (2018) Rhouma et al. (2015); Barreto et al. (2013); Kwon and Hwang (2013b); De Persis and Tesi (2015); Liu et al. (2014c); Bezzo et al. (2014); Sajjad et al. (2015); Shoukry et al. (2015b); Xu and Zhu (2015); Shoukry et al. (2015a); Lee et al. (2015); Sanjab and Saad (2015)

Bobba et al. (2010), Kim and Poor (2011), Deka et al. (2014) and Hao et al. (2015) present greedy algorithms to select a subset of measurements to be protected. Besides secure sensor allocation, there are obviously several other protection-based approaches considered in the primary studies. For instance, to validate the correctness of customers' energy usage by detecting anomaly activities at the consumption level in the power distribution network, Lo and Ansari (2013) present *"a hybrid anomaly intrusion detection system framework, which incorporates power information and sensor placement along with grid-placed sensor algorithms using graph theory to provide network observability."* To reveal zero-dynamics attacks, Teixeira et al. (2012) provide necessary and sufficient conditions on modifications of the CPS's structure and presents an algorithm to deploy additional measurements to this end, while Bopardikar and Speranzon (2013) develop design strategies that can prevent or make stealth attacks difficult to be carried out; the proposed modifications of the legacy control system include optimal allocation of countermeasures and design of augmented system using a Moore-Penrose pseudo-inverse. Then, Mohsenian-Rad and Leon-Garcia (2011) discuss the defense mechanisms against static load altering attacks and presents a cost-efficient load protection design problem minimizing the cost of protection while ensuring that the remaining unprotected load cannot cause circuit overflow or any other major harm to the electric grid. For electricity market domain, Esmalifalak et al. (2013) use a two-person zero-sum game model to obtain an equilibrium solution in protecting different measurements against false data injection attacks impacting locational marginal price (LMP). Within the same domain, Ma et al. (2015) consider a multiact dynamic game where the attacker can jam a reduced number of signal channels carrying measurement information in order to manipulate the LMP creating an opportunity for gaining profit, and the defender is able to guarantee a limited number of channels in information delivery. Other protection-based approaches include, for instance *"intentionally switch on/off one of the selected transmission lines by turns, and therefore change the system topology"* (Wang and Ren, 2014); dynamically change the set of measurements considered in state estimation and the admittances of a set of lines in the topol-

ogy in a controlled fashion (Rahman et al., 2014), that is an application of a moving target defense (MTD) paradigm; use covert topological information by keeping the exact reactance of a set of transmission lines secret, possibly jointly with securing some meter measurements (Bi and Zhang, 2014); use an algebric criterion to reconfigure and partition a Jacobian matrix **H** into two sub-matrices, on each of which to perform a corresponding residual test (Talebi et al., 2010); use graph partition algorithms to decompose a power system into several subsystems, where false data do not have enough space to hide behind normal measurement errors (Wang et al., 2014); or even use voltage stability index (Chakravorty and Das, 2001) to identify nodes in power distribution networks with similar levels of vulnerabilities to false data injection attacks via a hybrid clustering algorithm (Anwar et al., 2015); *"employ a coding matrix to the original sensor outputs to increase the estimation residues, such that the alarm will be triggered by the detector even under intelligent data injection attacks"* (Miao et al., 2014), under the assumption that the attacker does not know the coding matrix yet. Finally, in order to detect and isolate the disconnected lines and recover the phase angles, in front of the joint cyber and physical attack (Soltan et al., 2015) outlined in Section 5.12. Soltan et al. (2015) present an algorithm that partitions the power grid into the minimum number of attack-resilient zones, ensuring the proposed online methods are guaranteed to succeed.

Moreover, nine over eleven **resilient controllers** and eight over ten **state estimators** presented in the primary studies and reported in Table 18 were already described in the end of Sections 5.10 and 5.8, respectively. The only works not discussed there are Bezzo et al. (2015), Mishra et al. (2014), and Shoukry et al. (2013). In Bezzo et al. (2015), an algorithm that leverages the theory of Markov decision processes was built to determine the optimal policy to plan the motion of unmanned vehicles and avoid unsafe regions of a state space despite the attacks on sensor measurements, when *"the system is fully observable and at least one measurement (however unknown) returns a correct estimate of a state"*. In Mishra et al. (2014), the state estimation was performed in a private and secure manner across multiple computing nodes (observers) with an approach inspired by techniques in cryptography, i.e. decoding Reed-Solomon codes, and results from estimation theory, such as Cramer-Rao lower bound, as a guarantee on the secrecy of the plant's state against corrupting observers. Finally, Shoukry et al. (2013) presented a minimax **state estimator and controller** design as a defense against packet scheduling attacks.

Always under the umbrella of prevention-based defense, there are 9 works presenting **security metrics**, such as *security indices* defined in the context of power networks as a minimum number of meters to perform an unobservable attack whether including [S004] or not [S002] a given meter, and ϵ-*stealthiness*, which is a notion that quantifies the difficulty to detect an attack when an arbitrary detection algorithm is implemented by the controller (Bai et al., 2015). A vulnerability measure for topologies of power grids subject to false data injection attacks based on incomplete information is presented by Rahman and Mohsenian-Rad (2012), while the vulnerability of the power system state estimator to attacks performed against the communication infrastructure is analyzed by Vuković et al. (2012) via security metrics that quantify the importance of individual substations and the cost of attacking individual measurements in terms of number of substations that have to be attacked. For the domain of electricity market, Jia et al. (2014) introduces the *average relative price perturbation* as a measure of a system-wide price perturbation resulting from a deception attack described in Section 5.12. In the context of canonical double-integrator-network (DIN) model of autonomous vehicle networks, to reflect the quality of the adversary's estimate of the desired nonrandom statistics Xue et al. (2014) defines *"the error covariance for a minimum-variance-unbiased estimate of the initial-condition vector as the* security level matrix" and considers its scalar measures as security levels characterizing the confidentiality of network's state. Kwon and Hwang (2013a) consider the *dynamic behavior cost* and *estimation error costs* to analytically test the behavior of unmanned aerial systems under various deception attacks and quantify their severity accordingly. Finally, for generic CPS described as linear time-invariant dynamical systems, Chen et al. (2015b) give a necessary and sufficient condition for the attacker to be undetectable in terms of the system dynamics eigenvectors, and provides an index that determines the minimum number of sensors that must be attacked in order for an attack to be undetectable and use this index to demonstrate a design guideline for improving the resilience of the system to sensor attacks.

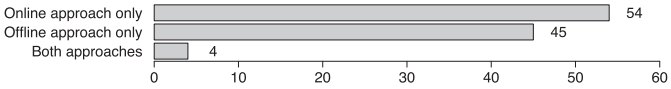


Fig. 24. Distribution between defense strategies.

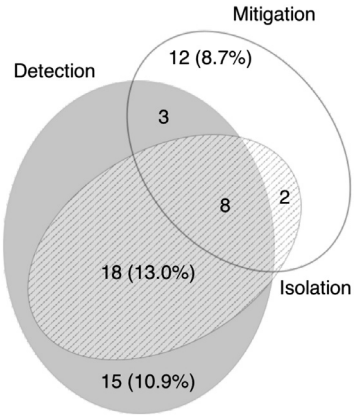


Fig. 25. Distribution by online defense strategy.

The distribution of primary studies between offline and online defense strategies is shown in Fig. 24, while the distribution of studies by online defense strategy is reported in Fig. 25.

The **online** approaches come into play after adversarial events happen (Zhu and Başar, 2015). *Detection* is an online approach in which the system is continuously monitored for anomalies caused by adversary actions (Teixeira et al., 2015), in order to decide whether an attack has occurred. Attack *isolation* is one step beyond attack detection, since it distinguishes between different types of attacks (Hwang et al., 2010), and requires also that the exact location(s) of the compromised components(s) be identified (Sou et al., 2014). Once an anomaly or attack is detected (and isolated), *mitigation* actions may be taken to disrupt and neutralize the attack, thus reducing its impact (Teixeira et al., 2015).

Among the 55 studies concerned with online defenses, 16 are focused on detection only, other 18 on detection and isolation, 3 on detection and mitigation, and 8 on detection, isolation and mitigation. There are 12 works studying mitigation only, and two works on isolation and mitigation, as reported in Table 19.

To contrast unidentifiable false data injection, Qin et al. (2013) present an algorithm to enumerate all feasible cases and proposes a mitigation strategy to minimize the average damage to the system. Another work on **isolation and mitigation** is Foroush and Martínez (2013), which introduces joint identification and control strategy, that renders the system asymptotically stable in front of unknown periodic DoS in form of pulse-width modulated jamming attacks.

Four of the works focused on **mitigation** were already described in previous Sections (i.e. Fawzi et al., 2014 in 5.8, Zhu et al., 2018; Kwon and Hwang, 2013b; Xu and Zhu, 2015 in 5.10). Here we spend some words on the remaining 8 studies. Lee et al. (2015) presents a secure and robust state estimation scheme that correctly estimates the states under sensor attacks by exploiting sensing redundancy. It guarantees a bounded estimation error despite measurement noises and process disturbances. Sanjab and Saad (2015) instead introduces a novel game-theoretic approach to analyze false data injections attacks that involve a smart grid defender and multiple adversaries, showing that at the equilibrium, multiple attacks can eliminate the effect of one another thus requiring no defense; however, under different conditions, a defense mechanism can be beneficial in reducing the combined effect of the different attacks on the system. Liu et al. (2014b) recalls their own study of strategies to be *"employed by a power system operator in the face of a switching attack to steer the system to a stable equilibrium through persistent co-switching and by leveraging the existence of a stable sliding mode"* (Liu et al., 2012). Zhu and Başar (2015) presents a cross-layer, hybrid dynamic game-theoretic model that captures the coupling between the cyber and the physical layers of the system dynamics, extending the control and defense strategy designs *"to incorporate post-event system states, where resilient control and cyber strategies are developed to deal with uncertainties and events that are not taken into account in pre-event robustness and security designs"* (Zhu and Başar, 2015). The overall optimal design of the cyber-physical system is characterized here by a Hamilton-Jacobi-Isaacs equation, together with a Shapley optimality criterion. Also Barreto et al. (2013) studies a game-theory problem (via differential games and heuristic stability games) where the actions of the players are the control signals each of them has access to. It focuses on reactive security mechanisms, which change the control actions in response to attacks. Another game-theoretic study is Liu et al. (2014c), in which the objective of the defender is to guarantee the dynamic performance of the NCS by transmitting signals with higher power levels than that of jammer's noisy signals. The cost function of the proposed two-player zero-sum stochastic game includes *"not only the resource costs used to conduct cyber-layer defense or attack actions, but also the dynamic performance (indexed by quadratic state errors) of the NCS"* (Liu et al., 2014c). Also Li et al. (2015b) present a two-player zero-sum game, to investigate the interactive decision-making process between a sensor node of a remote state estimator and an attacker who can launch DoS attacks. It uses a novel payoff function and strategies set, which take into account the energy constraints on both sides. To contrast the DoS attacks characterized by their frequency and duration, De Persis and Tesi (2015) determines suitable scheduling of the transmission times achieving input-to-state stability (ISS) of the closed-loop system. It considers periodic, event-based and self-triggering implementation of sampling logics, all of which adapt the sampling rate to the occurrence of DoS and, sometimes, to the closed-loop behavior.

The research line of Rhouma et al. (2015) comprises both mitigation and detection in separate papers. Specifically, in Rhouma et al. (2015) the generalized likelihood ratio test is designed to detect the termination of a zero dynamics attack and quickly recover the nominal behaviour of the linear quadratic Gaussian controller, while in Keller and Sauter (2013) a modified Kalman filter able to detect the zero-dynamic attack in absence of sensor or actuator faults is presented.

Regarding other **detection** mechanisms, most of all related works were already described in Section 5.9. Here we introduce only the remaining ones. Pasqualetti et al. (2013) characterizes fundamental monitoring limitations of descriptor systems from system-theoretic and graph-theoretic perspectives, and designs centralized and distributed monitors, which are complete, in the sense that they detect and identify every (detectable and identifiable) attack. To protect active sensing systems against physical attacks occurring in the analog domain, Shoukry et al. (2015a) introduced a physical challenge-response authentication scheme, that continually challenge the surrounding environment via random but deliberate physical probes. For a system equipped with multiple controllers/estimators/detectors, such that each combination of these components constitute a subsystem, Miao and Zhu (2014) presents a moving-horizon approach to solve a zero-sum hybrid stochastic game and obtain a saddle-point equilibrium policy for balancing the system's security overhead and control cost, since each subsystem has a probability to detect specific types of attacks with different control and detection costs. In the power systems domain, Hao et al. (2015) takes advantage of the sparse and low rank properties of the block measurements for a time interval to make use of robust PCA with element-wise constraints to improve both the error tolerance and the capability of detecting false data with partial observations.

The **detection and identification** of false data injection attacks on power transmission systems is considered by Davis et al. (2012), which outlines an "observe and perturb methodology" to compare the expected results of a control action with the observed response of the system, while Ozay et al. (2013) use a modified version of normalized residual test coupled with proposed state vector estimation methods against sparse attacks. Assuming the attack signal enters through the electro-mechanical swing dynamics of the synchronous generators in the grid as an unknown additive disturbance, Nudell et al. (Sept. 2015) divide the grid into coherent areas via *"phasor-based model reduction algorithm by which a dynamic equivalent of the clustered network can be identified in real-time"*, and localizes which area the attack may have entered using relevant information extracted from the phasor measurement data.

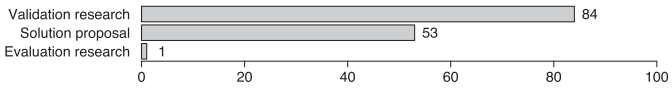


Fig. 26. Distribution of studies by research type.

6. Results - Validation Strategies (RQ3)

We determined the research type and related research methods of each primary study, simulation models, simulation test systems and experimental testbeds used, repeatability and availability of replication package. In the following we describe the main facts emerging from the collected data.

6.1. Research type and related research methods

Following the guidelines of systematic mapping studies, we reuse the classification of research approaches proposed by Wieringa et al. (2006), applying the research type classification presented in Petersen et al. (2015). Since our selection strategy (see Section 3.4) focuses on studies *proposing a method or technique* for CPS security, so the *philosophical papers, opinion papers* and *experience papers* are not considered in our study. The distribution of studies by research type is presented in Fig. 26, while the relative mapping is reported in Table 20.

Solution proposals for specific research problems, where the potential benefits and the applicability of a solution is simply shown through a small example or a line of argumentation, are given in 53 (i.e. 38.4% of all) studies. Those solutions are either novel or a significant extension of existing ones, and often correspond to the results of theoretical research.

Table 20
Research type.

Research type	Primary studies
Solution proposal	Bobba et al. (2010); Vrakopoulou et al. (2015); Teixeira et al. (2010); Huang et al. (2010); Li et al. (2015b); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2011); Tajer et al. (2011); Davis et al. (2012); Hug and Giampapa (2012); Liu et al. (2014a); Qin et al. (2013); Rawat and Bajracharya (2015) Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Ma et al. (2015); Amin et al. (2009); Zhu and Martínez (2014); Smith (2015); Zhu and Başar (2015); Teixeira et al. (2012); Xue et al. (2014); Foroush and Martínez (2013); Zhu et al. (2018); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Rhouma et al. (2015); Barreto et al. (2013); Chen et al. (2015a); Djouadi et al. (2015); Bai et al. (2015); Weimer et al. (2014); De Persis and Tesi (2015) Li et al. (2015c); Shoukry and Tabuada (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014); Sajjad et al. (2015); Qi et al. (2015); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Yuan and Mo (2015); Cetinkaya et al. (2015); Chen et al. (2015b); Tang et al. (2015); Kontouras et al. (2015); Lee et al. (2015)
Validation research	Liu et al. (2011); Kosut et al. (2011); Hendrickx et al. (2014); Pasqualetti et al. (2013); Esmalifalak et al. (2011); Hammad et al. (2015b,a); Liu et al. (2014b); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Mohsenian-Rad and Leon-Garcia (2011); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012) Wei and Kundur (2015); Ozay et al. (2013); Zonouz et al. (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Mishra et al. (2015a); Wang et al. (2014); Valenzuela et al. (2013); Lo and Ansari (2013); Sedghi and Jonckheere (2015); Yang et al. (2016); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b); Liang et al. (2014); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Manandhar et al. (2014); Tan et al. (2014); Amini et al. (2015); Kim et al. (2015); Yu and Chin (2015); Soltan et al. (2015); Liu et al. (2015a); Anwar et al. (2015); Chakhchoukh and Ishii (2015); Gu et al. (2015); Nudell et al. (Sept. 2015); Li et al. (2015a); Mo et al. (2015); Mo and Sinopoli (2012); Gupta et al. (2010); Sundaram et al. (2010); Cáardenas et al. (2011); Befekadu et al. (2015) Fawzi et al. (2014); Teixeira et al. (2015b); Kwon et al. (2014); Shoukry et al. (2013); D'Innocenzo et al. (2015); Kwon and Hwang (2013b); Miao and Zhu (2014); Mo and Sinopoli (2015); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Zhang et al. (2014); Liu et al. (2014c); Bezzo et al. (2014) Park et al. (2014); Miao et al. (2014); Mishra et al. (2014); Bezzo et al. (2015); Mishra et al. (2015b); Shoukry et al. (2015b); Xu and Zhu (2015); Zhang and Sankar (2015); Do et al. (2015); Shoukry et al. (2015a); Teixeira et al. (2015a); Tan et al. (2015); Sanjab and Saad (2015)
Evaluation research	Amin et al. (2010)

Validation research is applied in 84 studies (60.9%), where the techniques investigated are novel and have not yet been implemented in practice; the research methods used are formal mathematical proofs, case studies and lab experiments, together with simulations as a means for conducting an empirical study.

Finally, *evaluation research*, where the techniques are implemented in practice with identification of problems in industry, is done only in one study (Amin et al., 2010), in which the Gignac irrigation canal network is used to demonstrate the feasibility of stealthy deception attacks on water SCADA systems.

The mapping of the validation methods used by each primary study is documented in Table 21. Notably, formal *mathematical proofs* are employed in 75 studies (54.3%), while the remaining 63 works are using just the sound argument. Small numerical examples can be found in 79 works (57.2%), whilst simulation test systems, described in Section 6.3, are used to validate the presented results in 90 primary studies (65.2%).

Case studies via simulation, understood as empirical inquiries that draw on multiple sources of evidence to investigate contemporary phenomena in their real-life context, especially when the boundary between phenomenon and context cannot be clearly specified (Wohlin et al., 2012), are employed in 7 studies, as reported in Table 21. It is worth noting that in Bezzo et al. (2015) also a hardware evaluation on a remotely controlled flying quadricopter is performed, while the case study of D'Innocenzo et al. (2015) is extracted from its previous work cited therein (D'Innocenzo et al., 2013).

Experiments are formal, rigorous and controlled empirical investigations, where one factor or variable of the studied setting is manipulated, while all the other parameters are regulated at fixed levels (Wohlin et al., 2012). Among all the considered studies, there are only 7 works (5.1%) using *experimental testbeds*, namely *Gignac irrigation canal network* seen in Amin et al. (2010); *quadruple-tank process* (Johansson, 2000), that is a multivariable laboratory process consisting of four interconnected water tanks, used by Teixeira et al. (2015b); *LandShark*[10] robot, i.e. a fully electric unmanned ground vehicle developed by Black I Robotics, adopted in 3 works (Tiwari et al., 2014; Pajic et al., 2015)[11], Bezzo et al. (2014); ad-hoc testbed consisting of sensors attached to a Mazda Rx7 tone ring, which in turn is attached to a DC motor simulating a rotating wheel, used as a platform for testing security of magnetic encoder[12] against active spoofing attacks in Shoukry et al. (2015a); *micro grid* experimental testbed consisting of three Siemens SENTRON PAC4200 smart meters connected into the network with YanHua Industry control machine, which is used to monitor all traffic of lab network and read the data from all meters, employed in Mishra et al. (2015a).

This data indicates that experimental testbed used by researchers on CPS security (with ties to Automatic Control community) are still too few, and the validation of the proposed solutions requires major attention. We believe that there is a pressing need for implementation and adoption of testbeds with different capabilities for extensive experimental verifications of proposed solutions.

6.2. Simulation model

As in the case of plant models used by attackers, also the plant models adopted for simulation purposes can be different from the plant models used in the analysis. As we can see from Fig. 27, an overwhelming majority of primary studies uses the same model of plant for both the analysis and simulation, while only in 6 studies (4.3%) these models are different (Kim and Tong, 2013; Wang et al., 2014; Kim et al., 2015; Chakhchoukh and Ishii, 2015; Jia et al., 2014; Kim et al., 2014b). Those six studies are

[10] http://www.blackirobotics.com/LandShark_UGV_UC0M.html.

[11] The LandShark is used in Pajic et al. (2014), which belongs to the research line of Pajic et al. (2015).

[12] It relies on magnetic variations to measure the angular velocity of a gear or wheel.

Table 21
Validation methods.

Validation method	Primary studies
Sound argument	Bobba et al. (2010); Vrakopoulou et al. (2015); Huang et al. (2010); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2011); Esmalifalak et al. (2011); Hammad et al. (2015b,a); Tajer et al. (2011); Mohsenian-Rad and Leon-Garcia (2011); Davis et al. (2012); Hug and Giampapa (2012); Wei and Kundur (2015); Ozay et al. (2013); Zonouz et al. (2012) Wang et al. (2014); Valenzuela et al. (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016); Qin et al. (2013); Li (2014); Liang et al. (2014); Yamaguchi et al. (2014); Rahman et al. (2014); Manandhar et al. (2014); Amini et al. (2015); Liu et al. (2015a); Rawat and Bajracharya (2015); Anwar et al. (2015); Chakhchoukh and Ishii (2015); Gu et al. (2015); Nudell et al. (Sept. 2015); Li et al. (2015a); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Ma et al. (2015); Amin et al. (2009) Cáardenas et al. (2011); Zhu and Martínez (2014); Smith (2015); Zhu and Başar (2015); Kwon and Hwang (2013a); Barreto et al. (2013); Tiwari et al. (2014); Djouadi et al. (2015); Liu et al. (2014c); Park et al. (2014); Shoukry and Tabuada (2014); Jones et al. (2014) Bezzo et al. (2015); Yuan and Mo (2015); Zhang and Sankar (2015); Do et al. (2015); Shoukry et al. (2015a,a); Tan et al. (2015)
Mathematical proof	Liu et al. (2011); Kosut et al. (2011); Hendrickx et al. (2014); Teixeira et al. (2010); Li et al. (2015b); Pasqualetti et al. (2013); Liu et al. (2014b); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012) Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Mishra et al. (2015a); Lo and Ansari (2013); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b); Hao et al. (2015); Tan et al. (2014); Kim et al. (2015); Yu and Chin (2015); Soltan et al. (2015) Mo et al. (2015); Mo and Sinopoli (2012); Amin et al. (2010); Gupta et al. (2010); Sundaram et al. (2010); Befekadu et al. (2015); Fawzi et al. (2014); Teixeira et al. (2015b); Kwon et al. (2014); Teixeira et al. (2012); Xue et al. (2014); Foroush and Martínez (2013); Zhu et al. (2018); Shoukry et al. (2013); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Rhouma et al. (2015); Kwon and Hwang (2013b); Miao and Zhu (2014); Chen et al. (2015a); Mo and Sinopoli (2015); Eyisi and Koutsoukos (2014); Pajic et al. (2015) Bai et al. (2015); Weimer et al. (2014); De Persis and Tesi (2015); Zhang et al. (2014); Bezzo et al. (2014); Li et al. (2015c); Miao et al. (2014); Mishra et al. (2014); Weerakkody and Sinopoli (2015); Sajjad et al. (2015); Mishra et al. (2015b); Shoukry et al. (2015b); Qi et al. (2015); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Cetinkaya et al. (2015); Xu and Zhu (2015); Chen et al. (2015b) Tang et al. (2015); Kontouras et al. (2015); Lee et al. (2015); Sanjab and Saad (2015)
Example	Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Vrakopoulou et al. (2015); Teixeira et al. (2010); Huang et al. (2010); Li et al. (2015b); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2013, 2011); Giani et al. (2013); Yang et al. (2014); Davis et al. (2012); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012); Kim and Tong (2013); Vuković and Dán (2014); Lo and Ansari (2013); Liu et al. (2014a) Qin et al. (2013); Kim et al. (2014a); Deka et al. (2014, 2015a); Wang and Ren (2014); Amini et al. (2015); Rawat and Bajracharya (2015); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Ma et al. (2015); Mo et al. (2015); Mo and Sinopoli (2012); Gupta et al. (2010); Zhu and Martínez (2014); Smith (2015); Fawzi et al. (2014); Zhu and Başar (2015); Teixeira et al. (2015b) Teixeira et al. (2012); Foroush and Martínez (2013, 2013); Shoukry et al. (2013); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Rhouma et al. (2015); Bopardikar and Speranzon (2013); Barreto et al. (2013); Kwon and Hwang (2013b); Miao and Zhu (2014); Chen et al. (2015a); Mo and Sinopoli (2015); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Djouadi et al. (2015); Bai et al. (2015); Weimer et al. (2014); De Persis and Tesi (2015); Zhang et al. (2014); Li et al. (2015c); Miao et al. (2014); Shoukry and Tabuada (2014); Weerakkody and Sinopoli (2015); Jones et al. (2014) Sajjad et al. (2015); Shoukry et al. (2015b); Qi et al. (2015); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Cetinkaya et al. (2015); Chen et al. (2015b); Tang et al. (2015); Do et al. (2015); Kontouras et al. (2015); Teixeira et al. (2015a); Lee et al. (2015)
Case study	Zonouz et al. (2012); Kwon et al. (2014); D'Innocenzo et al. (2015); Bezzo et al. (2015); Xu and Zhu (2015); Shoukry et al. (2015a); Tan et al. (2015)
Experiment	Liu et al. (2015a); Amin et al. (2010); Teixeira et al. (2015b); Tiwari et al. (2014); Pajic et al. (2015); Bezzo et al. (2014); Shoukry et al. (2015a)
Simulation	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Vrakopoulou et al. (2015); Teixeira et al. (2010); Huang et al. (2010); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2013, 2011); Esmalifalak et al. (2011); Hammad et al. (2015b,a); Liu et al. (2014b); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Mohsenian-Rad and Leon-Garcia (2011); Davis et al. (2012); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012); Wei and Kundur (2015); Ozay et al. (2013); Zonouz et al. (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Mishra et al. (2015a); Wang et al. (2014); Valenzuela et al. (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016); Qin et al. (2013); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b); Liang et al. (2014); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Manandhar et al. (2014); Tan et al. (2014); Amini et al. (2015); Kim et al. (2015); Yu and Chin (2015); Soltan et al. (2015); Liu et al. (2015a); Rawat and Bajracharya (2015); Anwar et al. (2015); Chakhchoukh and Ishii (2015); Gu et al. (2015); Nudell et al. (Sept. 2015); Li et al. (2015a); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Kim et al. (2014b); Ma et al. (2015); Mo et al. (2015); Amin et al. (2010) Cáardenas et al. (2011); Smith (2015); Fawzi et al. (2014); Kwon et al. (2014); Foroush and Martínez (2013); Shoukry et al. (2013); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Barreto et al. (2013); Kwon and Hwang (2013b); Miao and Zhu (2014); Chen et al. (2015a); Eyisi and Koutsoukos (2014); Djouadi et al. (2015); De Persis and Tesi (2015) Liu et al. (2014c); Bezzo et al. (2014); Park et al. (2014); Shoukry and Tabuada (2014); Jones et al. (2014); Shoukry et al. (2015b); Xu and Zhu (2015); Zhang and Sankar (2015); Tan et al. (2015); Sanjab and Saad (2015)

Table 22
MATPOWER test cases.

MATPOWER test case	Primary studies
IEEE 4-bus	Huang et al. (2010); Esmalifalak et al. (2011); Tan et al. (2015)
PJM 5-bus system	Jia et al. (2014); Esmalifalak et al. (2013); Ma et al. (2015)
IEEE 9-bus	Liu et al. (2011); Bobba et al. (2010); Yang et al. (2014); Talebi et al. (2010); Ozay et al. (2013); Yamaguchi et al. (2014); Hao et al. (2015); Manandhar et al. (2014); Rawat and Bajracharya (2015)
WSCC 9 bus	Pasqualetti et al. (2013); Davis et al. (2012); Amini et al. (2015); Sanjab and Saad (2015)
IEEE 14-bus	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Yuan et al. (2012); Pasqualetti et al. (2013); Esmalifalak et al. (2011); Yang et al. (2014); Bi and Zhang (2014); Davis et al. (2012); Sou et al. (2014); Ozay et al. (2013) Kim and Tong (2013); Wang et al. (2014); Sedghi and Jonckheere (2015); Yang et al. (2016); Qin et al. (2013); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Li (2014); Wang and Ren (2014); Liu et al. (2015b); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Tan et al. (2014) Kim et al. (2015); Yu and Chin (2015); Soltan et al. (2015); Liu et al. (2015a); Chakhchoukh and Ishii (2015); Gu et al. (2015); Li et al. (2015a); Xie et al. (2011); Jia et al. (2014); Choi and Xie (2013); Kim et al. (2014b); Fawzi et al. (2014)
IEEE 24-bus RTS/RTS-79/RTS-96	Pasqualetti et al. (2013); Giani et al. (2013); Mohsenian-Rad and Leon-Garcia (2011); Davis et al. (2012); Zonouz et al. (2012); Valenzuela et al. (2013); Liu et al. (2015b); Liang et al. (2014); Zhang and Sankar (2015)
IEEE 30-bus	Liu et al. (2011); Bobba et al. (2010); Kim and Poor (2011); Esmalifalak et al. (2011); Giani et al. (2013); Yang et al. (2014); Talebi et al. (2010); Ozay et al. (2013); Sedghi and Jonckheere (2015); Yang et al. (2016) Deka et al. (2014, 2015a); Liu et al. (2015b); Yamaguchi et al. (2014); Rahman et al. (2014); Soltan et al. (2015); Chakhchoukh and Ishii (2015); Esmalifalak et al. (2012)
39-bus New England system	Hammad et al. (2015b,a); Liu et al. (2014b); Giani et al. (2013); Wei and Kundur (2015); Ozay et al. (2013); Wang et al. (2014); Sanandaji et al. (2014); Liu et al. (2015b,a); Nudell et al. (Sept. 2015)
IEEE 57-bus	Hendrickx et al. (2014); Kim and Poor (2011); Giani et al. (2013); Bi and Zhang (2014); Hug and Giampapa (2012); Ozay et al. (2013); Mishra et al. (2015a); Liu et al. (2014a); Deka et al. (2014, 2015a, 2015b) Liu et al. (2015b); Hao et al. (2015); Rahman et al. (2014)
IEEE 118-bus	Liu et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Vrakopoulou et al. (2015); Kim and Poor (2011); Pasqualetti et al. (2013, 2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Vuković et al. (2012); Ozay et al. (2013) Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Wang et al. (2014); Valenzuela et al. (2013); Liu et al. (2014a); Yang et al. (2016); Kim et al. (2014a); Deka et al. (2014); Li (2014); Liu et al. (2015b) Yamaguchi et al. (2014); Rahman et al. (2014); Kim et al. (2015); Soltan et al. (2015); Liu et al. (2015a); Jia et al. (2014); Tan et al. (2015)
IEEE 300-bus	Liu et al. (2011); Bobba et al. (2010); Kim and Poor (2011); Giani et al. (2013); Yang et al. (2014); Vuković et al. (2012); Ozay et al. (2013); Kim and Tong (2013); Wang et al. (2014); Yamaguchi et al. (2014) Rahman et al. (2014); Yu and Chin (2015); Soltan et al. (2015)
Polish system (2383|...|3375)-bus	Hendrickx et al. (2014); Giani et al. (2013); Ozay et al. (2013); Liu et al. (2014a, 2015b); Yamaguchi et al. (2014); Soltan et al. (2015)
33-bus|69-bus RTS	Anwar et al. (2015)

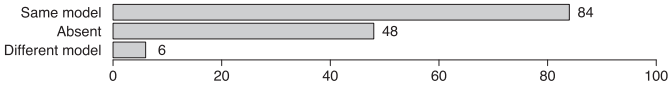


Fig. 27. Distribution of primary studies by simulation model.

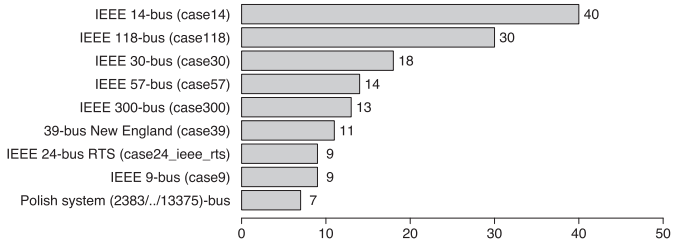


Fig. 28. Distribution of power grid test cases.

within the power transmission or electricity market application domains and use nonlinear AC model for simulation, while consider a DC model (sometimes together with AC model) for analysis purposes. It is worth to mention that in 48 primary studies (34.8%) there are no simulations. Those works account for those solution proposals and validation research papers already introduced in Subsection 6.1 that use only good line of argumentation, formal mathematical proofs and illustrative numerical examples as the research methods. The only exception is Tiwari et al. (2014), which uses LandShark robot as the experimental testbed, without relying on simulations.

6.3. Simulation test system

As it was anticipated in the previous section, 90 primary studies (65.2%) use simulation test systems to validate the presented results. The mapping of each study to the adopted simulation test system is reported in Tables 22 and 23.

The main tool used by researchers on security of smart grid is MATPOWER, which is an open-source Matlab-based power system simulation package (Zimmerman et al., 2011). The distribution of its test cases (Zimmerman and Murillo-Sánchez, 2016) is shown in Fig. 28.

From Table 22 it is evident that the works studying applications to electricity market (see Table 3) use only small MATPOWER test cases, namely a modified 5-bus PJM example case (case5), a 4-bus example case from Grainger & Stevenson[13] (case4gs), IEEE 14-bus case (case14), IEEE 30-bus case (case_ieee30) and its variants, 39-bus New England case (case39), IEEE 118-bus case (case118), IEEE 300-bus case (case300), and an implementation of WSCC 9-bus (Sauer and Pai, 1997) case.

Generally speaking, the most used MATPOWER test cases are the small ones, IEEE 14-bus case and IEEE 118-bus case, used through all the considered power grid domains, while the bigger Polish sys-

[13] In some works it is referred to as IEEE 4-bus.

Table 23
Primary studies adopting simulation testbeds different from MATPOWER.

Various testbes	Vrakopoulou et al. (2015); Hammad et al. (2015b); Nudell et al. (Sept. 2015); Mo et al. (2015); Amin et al. (2010); Cáardenas et al. (2011); Smith (2015); Kwon et al. (2014); Shoukry et al. (2013); D'Innocenzo et al. (2015); Kwon and Hwang (2013a,b); Miao and Zhu (2014) Eyisi and Koutsoukos (2014); Liu et al. (2014c); Bezzo et al. (2014); Park et al. (2014); Shoukry and Tabuada (2014); Jones et al. (2014); Shoukry et al. (2015b); Xu and Zhu (2015)

tem test cases (such as case3375wp) found their way just in 7 works, all in the power transmission domain.

The primary studies that are using testbeds different from MATPOWER are listed in Table 23. Two-area Kundur system test case (Kundur, 1994), whose parameters can be found in Matlab Power System Toolbox (Chow and Cheung, 1992), is used to study power generation in [S005, S014, S064]. Other typical test cases implemented in Matlab include an irrigation system consisting of a cascade of a number of canal pools, as presented in Amin et al. (2013), which is used in Amin et al. (2010); Smith (2015); an unstable batch reactor system presented by Walsh et al. (2002), which is a fourth order unstable linear system with two inputs, employed in Shoukry et al. (2013); Miao and Zhu (2014); Tennessee Eastman process control system model and associated multi-loop proportional-integral control law, as proposed by Ricker (1993), that is adopted in Mo et al. (2015); Cáardenas et al. (2011); Miao and Zhu (2014); PHANToM Premium 1.5A (Taati et al., 2008), that is a haptic device from SensAble Technologies, used in a simulation setup in Liu et al. (2014c); finally, a rotorcraft in a cruise flight (Narendra and Tripathi, 1973) is simulated in Kwon and Hwang (2013a,b).

The remaining primary studies listed in Table 23 use ad hoc simulation test cases to validate their results. Specifically, Kwon et al. (2014) use Monte Carlo simulation with 1000 runs on an unmanned aerial system navigation system integrating the inertial navigation system and the global positioning system implemented in Matlab. D'Innocenzo et al. (2015) perform Matlab/Simulink simulations on the multi-hop wireless network deployed in a room to connect the temperature sensor to the variable-air-volume box, which is positioned nearby the room. Also Eyisi and Koutsoukos (2014) perform Matlab/Simulink simulations on a single-input single-output (SISO) system; it deals with a velocity control of a single joint robotic arm over a communication network. Bezzo et al. (2014) use robot operating system[14] (ROS) based simulator emulating electromechanical and dynamical behavior of the real robot. In Park et al. (2014) simulations are carried out using a simple model of air traffic operations. Shoukry and Tabuada (2014) use an UGV model implemented in Matlab. Jones et al. (2014) simulate a train, which uses an electronically-controlled pneumatic braking system modeled as a classical hybrid automaton. In the research line of Shoukry et al. (2015b), the authors developed a *"theory solver in Matlab and interfaced it with the pseudo-Boolean SAT solver SAT4J"* (Shoukry et al., 2015), where the simulations are performed on linear dynamical systems with a variable number of sensors and system states. Finally, Xu and Zhu [S128] perform Matlab/Simulink simulations on a small-scale unmanned helicopter whose dynamic model is linearized at its hovering point (Cai et al., 2011).

From the analysed data it is evident that most of the works still use relatively small simulation test cases to validate the proposed results, while more challenging examples can be found only in the power networks application domain, with some simulations performed on MATPOWER Polish system test cases. Despite research on CPS security in this domain appears quite mature, a benchmark is still missing.

[14] http://www.ros.org.

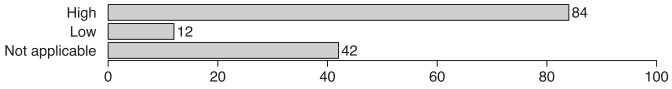


Fig. 29. Distribution of primary studies by repeatability.

6.4. Repeatability and availability of replication package

The possibility of reproducing the evaluation or validation results provided by the authors is called repeatability, while the possibility of exploring changes to experiment parameters is known as workability. The repeatability process is a good scientific practice (Bonnet et al., 2011). The so called Artifact Evaluation Process[15] is used in a number of conferences in computer science, and a similar concept of repeatability evaluation of computational elements has been introduced in cyber-physical systems domain in 2014 ACM Hybrid Systems Computation and Control (HSCC) conference[16]. However, such practice is rather new to research communities adopting automatic control perspective on security of CPS: we found no primary study with a replication package. Thus, we have isolated the information concerning the availability of a replication package and extended the simple dimension provided in Yuan et al. (2014) in a way that *repeatability* is considered *high* when the authors provide enough details about (i) the steps performed for evaluating or validating the study, (ii) the developed or used software, (iii) the used or simulated testbed, if any, and (iv) any other additional resource, in a way that interested third parties can be able to repeat the evaluation or validation of the study. Otherwise, we have *low* repeatability.

Such high-level definition of repeatability values has ensured that the primary studies using standard test systems from Section 6.3 and well known experimental testbeds have received high values of repeatability, where steps performed in their experiments, case studies and/or simulation examples have been described with enough details. On the other hand, the usage of some ad hoc simulation test system has caused some low values of repeatability assigned. As shown in Fig. 29, 84 studies (60.9%) have a high repeatability value, and 12 studies (8.7%) have a low repeatability score. As a note, we did not have the possibility to evaluate the repeatability of 42 studies (30.4%) since they do not present any experiment, case study or simulation example. Overall, we advocate the improving of repeatability and workability of computational results of the papers by adopting the best practices of repeatability process and creating related replication packages, because we strongly believe in the usefulness of repeatability to empower others to build on top of the contributions of a paper[17] and thus accelerate scientific and technological progress.

7. Implications for future research

We discussed potential future research trends and challenges for CPS security from automatic control perspective throughout this paper in the context of the various discussions of results ob-

[15] http://www.artifact-eval.org.
[16] http://www.cs.ox.ac.uk/conferences/hscc2016/re.html.
[17] http://evaluate.inf.usi.ch/artifacts/aea.

tained in our systematic mapping study of the first ten years of the field (Sections 4, 5, and 6); in the following we present how research on security in cyber-physical realm has evolved since 2016 and provide more general observations about implications for future research.

First of all, CPS security is a relatively young research domain that is experiencing a strong academic (and industrial) interest in the very few years, as seen from the publication trend reported in Fig. 2, and both European Commission and NSF are very oriented in financing research in this area. From the data obtained in the systematic mapping part of our study it can be inferred that the potential of the developed results and methodologies in addressing realistic emerging problems in several application domains (first of all, power systems) is very promising. As a consequence it is predictable that CPS security will be a "hot topic" for the forthcoming years.

Based on the informal analysis of several notable works available in literature from 2016 to mid 2018, we can affirm that the increasing trend did not stop. In fact, also if we consider CPS dealing with cyber attacks with a generic dynamical systems modeling framework only, a huge amount of works can be found, as for example (Weerakkody et al., 2016; Bai et al., 2017a; Chen et al., 2018b; Pajic et al., 2017b; Ding et al., 2017b; 2017a; Zheng et al., 2016; Yuan et al., 2016; Mo and Sinopoli, 2016; Chen et al., 2017b; Jin et al., 2017; Kung et al., 2017), just to cite a few. Another large amount of works can be found if we only focus our attention on attack detection and identification, and state estimation (Nakahira and Mo, 2018; Mo and Garone, 2016; Weerakkody et al., 2017; Bai et al., 2017b; Mishra et al., 2017; Murguia and Ruths, 2016; Li et al., 2017c; 2017d; Chen et al., 2017a; Shi et al., 2017; Shoukry et al., 2018; 2017; Pajic et al., 2017a; Shoukry and Tabuada, 2016; Weerakkody and Sinopoli, 2016; Ao et al., 2018; Lee et al., 2018; Forti et al., 2018; Kim et al., 2018). It is worth to emphasize that one of the path followed by researcher to improve the research in CPS security consists on considering more accurate, but also more complex, models such as stochastic, nonlinear and delayed systems (Ding et al., 2018b; Hu et al., 2016; Liu et al., 2016a; Wang et al., 2017). We should also note that some of the aforementioned works are extensions of the research lines considered by our systematic mapping, since Bai et al. (2017a); Mishra et al. (2017); Shoukry and Tabuada (2016); Lee et al. (2018) are clearly related to Bai et al. (2015); Mishra et al. (2015b); Shoukry and Tabuada (2014); Lee et al. (2015), respectively, while both Pajic et al. (2017b,a) are linked to Pajic et al. (2015), and Shoukry et al. (2018, 2017) are associated with [S122].

From a modeling point of view, while Gaussian model of noise (used e.g. in Weerakkody et al., 2016; Bai et al., 2017a; Chen et al., 2018b; Ding et al., 2017b; Ding et al., 2017a; Zheng et al., 2016; Mo and Sinopoli, 2016; Chen et al., 2017b; Kung et al., 2017; Mo and Garone, 2016; Bai et al., 2017b; Mishra et al., 2017; Murguia and Ruths, 2016; Li et al., 2017c; Li et al., 2017d; Shi et al., 2017; Weerakkody and Sinopoli, 2016; Forti et al., 2018; Ding et al., 2018b; Hu et al., 2016; Liu et al., 2016a; Wang et al., 2017) still clearly dominates the scene, the bounded model (found in Pajic et al., 2017b; Nakahira and Mo, 2018; Shoukry et al., 2018; Shoukry et al., 2017; Pajic et al., 2017a; Lee et al., 2018; Kim et al., 2018) is considered more and more often. This fact indicates an increasing attention to the aspects of robustness of the proposed solutions, and that the model-based methods and techniques for enforcing security in the cyber-physical domain are acquiring certain maturity.

Another confirmation concerns a cornerstone application of the CPS security: power grids. Indeed, due to the integration of information technology and the vulnerability of communication networks, power grids are extremely exposed to cyber-attacks. Thus researchers are still very involved in this context, see for example Wei et al. (2018); Zhang et al. (2017); Li et al. (2017e); Yang et al. (2017a); Rahman et al. (2017); Ashok et al. (2017); Farraj et al. (2016); Anwar et al. (2017); Ao et al. (2016); Liu et al. (2016b); Sanjab and Saad (2016); Esnaola et al. (2016); Srikantha and Kundur (2016); Liu and Li (2017b); Zhang and Sankar (2016); Liu et al. (2017); Taha et al. (2018); Ye et al. (2016); Giraldo et al. (2017a); Isozaki et al. (2016); Li et al. (2016b); Lin et al. (2018a); Liu and Li (2017c); Zhao et al. (2017b); Deng et al. (2017a); Ashok et al. (2018); Yang et al. (2017b); Chen et al. (2018a); Yang et al. (2017b); Bretas et al. (2017); Attia et al. (2018); Amini et al. (2018), and many others. These works mainly consider IEEE bus systems as testbeds to simulate the methodology they propose. Much less works consider different testbeds, such as a hybrid automaton model of DC microgrids (Beg et al., 2017), or simulators built by the authors, like the MASSIM (Gai et al., 2017) (that unfortunately at the moment is not publicly available for independent use or just replication purposes) and the PowerWorld (Li et al., 2016a; 2017a). Also novel algorithms that are validated by experiments on a physical system, as the case of the 16-bus power system testbed in Tan et al. (2017), are still rare. This fact highlights a significant need to evaluate new concepts and vulnerabilities by experimental facilities, as those surveyed by Cintuglu et al. (2017). The theoretical research on security of power grids is expanding in several directions, such as considering the consequences of false data injection attacks on an AC state estimation, by analyzing the results of a DC-based optimization problem (Liang et al., 2016), or dealing with reduced amount of information available to an attacker when constructing an undetectable attack vector (Liu and Li, 2017a; Chin et al., 2017). Also Markovian models to represent the power system and the attack has been under investigation in the last years, as in the case of Huang et al. (2016); Karimipour and Dinavahi (2018); Xiang et al. (2017). Other researchers are exploring completely different approaches, such as consensus (Zhao et al., 2017a), and considering specific categories of attacks, as part of the larger class of deception attacks, like coordinated cyber-physical attacks (CCPAs) (Deng et al., 2017c), and control-related attacks (Lin et al., 2018b). Notably, some of the named works on smart grid security are the follow up of the research lines already seen in our systematic mapping: for instance, Sanjab and Saad (2016); Amini et al. (2018); Huang et al. (2016) are the journal versions of the respective conference works (Sanjab and Saad, 2015; Amini et al., 2015; Huang et al., 2010).

An increasing trend, with respect to the period 2006–2015, can be seen in networked CPSs (Satchidanandan and Kumar, 2017; Ding et al., 2016; Zhang et al., 2016; Sun et al., 2018; Teixeira et al., 2017). Several aspects have been investigated on this topic, with paper focusing on stability (De Persis and Tesi, 2016; Feng and Tesi, 2017; Dolk et al., 2017; Pang et al., 2018), state estimation (Tsiamis et al., 2017; Miao et al., 2017; Keller et al., 2016; Guo et al., 2018; 2017), and output tracking control (Pang et al., 2016). Also in this case, one of the research directions is taking into account more complex models, such as Markovian models, addressing stability and state estimation problems (Cetinkaya et al., 2017; 2018; Ding et al., 2017c; Zhang et al., 2018). Furthermore, although we would have excluded papers on sensor networks due to our selection criteria, it is worth to mention few papers to underline that CPS security with focus on wireless sensor networks is an active research area (Li et al., 2017b; 2018; Ma et al., 2017). The same also applies to works on consensus (Senejohnny et al., 2017; Zhao et al., 2017a). Also here several results from research lines presented in our systematic mapping are spread through new publications, with e.g. Keller et al. (2016); Cetinkaya et al. (2017) following Rhouma et al. (2015); Cetinkaya et al. (2015), respectively, and Ding et al. (2017c); Li et al. (2017b) both linked to Li et al. (2015b).

Differently from networked control systems, CPS security with unmanned aerial vehicle applications did not explode until now,

despite some good papers can be found in literature (Chen et al., 2016; Abbaspour et al., 2016). This is true also for works that focus specifically on industrial control systems (Garcia et al., 2017; Urbina et al., 2016b; Paridari et al., 2018; Huang et al., 2018), also proposing a testbed to understand the impact of cyber and physical attacks on a particular type of industrial control systems, i.e. water treatment system (Adepu and Mathur, 2016; Mathur and Tippenhauer, 2016), on cryptography for CPS, which has been further investigated in recent years considering for example both fully and semi-homomorphic encryption techniques for secuirity of CPS (Kim et al., 2016; Farokhi et al., 2017), and on applications of formal methods to reason about CPS and cyber-physical attacks (Lanotte et al., 2017).

Novel directions have also started, exploring different fields other than the ones described in this paper. In particular, security in teleoperated robotics rised up too, addresing vulnerability issues against different type of cyber attacks, as for example static malignant content modification attacks (MCoMA) (Dong et al., 2016), or focusing on experimental analysis on specific systems, as for the advanced teleoperated robotic surgery system considered in Bonaci et al. (2015), although its journal version is still in preparation.

A very interesting aspect that came up analyzing papers of the last years is the increasing consideration of data-driven methods. Indeed, all the approaches described above can be affected by issues that are not always considered during the definition of the modeling framework. For example, it can be difficult, in general, to know a priori what type of attacks may be inserted into the system, moreover it can also be difficult to derive a mathematical description of the system that is based on the physics when the system is extremely complex. As experience demonstrates, e.g. in the context of energy efficient control of building automation systems (Smarra et al., 2018), in many CPS application domains the cost of modeling is much larger than the improvement margin in terms of efficiency/cost/performance. In this scenario, the data-driven approaches introduce an important novelty. In the last years, this topic attracted researcher's interest, and few papers are available in different domains, as for example anomaly detection for CPSs (Shi et al., 2018), detection of cyber attacks against vehicles (Loukas et al., 2018), attack detection on unmanned aerial vehicles (Abbaspour et al., 2016) and smart grids (Ozay et al., 2016).

In the future data-driven methods will play a key role to improve the modeling framework of CPSs and attacks, and to help the system to correct itself based on the data generated on-line by the system, leveraging the learning potential of the machine learning. Coupled with classical modeling techniques they could also be used to come up with an unified paradigm to address CPS security.

8. Related work

Recently, we have seen a large increase in the surveys of CPS focusing exclusively on security and/or privacy from different points of view, and a recent survey by Giraldo et al. (2017b) has provided a useful overview of 32 papers (including the early preliminary version of this work) categorized by application domains (such as smart grids (He and Yan, 2016; Cintuglu et al., 2017), medical devices (Rushanan et al., 2014; Camara et al., 2015; AlTawy and Youssef, 2016), industrial control systems (Stouffer et al., 2015b; McLaughlin et al., 2016; Urbina et al., 2016a), manufacturing (Wells et al., 2014; Pan et al., 2017; Zeltmann et al., 2016), and intelligent transportation systems), the addressed attacks and defences, research trends, network security, security-level implementation, and computational strategies. Notably, among all 32 works analysed by Giraldo et al. (2017b), there was only one other systematic study, developed by Nguyen et al. (2017), which had a very different scope from ours, with a very specialized focus on model-based security engineering. Nguyen et al. (2017) employed the same commonly accepted guidelines reported in Petersen et al. (2015) and Kitchenham and Charters (2007) to show how software models can help in design and verification of CPS.

Later on, two new surveys on false data injection attacks on state estimation in power systems, both summarising the theoretical basis of such attacks, their impact in case of success and the defence strategies against them, were conducted by Deng et al. (2017b) and Liang et al. (2017).

Before them, the cyber-physical systems security within the smart grid domain has been reviewed by Mo et al. (2012) and by Sridhar et al. (2012).

The work from Mo et al. (2012) is a good starting point to face the area of CPS security since it gives a broad overview on cyber and system-theoretic approaches to security and shows how a combination of both of them together can provide better security level than traditional methods. The provided example describes defense against replay attack following secure control (Cárdenas et al., 2008b) method.

The article from Sridhar et al. (2012) is more domain-specific. Since power system is functionally divided into generation, transmission, and distribution, the survey considers cyber vulnerabilities and security solutions for each of the underlying fields. Notably, it deals with a wide range of (sophisticated) attacks, some bad data detection techniques and mentions attack resilient control. This work provides also an overview on supporting infrastructure security, with a look on secure communication, device security, security management and awareness, cyber security evaluation, and intrusion tolerance. All in all, the paper identifies the importance of combining both power application security and supporting infrastructure security into the risk assessment process and provides a methodology for impact evaluation. Conclusively, it lists a number of emerging research challenges in risk modeling and mitigation, pointing out the importance of attack resilient control, domain-specific anomaly detection and intrusion tolerance.

Lastly, Ding et al. (2018a) surveyed the recent advances on security control and attack detection for industrial CPS from a control theory perspective, rising some challenging issues for the future research.

Finally, we should observe that based on the guidelines for performing systematic literature reviews from Kitchenham and Charters (2007), all but Nguyen et al. (2017) the aforementioned articles cannot be considered as a systematic literature reviews but as *informal literature surveys*, and cannot be compared directly to this mapping study.

9. Conclusions and future work

In this work we provided an overview of the state of the art of research in CPS security enforcing or breaching, considering an automatic control perspective. The presented survey is based on a well-established empirical methodology, called systematic mapping, which allowed us to provide a review that is complete, comprehensive, and not biased from personal experience.

The main contribution of this paper is a systematic map that covers the first ten years of research on cyber-physical security. It provides a statistical summary of important features in the field, such as targeted applications and system components, adopted strategies and validation of results, together with emerging publication trends. The obtained results permit to find a clear picture of the sate-of-the-art of a topic of interest, as for example deception attacks on state estimation in power grids, while remaining aware of a broader picture on the works with similar characteristics, as for instance deception attacks on state estimation of a generic cyber-physical system.

Starting from these results, that systematically cover the evolution of the topic from its beginning, we analyzed the relevant works on cyber-physical security published from 2016 to mid 2018. This allowed us to show, through empirical evidence, that investigation of cyber-physical security enforcing or breaching is indeed a very active and expanding area of research, and emphasize how the topic evolved, thus providing hints on the weak points and promising new directions of this appealing research area.

We believe that this study may inspire researchers with new research lines, as happened to us. In particular, we got exposed to the literature on hybrid systems with stochastic switching, and started our research line on time-inhomogeneous Markov jump linear systems with bounded uncertainties on transition probabilities. After having solved the fundamental problems of stability and optimal control (Zacchia Lun et al., 2016; 2017), we are now approaching the issues of fault (and attack) detection and isolation. In the domain of multi-hop control networks, we already got some exciting results on the topic, providing stabilizability, and fault detection and isolation conditions for the networks subject to node failures and malicious attacks (D'Innocenzo et al., 2016).

Acknowledgments

The research leading to these results has received funding from the Italian Government under CIPE resolution n.135 (Dec. 21, 2012), project *INnovating City Planning through Information and Communication Technologies* (INCIPICT). Our thanks to Paolo Tell for his valuable comments, suggestions, and feedback on an early version of this work. We are also thankful to Fabio Pasqualetti, Chung-Wei Lin, Neil Ernst and the anonymous reviewers for their useful and constructive comments.

Appendix A. Additional results

This section of appendix provides the results of analysis of some additional characteristics of our primary studies, which are not related to CPS security per se, but are still useful to better understand this scientific area. These important characteristics are the theoretical foundations and time-scale models.

A1. Theoretical foundation

Because of the intrinsic multidisciplinary nature of cyber-physical systems, we paid attention also on the theoretical background on which primary studies are built upon. This information is particularly useful for the new researchers who would like to explore this exciting research area. Since the control systems are at the heart of CPS, and the provided perspective is that of researchers from the Automatic Control community, it is not a surprise that control theory is used in every study considered in our mapping study. The mapping of other theoretical backgrounds to each primary study is provided in the Table 24. As a reference to the related application fields, see also Table 3.

The study of graphs is the most used theoretical foundation, found in 38 studies (27.5%). *Graph theory* (see e.g. Kleinberg and Tardos, 2006; Bondy and Murty, 1976) is well suited to represent any kind of topological information, and, in fact, it is used in 29 studies on security of power transmission networks.

To asymptotically analyze the intrinsic difficulty of problems and algorithms, and to decide which of these are likely to be tractable, *computational complexity theory* (see e.g. Horst and Pardalos, 1995; Kleinberg and Tardos, 2006) is employed in 16 works, most of them within the field of power transmission.

Information theory (see e.g. Cover and Thomas, 2006) is used in 12 works[18], most of which treating the security of generic linear dynamical systems.

The methods of dimensionality reduction (such as principal component analysis) and of latent variable separation (e.g. independent component analysis) from *machine learning* and *statistics* provide a way to understand and visualize the structure of complex data sets (see e.g. Lee and Verleysen, 2007). They are used in 7 works, whose application domain is power grids and generic dynamical systems.

Other methods of linear dimensionality reduction are used for simultaneous sensing and compression of finite-dimensional vectors. Providing means for recovering sparse high-dimensional signals from highly incomplete measurements by using efficient algorithms, (Eldar and Kutyniok, 2012), *compressed sensing* is applied in 7 works on power grids and linear dynamical systems.

Starting from 2014, typical *formal methods* concepts of signal temporal logic (STL, which is a rigorous formalism for specifying desired behaviors of continuous signals (Maler and Nickovic, 2004)) and satisfiability modulo theories (SMT) (Barrett et al., 2009) have found their way in 3 studies on CPS security, with applications to anomaly detection and resilient state estimation in generic cyber-physical systems and power grids.

The mathematical *optimization* (see e.g. Horst and Pardalos, 1995; Rao, 2009) is used in several studies and application areas. The sub-fields of optimization found in primary studies include *convex optimization* (21 studies), *linear programming* (16 studies), *dynamic programming* and *integer programming* (both appeared in 11 studies), *nonlinear programming* (6 studies), *quadratic programming* (adopted in 7 works) and *semidefinite programming* (3 studies).

The most used sub-field of *game theory*, Başar and Olsder (1999), found in 8 primary studies, is zero-sum game, which do not allow for any cooperation between the players, since what one player gains incurs a loss to the other player. As expected, all considered games belong to a class of continuous-time infinite dynamic games, also known as *differential games*, wherein the evolution of the state is described by a differential equation and the players act throughout a time interval.

A2. Time-scale model

The dynamic system behavior can be modeled via different time-scale models, such as continuous, discrete and hybrid. In the case of the (quasi-)steady state assumption, the system is treated as (quasi-)static, and the time-scale model is named accordingly. In particular, quasi-static analysis is mostly chosen for addressing control architectures like SCADA, which provide steady-state setpoints to inner control loops. The mapping of each primary study to related time-scale model is reported in Table 25, while the related distribution is shown in Fig. A.30.

The quasi-static model is used in 55 studies (39,9%), all but one (Mo and Sinopoli, 2015)) of them concerned with power systems state estimation, while there are 26 studies (18.8%) considering continuous time, 65 (47.1%) discrete time, and only 5 considering both continuous and discrete time, only 3 of which actually using hybrid time (Zhu and Başar, 2015; Zhu et al., 2018; Jones et al., 2014)).

Appendix B. Threats to validity

We assessed the level of quality of our study by applying the quality checklist proposed by Petersen et al. in

[18] The reference Gupta et al. (2010) is related to Gupta et al. (2011), which is a part of the same research line.

Table 24
Theoretical foundations.

Theoretical framework	Primary studies
Compressed sensing	Hendrickx et al. (2014); Kim and Poor (2011); Ozay et al. (2013); Liu et al. (2014a); Hao et al. (2015); Fawzi et al. (2014); Shoukry and Tabuada (2014)
Computational complexity theory	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Li et al. (2015b); Pasqualetti et al. (2013); Giani et al. (2013); Yang et al. (2014); Mishra et al. (2015a); Lo and Ansari (2013) Deka et al. (2014, 2015a, 2015b); Soltan et al. (2015); Li et al. (2015a); Xu and Zhu (2015)
Control theory	Liu et al. (2011, 2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Vrakopoulou et al. (2015); Teixeira et al. (2010); Huang et al. (2010); Li et al. (2015b); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2013, 2011); Esmalifalak et al. (2011); Liu et al. (2014b); Tajer et al. (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Mohsenian-Rad and Leon-Garcia (2011); Davis et al. (2012); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012); Wei and Kundur (2015); Ozay et al. (2013); Zonouz et al. (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Mishra et al. (2015a); Wang et al. (2014); Valenzuela et al. (2013); Lo and Ansari (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Yang et al. (2016); Qin et al. (2013); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Li (2014); Sanandaji et al. (2014); Wang and Ren (2014); Liu et al. (2015b); Liang et al. (2014); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Manandhar et al. (2014); Tan et al. (2014); Amini et al. (2015); Kim et al. (2015); Yu and Chin (2015); Soltan et al. (2015); Liu et al. (2015a); Rawat and Bajracharya (2015); Anwar et al. (2015); Chakhchoukh and Ishii (2015); Gu et al. (2015); Nudell et al. (Sept. 2015); Li et al. (2015a); Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Ma et al. (2015); Amin et al. (2009); Mo et al. (2015); Mo and Sinopoli (2012); Amin et al. (2010); Gupta et al. (2010); Sundaram et al. (2010); Cáardenas et al. (2011); Befekadu et al. (2015); Zhu and Martínez (2014); Smith (2015); Fawzi et al. (2014); Zhu and Başar (2015); Teixeira et al. (2015b); Kwon et al. (2014); Teixeira et al. (2012); Xue et al. (2014); Foroush and Martínez (2013); Zhu et al. (2018); Shoukry et al. (2013); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Rhouma et al. (2015); Barreto et al. (2013); Kwon and Hwang (2013b); Miao and Zhu (2014); Chen et al. (2015a); Mo and Sinopoli (2015); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Djouadi et al. (2015); Bai et al. (2015); Weimer et al. (2014); De Persis and Tesi (2015); Zhang et al. (2014); Sajjad et al. (2015); Mishra et al. (2015b); Shoukry et al. (2015b); Qi et al. (2015); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Yuan and Mo (2015); Cetinkaya et al. (2015); Xu and Zhu (2015); Zhang and Sankar (2015); Chen et al. (2015b); Tang et al. (2015); Do et al. (2015); Kontouras et al. (2015); Shoukry et al. (2015a); Teixeira et al. (2015a); Tan et al. (2015); Lee et al. (2015); Sanjab and Saad (2015)
Convex optimization	Kosut et al. (2011); Hendrickx et al. (2014); Teixeira et al. (2010); Ozay et al. (2013); Rahman and Mohsenian-Rad (2012); Vuković and Dán (2014); Liu et al. (2014a); Hao et al. (2015); Xie et al. (2011); Jia et al. (2014) Bi and Zhang (2013); Kim et al. (2014b); Amin et al. (2009); Fawzi et al. (2014); Zhu and Başar (2015); Mo and Sinopoli (2015); Pajic et al. (2015); Weimer et al. (2014); Miao et al. (2014); Weerakkody and Sinopoli (2015) Sanjab and Saad (2015)
Dynamic programming	Li et al. (2015b); Deka et al. (2015a,b); Ma et al. (2015); Amin et al. (2009); Mo et al. (2015); Befekadu et al. (2015); Shoukry et al. (2013); Barreto et al. (2013); Liu et al. (2014c); Bezzo et al. (2015)
Formal methods	Rahman et al. (2014); Jones et al. (2014); Shoukry et al. (2015b)
Graph theory	Kosut et al. (2011); Hendrickx et al. (2014); Kim and Poor (2011); Pasqualetti et al. (2013, 2011); Tajer et al. (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Sou et al. (2014); Vuković et al. (2012); Hug and Giampapa (2012); Wei and Kundur (2015) Zonouz et al. (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013); Vuković and Dán (2014); Mishra et al. (2015a); Wang et al. (2014); Lo and Ansari (2013); Sedghi and Jonckheere (2015); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Wang and Ren (2014); Yamaguchi et al. (2014); Kim et al. (2015) Soltan et al. (2015); Nudell et al. (Sept. 2015); Jia et al. (2014); Sundaram et al. (2010); Xue et al. (2014); Zhu et al. (2018); D'Innocenzo et al. (2015); Djouadi et al. (2015); Sajjad et al. (2015); Zhang and Sankar (2015)
Integer programming	Hendrickx et al. (2014); Yuan et al. (2012); Giani et al. (2013); Bi and Zhang (2014); Vuković et al. (2012); Mishra et al. (2015a); Liu et al. (2015b); Yamaguchi et al. (2014); Teixeira et al. (2015b); Pajic et al. (2015) Shoukry et al. (2015b)
Information theory	Mohsenian-Rad and Leon-Garcia (2011); Gupta et al. (2010); Sundaram et al. (2010); Fawzi et al. (2014); Bai et al. (2015); Mishra et al. (2014, 2015b); Kogiso and Fujita (2015); Yuan and Mo (2015); Xu and Zhu (2015) Tang et al. (2015); Shoukry et al. (2015a)
Linear programming	Yuan et al. (2012); Kim and Poor (2011); Bi and Zhang (2014); Mohsenian-Rad and Leon-Garcia (2011); Lo and Ansari (2013); Yamaguchi et al. (2014); Soltan et al. (2015); Jia et al. (2014); Esmalifalak et al. (2012, 2013) Bi and Zhang (2013); Mo et al. (2015); Zhu and Başar (2015); Teixeira et al. (2015b); Pajic et al. (2015); Liu et al. (2014c)
Machine learning and statistics	Esmalifalak et al. (2011); Valenzuela et al. (2013); Liu et al. (2014a); Yu and Chin (2015); Anwar et al. (2015); Tiwari et al. (2014); Jones et al. (2014)
Nonlinerar programming	Vrakopoulou et al. (2015); Qin et al. (2013); Kim et al. (2014a); Li (2014); Nudell et al. (Sept. 2015); Kwon et al. (2014)
Nonzero-sum (differential) game	Zhu et al. (2018); Barreto et al. (2013); Sanjab and Saad (2015)
Quadratic programming	Kim et al. (2015); Liu et al. (2015a); Zhu and Martínez (2014); Zhu and Başar (2015); Weerakkody and Sinopoli (2015); Shoukry et al. (2015b); Xu and Zhu (2015)
Semidefinite programming	Amin et al. (2009); Mo et al. (2015); Weimer et al. (2014)
Stackelberg game	Zhu and Martínez (2014); Sanjab and Saad (2015)
Zero-sum (differential) game	Li et al. (2015b); Esmalifalak et al. (2013); Ma et al. (2015); Gupta et al. (2010); Zhu and Başar (2015); Shoukry et al. (2013); Miao and Zhu (2014); Liu et al. (2014c)

Petersen et al. (2015). The goal of Petersen's quality checklist is to assess an objective quality rating for systematic mapping studies. According to the metrics defined in Petersen's quality checklist, we achieve an outstanding score of 54%, defined as the ratio of the number of actions taken in comparison to the total number of actions reported in the quality checklist. *The quality score of our study is far beyond the scores obtained by existing systematic mapping studies in the literature*, which have a distribution with a median of 33% and 48% as absolute maximum value.

Table 25
Time-scale models.

time-scale model	Primary studies
Continuous	Vrakopoulou et al. (2015); Pasqualetti et al. (2013); Hammad et al. (2015b,a); Liu et al. (2014b); Giani et al. (2013); Wei and Kundur (2015); Nudell et al. (Sept. 2015); Amin et al. (2010); Smith (2015); Zhu and Başar (2015); Teixeira et al. (2012); Xue et al. (2014); Foroush and Martínez (2013); Zhu et al. (2018); D'Innocenzo et al. (2015) Barreto et al. (2013); Djouadi et al. (2015); De Persis and Tesi (2015); Li et al. (2015c); Jones et al. (2014); Bezzo et al. (2015); Sajjad et al. (2015); Teixeira et al. (2015a); Tan et al. (2015); Lee et al. (2015)
Discrete	Huang et al. (2010); Li et al. (2015b); Tajer et al. (2011); Yang et al. (2014); Talebi et al. (2010); Ozay et al. (2013); Zonouz et al. (2012); Vuković and Dán (2014); Yang et al. (2016); Sanandaji et al. (2014); Manandhar et al. (2014); Amini et al. (2015); Rawat and Bajracharya (2015) Gu et al. (2015); Li et al. (2015a); Ma et al. (2015); Amin et al. (2009); Mo et al. (2015); Mo and Sinopoli (2012); Gupta et al. (2010); Sundaram et al. (2010); Cáardenas et al. (2011); Befekadu et al. (2015); Zhu and Martínez (2014); Fawzi et al. (2014); Zhu and Başar (2015); Teixeira et al. (2015b); Kwon et al. (2014); Teixeira et al. (2012); Zhu et al. (2018); Shoukry et al. (2013); D'Innocenzo et al. (2015); Bopardikar and Speranzon (2013); Kwon and Hwang (2013a); Rhouma et al. (2015) Kwon and Hwang (2013b); Miao and Zhu (2014); Chen et al. (2015a); Tiwari et al. (2014); Eyisi and Koutsoukos (2014); Pajic et al. (2015); Bai et al. (2015); Weimer et al. (2014); De Persis and Tesi (2015); Zhang et al. (2014); Liu et al. (2014c); Bezzo et al. (2014); Park et al. (2014); Miao et al. (2014); Mishra et al. (2014); Shoukry and Tabuada (2014); Weerakkody and Sinopoli (2015); Mishra et al. (2015b,b); Shoukry et al. (2015b); Qi et al. (2015); Kogiso and Fujita (2015); Naghnaeian et al. (2015); Yuan and Mo (2015); Cetinkaya et al. (2015); Xu and Zhu (2015); Chen et al. (2015b); Tang et al. (2015); Do et al. (2015); Kontouras et al. (2015); Shoukry et al. (2015a)
(Quasi-)static	Liu et al. (2011); Kosut et al. (2011); Bobba et al. (2010); Hendrickx et al. (2014); Teixeira et al. (2010); Yuan et al. (2012); Kim and Poor (2011); Pasqualetti et al. (2011); Esmalifalak et al. (2011); Giani et al. (2013); Yang et al. (2014); Bi and Zhang (2014); Mohsenian-Rad and Leon-Garcia (2011); Davis et al. (2012); Sou et al. (2014); Talebi et al. (2010); Vuković et al. (2012); Hug and Giampapa (2012); Rahman and Mohsenian-Rad (2012); Kim and Tong (2013) Mishra et al. (2015a); Wang et al. (2014); Valenzuela et al. (2013); Lo and Ansari (2013); Liu et al. (2014a); Sedghi and Jonckheere (2015); Qin et al. (2013); Kim et al. (2014a); Deka et al. (2014, 2015a, 2015b); Li (2014); Wang and Ren (2014); Liu et al. (2015b); Liang et al. (2014); Yamaguchi et al. (2014); Hao et al. (2015); Rahman et al. (2014); Tan et al. (2014); Kim et al. (2015); Yu and Chin (2015); Soltan et al. (2015); Liu et al. (2015a); Anwar et al. (2015); Chakhchoukh and Ishii (2015) Xie et al. (2011); Jia et al. (2014); Esmalifalak et al. (2012); Choi and Xie (2013); Esmalifalak et al. (2013); Bi and Zhang (2013); Kim et al. (2014b); Mo and Sinopoli (2015); Zhang and Sankar (2015); Sanjab and Saad (2015)

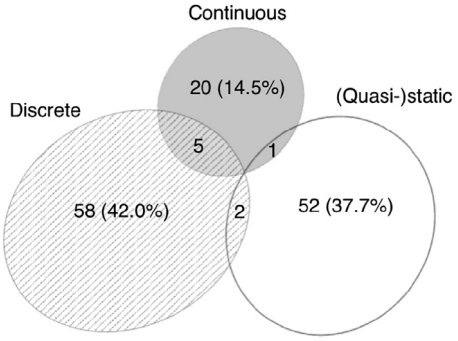


Fig. A1. Distribution of primary studies by time-scale model.

Overall, the high quality of our study has being ensured by producing a detailed research protocol document in which all of its steps have been subject to three external reviews by independent researchers (see Section 3) and by conducting our study by following the well-accepted and updated guidelines of systematic review/mapping study (Kitchenham and Charters, 2007; Petersen et al., 2015). In the following we detail the main threats to validity of our study and how we alleviated them.

Conclusion validity. Conclusion validity refers to the relationship between the extracted data, the produced map, and the resulting findings (Wohlin et al., 2012).

In order to mitigate possible conclusion validities, first of all we defined the search terms systematically and we document procedures in our research protocol, so that our research can be replicated by other researchers interested in the topic. Moreover, we documented and used a rigorously defined data extraction form, so that we could reduce possible biases that may happen during the data extraction process; also, in so doing we had the guarantee that the data extraction process has been consistent to our research questions.

On the same line, the classification scheme could have been another source of threats to the conclusion validity of our study; indeed, other researchers may identify classification schemes with different facets and attributes. In this context, we mitigated this bias by (i) performing an external evaluation by independent researchers who were not involved in our research, and (ii) having the data extraction process conducted by the principle researcher and validated by the secondary researcher.

Internal validity. Internal validity is concerned with the degree of control of our study design with respect to potential extraneous variables influencing the study itself.

In this case, having a rigorously defined protocol with a rigorous data extraction form has surely helped in mitigating biases related to the internal validity of our research. Also, for what concerns the data analysis validity, the threats have been minimal since we employed well-assessed descriptive statistics when dealing with quantitative data. When considering qualitative data, the sensitivity analysis performed on all extracted data has helped in having good internal validity.

Construct validity. It concerns the validity of extracted data with respect to our research questions. Construct validity concerns the selection of the primary studies with respect to how they really represent the population in light of what is investigated.

Firstly, as described in Section 3.3, the automatic search has been performed on multiple electronic databases to get relevant studies independently of publishers' policies and business concerns. Moreover, we are reasonably confident about the construction of the search string used in our automatic search since the used terms have been identified by rigorously applying a systematic procedure (i.e., the quasi-gold standard systematic procedure as defined in Zhang et al. (2011a)). Moreover, the automatic search is complemented by the snowballing activity performed during the search and selection activity of our review process (see Fig. 1), thus

making us reasonably confident about our search strategy. Since our automated search strategy actually relies on search engines quality and on how researchers write their abstracts, the set of primary selected studies have been extended by means of the backward and forward snowballing procedure.

After having collected all relevant studies from the automatic search, we rigorously screened them according to well-documented inclusion and exclusion criteria (see Section 3.4); this selection stage has been performed by the principle researcher, under the supervision of the secondary researcher. Also, in order to assess the quality of the selection process, both principle and secondary researchers assessed a random sample of studies, and inter-researcher agreement has been statistically measured with very good results (i.e., we obtained a Cohen-Kappa coefficient of inter-rater agreement of more than 0.80).

External validity. It concerns the generizability of the produced map and of the discovered findings (Wohlin et al., 2012).

In our research, the most severe threat related to external validity consists in having a set of primary studies that is not representative of the whole research on security for cyber-physical systems. In order to mitigate this possible threat, we employed a search strategy consisting of both automatic search and backward-forward snowballing of selected studies. Using these two search strategies in combination empowered us in mitigating this threat to validity. Also, having a set of well-defined inclusion and exclusion criteria contributed to reinforcing the external validity of our study.

A potential source of issues regarding the external validity of our study can be the fact that only studies published in the English language have been selected in our search. This decision may result in a possible threat to validity because potentially important primary studies published in other languages may have not been selected in our research. However, the English language is the most widely used language for scientific papers, so this bias can be reasonably considered as minimal.

Similarly, grey literature (e.g., white papers, not-peer-reviewed scientific publications, etc.) is not included in our research; this potential bias is intrinsic to our study design, since we want to focus exclusively on the state of the art presented in high-quality scientific papers, and thus undergoing a rigorous peer-reviewed publication process is a well-established requirement for this kind of scientific works.

References

Abbaspour, A., Yen, K.K., Noei, S., Sargolzaei, A., 2016. Detection of fault data injection attack on UAV using adaptive neural network. Proc. Comp. Sci. 95, 193–200.

Abur, A., Exposito, A.G., 2004. Power System State Estimation: Theory and Implementation. CRC Press, Boca Raton, FL.

Adepu, S., Mathur, A., 2016. An investigation into the response of a water treatment system to cyber attacks. In: High Assurance Systems Engineering (HASE), 2016 IEEE 17th International Symposium on. IEEE, pp. 141–148.

Ali, N.B., Petersen, K., 2014. Evaluating strategies for study selection in systematic literature studies. In: Proceedings of the 8th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement. ACM, New York, NY, pp. 45:1–45:4.

Allocca, C., Wavering, A.J., 2013. Strategic Vision and Business Drivers for 21st Century Cyber-Physical Systems. Technical Report. NIST, Gaithersburg, MD. Executive Roundtable Highlights.

AlTawy, R., Youssef, A.M., 2016. Security tradeoffs in cyber physical systems: a case study survey on implantable medical devices. IEEE Access 4, 959–979.

Amin, S., Litrico, X., Sastry, S.S., Bayen, A.M., 2013. Cyber security of water SCADA systems – part II: attack detection using enhanced hydrodynamic models. IEEE Trans. Control Syst. Technol. 21 (5), 1679–1693.

Amini, S., Pasqualetti, F., Mohsenian-Rad, H., 2018. Dynamic load altering attacks against power system stability: attack models and protection schemes. IEEE Trans. Smart Grid 9 (4), 2862–2872.

Anwar, A., Mahmood, A.N., Pickering, M., 2017. Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements. J. Comput. Syst. Sci. 83 (1), 58–72.

Ao, W., Song, Y., Wen, C., 2016. Adaptive cyber-physical system attack detection and reconstruction with application to power systems. IET Control Theory Appl. 10 (12), 1458–1468.

Ao, W., Song, Y., Wen, C., Lai, J., 2018. Finite time attack detection and supervised secure state estimation for CPSs with malicious adversaries. Inf. Sci. 451, 67–82.

Ashok, A., Govindarasu, M., Ajjarapu, V., 2018. Online detection of stealthy false data injection attacks in power system state estimation. IEEE Trans. Smart Grid 9 (3), 2.

Ashok, A., Govindarasu, M., Wang, J., 2017. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. Proc. IEEE 105 (7), 1389–1407.

Attia, M., Senouci, S.M., Sedjelmaci, H., Aglzim, E.-H., Chrenko, D., 2018. An efficient intrusion detection system against cyber-physical attacks in the smart grid. Comput. Electr. Eng. 68, 499–512.

Avižienis, A., Laprie, J.-C., Randell, B., Landwehr, C., 2004. Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. Dependable Secure Comput. 1 (1), 11–33.

Başar, T., Olsder, G.J., 1999. Dynamic Noncooperative Game Theory. Classics in Applied Mathematics, 23, second SIAM, Philadelphia, PA.

Bai, C.-Z., Gupta, V., Pasqualetti, F., 2017. On Kalman filtering with compromised sensors: Attack stealthiness and performance bounds. IEEE Trans. Autom. Control 62 (12), 6641–6648.

Bai, C.-Z., Pasqualetti, F., Gupta, V., 2017. Data-injection attacks in stochastic control systems: detectability and performance tradeoffs. Automatica 82, 251–260.

Barrett, C., Sebastiani, R., Seshia, S., Tinelli, C., 2009. Satisfiability modulo theories. In: Biere, A., Heule, M., van Maaren, H., Walsh, T. (Eds.), Handbook of Satisfiability. In: Frontiers in Artificial Intelligence and Applications, 185. IOS Press, Amsterdam, Netherlands, pp. 825–885.

Basili, V.R., Caldiera, G., Rombach, H.D., 1994. The goal question metric approach. In: Encyclopedia of Software Engineering, 2. Wiley, Hoboken, NJ, pp. 528–532.

Beg, O.A., Johnson, T.T., Davoudi, A., 2017. Detection of false-data injection attacks in cyber-physical DC microgrids. IEEE Trans. Ind. Inf 13 (5), 2693–2703.

Bonaci, T., Herron, J., Yusuf, T., Yan, J., Kohno, T., Chizeck, H.J. To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robotics 2015.

Bondy, J.A., Murty, U.S.R., 1976. Graph theory with applications. North-Holland Publishing Company, Amsterdam, The Netherlands.

Bonnet, P., Manegold, S., Bjørling, M., Cao, W., Gonzalez, J., et al., 2011. Repeatability and workability evaluation of sigmod 2011. ACM SIGMOD Record 40 (2), 45–48.

Brereton, O.P., Kitchenham, B.A., Budgen, D., Turner, M., Khalil, M., 2007. Lessons from applying the systematic literature review process within the software engineering domain. J. Syst. Softw. 80 (4), 571–583.

Bretas, A.S., Bretas, N.G., Carvalho, B., Baeyens, E., Khargonekar, P.P., 2017. Smart grids cyber-physical security as a malicious data attack: an innovation approach. Electr. Power Syst. Res. 149, 210–219.

Cai, G., Chen, B.M., Dong, X., Lee, T.H., 2011. Design and implementation of a robust and nonlinear flight control system for an unmanned helicopter. Mechatronics 21 (5), 803–820.

Camara, C., Peris-Lopez, P., Tapiador, J.E., 2015. Security and privacy issues in implantable medical devices: a comprehensive survey. J. Biomed. Inf. 55, 272–289.

Cárdenas, A.A., Amin, S., Sastry, S.S., 2008. Research challenges for the security of control systems. In: Proceedings of the 3rd Conference on Hot Topics in Security. USENIX, Berkeley, CA, pp. 6:1–6:6.

Cárdenas, A.A., Amin, S., Sastry, S.S., 2008. Secure control: Towards survivable cyber-physical systems. In: Proceedings of the 28th International Conference on Distributed Computing Systems. IEEE, New York, NY, pp. 495–500.

Cetinkaya, A., Ishii, H., Hayakawa, T., 2017. Networked control under random and malicious packet losses. IEEE Trans. Autom. Control 62 (5), 2434–2449.

Cetinkaya, A., Ishii, H., Hayakawa, T., 2018. Analysis of stochastic switched systems with application to networked control under jamming attacks. IEEE Trans. Autom. Control.

Chakravorty, M., Das, D., 2001. Voltage stability analysis of radial distribution networks. Int. J. Electr. Power Energy Syst. 23 (2), 129–135.

Chen, C., Zhang, K., Yuan, K., Zhu, L., Qian, M., 2018. Novel detection scheme design considering cyber attacks on load frequency control. IEEE Trans. Ind. Inf. 14 (5), 1932–1941.

Chen, F., Lei, W., Zhang, K., Tao, G., Jiang, B., 2016. A novel nonlinear resilient control for a quadrotor UAV via backstepping control and nonlinear disturbance observer. Nonlinear Dyn. 85 (2), 1281–1295.

Chen, L., Ali Babar, M., Zhang, H., 2010. Towards an evidence-based understanding of electronic data sources. In: Proceedings of the 14th International Conference on Evaluation and Assessment in Software Engineering. British Computer Society, Swinton, UK, pp. 135–138.

Chen, T.M., Abu-Nimeh, S., 2011. Lessons from Stuxnet. Computer 44 (4), 91–93.

Chen, Y., Kar, S., Moura, J.M., 2017. Dynamic attack detection in cyber-physical systems with side initial state information. IEEE Trans. Autom. Control 62 (9), 4618–4624.

Chen, Y., Kar, S., Moura, J.M., 2017. Optimal attack strategies subject to detection constraints against cyber-physical systems. IEEE Trans. Control Netw. Syst.

Chen, Y., Kar, S., Moura, J.M., 2018. Cyber physical attacks with control objectives. IEEE Trans. Autom. Control 63 (5), 1418–1425.

Chin, W.-L., Lee, C.-H., Jiang, T., 2017. Blind false data attacks against AC state estimation based on geometric approach in smart grid communications. IEEE Trans. Smart Grid.

Chow, J.H., Cheung, K.W., 1992. A toolbox for power system dynamics and control engineering education and research. IEEE Trans. Power Syst. 7 (4), 1559–1564.

Cintuglu, M.H., Mohammed, O.A., Akkaya, K., Uluagac, A.S., 2017. A survey on smart grid cyber-physical system testbeds. IEEE Commun. Surv. Tutorials 19 (1), 446–464.

Cohen, J., 1968. Weighted kappa: Nominal scale agreement provision for scaled disagreement or partial credit. Psychol. Bull. 70 (4), 213.
Cover, T.M., Thomas, J.A., 2006. Elements of Information Theory, 2nd Wiley, Hoboken, NJ.
Cruzes, D.S., Dybå, T., 2011. Research synthesis in software engineering: atertiary study. Inf. Softw. Technol. 53 (5), 440–455. Special Section on Best Papers from {XP2010}.
De Persis, C., Tesi, P., 2016. Networked control of nonlinear systems under denial-of-service. Syst. Control Lett. 96, 124–131.
Deng, R., Xiao, G., Lu, R., 2017. Defending against false data injection attacks on power system state estimation. IEEE Trans. Ind. Inf. 13 (1), 198–207.
Deng, R., Xiao, G., Lu, R., Liang, H., Vasilakos, A.V., 2017. False data injection on state estimation in power systems – attacks, impacts, and defense: a survey. IEEE Trans. Ind. Inf. 13 (2), 411–423.
Deng, R., Zhuang, P., Liang, H., 2017. CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid. IEEE Trans. Smart Grid 8 (5), 2420–2430.
Ding, D., Han, Q.-L., Xiang, Y., Ge, X., Zhang, X.-M., 2018. A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing 275, 1674–1683.
Ding, D., Wang, Z., Han, Q.-L., Wei, G., 2018. Security control for discrete-time stochastic nonlinear systems subject to deception attacks. IEEE Trans. Syst. Man Cybern.Syst. 48 (5), 779–789.
Ding, D., Wang, Z., Ho, D.W., Wei, G., 2017. Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks. Automatica 78, 231–240.
Ding, D., Wang, Z., Wei, G., Alsaadi, F.E., 2016. Event-based security control for discrete-time stochastic systems. IET Control Theory Appl. 10 (15), 1808–1815.
Ding, D., Wei, G., Zhang, S., Liu, Y., Alsaadi, F.E., 2017. On scheduling of deception attacks for discrete-time networked systems equipped with attack detectors. Neurocomputing 219, 99–106.
Ding, K., Li, Y., Quevedo, D.E., Dey, S., Shi, L., 2017. A multi-channel transmission schedule for remote state estimation under DoS attacks. Automatica 78, 194–201.
D'Innocenzo, A., Di Benedetto, M.D., Serra, E., 2013. Fault tolerant control of multi--hop control networks. IEEE Trans. Autom. Control 58 (6), 1377–1389.
D'Innocenzo, A., Smarra, F., Di Benedetto, M.D., 2016. Resilient stabilization of multi-hop control networks subject to malicious attacks. Automatica 71, 1–9.
Dolk, V., Tesi, P., De Persis, C., Heemels, W., 2017. Event-triggered control systems under denial-of-service attacks. IEEE Trans. Control Netw. Syst. 4 (1), 93–105.
Dong, Y., Gupta, N., Chopra, N., 2016. On content modification attacks in bilateral teleoperation systems. In: American Control Conference (ACC), 2016. IEEE, pp. 316–321.
Eldar, Y.C., Kutyniok, G., 2012. Compressed Sensing: Theory and Applications. Cambridge University Press (CUP), Cambridge, UK.
Esnaola, I., Perlaza, S.M., Poor, H.V., Kosut, O., 2016. Maximum distortion attacks in electricity grids. IEEE Trans. Smart Grid 7 (4), 2007–2015.
Farokhi, F., Shames, I., Batterham, N., 2017. Secure and private control using semi-homomorphic encryption. Control Eng. Pract. 67, 13–20.
Farraj, A., Hammad, E., Al Daoud, A., Kundur, D., 2016. A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems. IEEE Trans. Smart Grid 7 (4), 1846–1855.
Feng, S., Tesi, P., 2017. Resilient control under denial-of-Service: robust design. Automatica 79, 42–51.
Forti, N., Battistelli, G., Chisci, L., Li, S., Wang, B., Sinopoli, B., 2018. Distributed joint attack detection and secure state estimation. IEEE Trans. Signal Inf.Process.Netw. 4 (1), 96–110.
Gai, K., Qiu, M., Ming, Z., Zhao, H., Qiu, L., 2017. Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. IEEE Trans. Smart Grid 8 (5), 2431–2439.
Garcia, L., Brasser, F., Cintuglu, M.H., Sadeghi, A.-R., Mohammed, O.A., Zonouz, S.A., 2017. Hey, my malware knows physics! attacking PLCS with physical model aware rootkit. In: 24th Annual Symposium on Network & Distributed System Security (NDSS). Internet Society, pp. 8:1–8:15.
Giraldo, J., Cárdenas, A.A., Quijano, N., 2017. Integrity attacks on real-time pricing in smart grids: impact and countermeasures. IEEE Trans. Smart Grid 8 (5), 2249–2257.
Giraldo, J., Sarkar, E., Cárdenas, A.A., Maniatakos, M., Kantarcioglu, M., 2017. Security and privacy in cyber-physical systems: A survey of surveys. IEEE Des. Test 34 (4), 7–17.
Greenhalgh, T., Peacock, R., 2005. Effectiveness and efficiency of search methods in systematic reviews of complex evidence: audit of primary sources. BMJ 331 (7524), 1064–1065.
Guo, Z., Shi, D., Johansson, K.H., Shi, L., 2017. Optimal linear cyber-attack on remote state estimation. IEEE Trans. Control Netw. Syst. 4 (1), 4–13.
Guo, Z., Shi, D., Johansson, K.H., Shi, L., 2018. Worst-case stealthy innovation-based linear attack on remote state estimation. Automatica 89, 117–124.
Gupta, A., Langbort, C., Başar, T., 2011. One-stage control over an adversarial channel with finite codelength. In: Proceedings of the 50th Annual Conference on Decision and Control and European Control Conference. IEEE, New York, NY, pp. 4072–4077.
Halperin, D., Heydt-Benjamin, T., Ransford, B., Clark, S., Defend, B., et al., 2008. Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. In: Proceedings of the 2008 IEEE Symposium on Security and Privacy. IEEE, New York, NY, pp. 129–142.
He, H., Yan, J., 2016. Cyber-physical attacks and defences in the smart grid: a survey. IET Cyber-Phys. Syst. Theory Appl. 1 (1), 13–27.
Holdren, J.P., Lander, E., Jackson, S.A., Schmidt, E., 2010. Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology. Executive Report. President's Council of Advisors on Science and Technology (PCAST).
, 1995. Handbook of Global Optimization. In: Horst, R., Pardalos, P.M. (Eds.). Nonconvex Optimization and Its Applications, 2. Springer, Dordrecht, The Netherlands.
Hu, J., Liu, S., Ji, D., Li, S., 2016. On co-design of filter and fault estimator against randomly occurring nonlinearities and randomly occurring deception attacks. Int. J. Gen. Syst. 45 (5), 619–632.
Huang, K., Zhou, C., Tian, Y.-C., Yang, S., Qin, Y., 2018. Assessing the physical impact of cyberattacks on industrial cyber-physical systems. IEEE Trans. Ind. Electron. 65 (10), 8153–8162.
Huang, Y., Tang, J., Cheng, Y., Li, H., Campbell, K.A., Han, Z., 2016. Real-time detection of false data injection in smart grid networks: an adaptive CUSUM method and analysis. IEEE Syst. J. 10 (2), 532–543.
Huang, Y.-F., Werner, S., Huang, J., Kashyap, N., Gupta, V., 2012. State estimation in electric power grids: meeting new challenges presented by the requirements of the future grid. IEEE Signal Process. Mag. 29 (5), 33–43.
Hwang, I., Kim, S., Kim, Y., Seah, C.E., 2010. A survey of fault detection, isolation, and reconfiguration methods. IEEE Trans. Control Syst. Technol. 18 (3), 636–653.
Isozaki, Y., Yoshizawa, S., Fujimoto, Y., Ishii, H., Ono, I., Onoda, T., Hayashi, Y., 2016. Detection of cyber attacks against voltage control in distribution power grids with PVs. IEEE Trans. Smart Grid 7 (4), 1824–1835.
Jalali, S., Wohlin, C., 2012. Systematic literature studies: database searches vs. backward snowballing. In: Proceedings of the ACM-IEEE International Symposium on Empirical Software Engineering and Measurement. ACM, New York, NY, pp. 29–38.
Jin, X., Haddad, W.M., Yucelen, T., 2017. An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems. IEEE Trans. Autom. Control 62 (11), 6058–6064.
Johansson, K.H., 2000. The quadruple-tank process: a multivariable laboratory process with an adjustable zero. IEEE Trans. Control Syst. Technol. 8 (3), 456–465.
Karimipour, H., Dinavahi, V., 2018. Robust massively parallel dynamic state estimation of power systems against cyber-attack. IEEE Access 6, 2984–2995.
Keller, J., Sauter, D., 2013. Monitoring of stealthy attack in networked control systems. In: Control and Fault-Tolerant Systems (SysTol), 2013 Conference on, pp. 462–467.
Keller, J.-Y., Chabir, K., Sauter, D., 2016. Input reconstruction for networked control systems subject to deception attacks and data losses on control signals. Int. J. Syst. Sci. 47 (4), 814–820.
Kim, J., Lee, C., Shim, H., Cheon, J.H., Kim, A., Kim, M., Song, Y., 2016. Encrypting controller using fully homomorphic encryption for security of cyber-physical systems. IFAC-PapersOnLine 49 (22), 175–180. Distributed Estimation and Control in Networked Systems (NECSYS), 6th IFAC Workshop on.
Kim, J., Lee, C., Shim, H., Eun, Y., Seo, J.H., 2018. Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems having redundant sensors. IEEE Trans. Autom. Control.
Kitchenham, B.A., Charters, S., 2007. Guidelines for performing systematic literature reviews in software engineering. Technical Report. Keele University and University of Durham.
Kleinberg, J., Tardos, É., 2006. Algorithm design. Addison-Wesley, Boston, MA.
Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., 2010. Experimental security analysis of a modern automobile. In: Proceedings of the 2010 IEEE Symposium on Security and Privacy. IEEE, New York, NY, pp. 447–462.
Kundur, P., 1994. Power System Stability and Control. McGraw-Hill Education, New York, NY.
Kung, E., Dey, S., Shi, L., 2017. The performance and limitations of e-stealthy attacks on higher order systems. IEEE Trans. Autom. Control 62 (2), 941–947.
Lanotte, R., Merro, M., Muradore, R., Viganò, L., 2017. A formal approach to cyber-physical attacks. In: 30th IEEE Computer Security Foundations Symposium (CSF). IEEE, pp. 436–450.
Lee, C., Shim, H., Eun, Y., 2018. On redundant observability: from security index to attack detection and resilient state estimation. IEEE Trans. Autom. Control.
Lee, E.A., Seshia, S.A., 2015. Introduction to Embedded Systems - A Cyber-Physical Systems Approach, 2 Lee & Seshia, Berkeley, CA.
Lee, I., Sokolsky, O., 2010. Medical cyber physical systems. In: Proceedings of the 47th Design Automation Conference. ACM, New York, NY, pp. 743–748.
Lee, J.A., Verleysen, M., 2007. Nonlinear Dimensionality Reduction, 1st Springer, New York, NY.
, 2010. In: Levine, W.S. (Ed.), The Control Handbook, 2nd. CRC Press, Boca Raton, FL.
Li, B., Lu, R., Wang, W., Choo, K.-K.R., 2016. DDOA: A Dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system. IEEE Trans. Inf. Forensics Secur. 11 (11), 2415–2425.
Li, B., Lu, R., Wang, W., Choo, K.-K.R., 2017. Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. J. Parallel Distrib. Comput. 103, 32–41.
Li, F., Yang, C., Tang, Y., 2018. Optimal linear attack on cyber physical systems with multiplicative noise. IEEE Access 6, 33318–33328.
Li, Y., Quevedo, D., Dey, S., Shi, L., 2015. Fake-acknowledgment attack on ACK-based sensor power schedule for remote state estimation. In: 54th IEEE Conference on Decision and Control (CDC), pp. 5795–5800.
Li, Y., Quevedo, D.E., Dey, S., Shi, L., 2017. A game-theoretic approach to fake-acknowledgment attack on cyber-physical systems. IEEE Trans. Signal Inf.Process.Netw. 3 (1), 1–11.

Li, Y., Quevedo, D.E., Dey, S., Shi, L., 2017. SINR-based DoS attack on remote state estimation: a game-theoretic approach. IEEE Trans. Control Netw. Syst. 4 (3), 632–642.

Li, Y., Shi, L., Chen, T., 2017. Detection against linear deception attacks on multi-sensor remote state estimation. IEEE Trans. Control Netw. Syst.

Li, Z., Avgeriou, P., Liang, P., 2015. A systematic mapping study on technical debt and its management. J. Syst. Softw. 101, 193–220.

Li, Z., Shahidehpour, M., Alabdulwahab, A., Abusorrah, A., 2016. Bilevel model for analyzing coordinated cyber-physical attacks on power systems. IEEE Trans. Smart Grid 7 (5), 2260–2272.

Li, Z., Shahidehpour, M., Aminifar, F., 2017. Cybersecurity in distributed power systems. Proc. IEEE 105 (7), 1367–1388.

Liang, G., Zhao, J., Luo, F., Weller, S.R., Dong, Z.Y., 2017. A review of false data injection attacks against modern power systems. IEEE Trans. Smart Grid 8 (4), 1630–1638.

Liang, J., Sankar, L., Kosut, O., 2016. Vulnerability analysis and consequences of false data injection attack on power system state estimation. IEEE Trans. Power Syst. 31 (5), 3864–3872.

Lin, H., Chen, C., Wang, J., Qi, J., Jin, D., Kalbarczyk, Z., Iyer, R.K., 2018. Self-healing attack-resilient PMU network for power system operation. IEEE Trans. Smart Grid 9 (3), 1551–1565.

Lin, H., Slagell, A., Kalbarczyk, Z., Sauer, P., Iyer, R., 2018. Runtime semantic security analysis to detect and mitigate control-related attacks in power grids. IEEE Trans. Smart Grid 9 (1), 163–178.

Liu, S., Kundur, D., Zourntos, T., Butler-Purry, K., 2012. Coordinated variable structure switching in smart power systems: attacks and mitigation. In: Proceedings of the 1st International Conference on High Confidence Networked Systems. ACM, New York, NY, pp. 21–30.

Liu, S., Wei, G., Song, Y., Liu, Y., 2016. Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks. Neurocomputing 207, 708–716.

Liu, X., Li, Z., 2017. False data attacks against AC state estimation with incomplete network information. IEEE Trans. Smart Grid 8 (5), 2239–2248.

Liu, X., Li, Z., 2017. Local topology attacks in smart grids. IEEE Trans. Smart Grid 8 (6), 2617–2626.

Liu, X., Li, Z., 2017. Trilevel modeling of cyber attacks on transmission lines. IEEE Trans. Smart Grid 8 (2), 720–729.

Liu, X., Li, Z., Li, Z., 2017. Optimal protection strategy against false data injection attacks in power systems. IEEE Trans. Smart Grid 8 (4), 1802–1810.

Liu, X., Li, Z., Liu, X., Li, Z., 2016. Masking transmission line outages via false data injection attacks. IEEE Trans. Inf. Forensics Secur. 11 (7), 1592–1602.

Lopez-Herrejon, R.E., Linsbauer, L., Egyed, A., 2015. A systematic mapping study of search-based software engineering for software product lines. Inf. Softw. Technol. 61, 33–51.

Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., Gan, D., 2018. Cloud-based cyber-physical intrusion detection for vehicles using deep learning. IEEE Access 6, 3491–3508.

Ma, L., Wang, Z., Han, Q.-L., Lam, H.-K., 2017. Variance-constrained distributed filtering for time-varying systems with multiplicative noises and deception attacks over sensor networks. IEEE Sens. J. 17 (7), 2279–2288.

Malavolta, I., Muccini, H., 2014. A study on MDE approaches for engineering wireless sensor networks. In: Proceedings of the 40th EUROMICRO Conference on Software Engineering and Advanced Applications. IEEE, New York, NY, pp. 149–157.

Maler, O., Nickovic, D., 2004. Monitoring temporal properties of continuous signals. In: Lakhnech, Y., Yovine, S. (Eds.), Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems. In: Lecture Notes in Computer Science, 3253. Springer, Berlin, Germany, pp. 152–166.

Mathur, A.P., Tippenhauer, N.O., 2016. SWaT: A water treatment testbed for research and training on ICS security. In: Cyber-physical Systems for Smart Water Networks (CySWater), 2016 International Workshop on. IEEE, pp. 31–36.

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M., Karri, R., 2016. The cybersecurity landscape in industrial control systems. Proc. IEEE 104 (5), 1039–1057.

Miao, F., Zhu, Q., Pajic, M., Pappas, G.J., 2017. Coding schemes for securing cyber-physical systems against stealthy data injection attacks. IEEE Trans. Control Netw. Syst. 4 (1), 106–117.

Micallef, L., Rodgers, P., 2014. euler APE: Drawing area-proportional 3-Venn diagrams using ellipses. PloS one 9 (7), e101717.

Mishra, S., Shoukry, Y., Karamchandani, N., Diggavi, S.N., Tabuada, P., 2017. Secure state estimation against sensor attacks in the presence of noise. IEEE Trans. Control Netw. Syst. 4 (1), 49–59.

Mo, Y., Garone, E., 2016. Secure dynamic state estimation via local estimators. In: Decision and Control (CDC), 2016 IEEE 55th Conference on. IEEE, pp. 5073–5078.

Mo, Y., Kim, T.H.-H., Brancik, K., Dickinson, D., Lee, H., Perrig, A., Sinopoli, B., 2012. Cyber-physical security of a smart grid infrastructure. Proc. IEEE 100 (1), 195–209.

Mo, Y., Sinopoli, B., 2016. On the performance degradation of cyber-physical systems under stealthy integrity attacks. IEEE Trans. Autom. Control 61 (9), 2618–2624.

Muradore, R., Quaglia, D., 2015. Energy-efficient intrusion detection and mitigation for networked control systems security. IEEE Trans. Ind. Inf. 11 (3), 830–840.

Murguia, C., Ruths, J., 2016. Characterization of a custum model-based sensor attack detector. In: Decision and Control (CDC), 2016 IEEE 55th Conference on. IEEE, pp. 1303–1309.

Nakahira, Y., Mo, Y., 2018. Attack-resilient $\mathcal{H}_2$, $\mathcal{H}_\infty$, and ℓ_1 state estimator. IEEE Trans. Autom. Control.

Narendra, K.S., Tripathi, S., 1973. Identification and optimization of aircraft dynamics. J. Aircraft 10 (4), 193–199.

Nguyen, P.H., Ali, S., Yue, T., 2017. Model-based security engineering for cyber-physical systems: a systematic mapping study. Inf. Softw. Technol. 83, 116–135.

NSF, 2016. Cyber-Physical Systems (CPS). Program Solicitation, NSF 16-549. National Science Foundation.

Ozay, M., Esnaola, I., Vural, F.T.Y., Kulkarni, S.R., Poor, H.V., 2016. Machine learning methods for attack detection in the smart grid. IEEE Trans. Neural Netw. Learn.Syst. 27 (8), 1773–1786.

Pajic, M., Lee, I., Pappas, G.J., 2017. Attack-resilient state estimation for noisy dynamical systems. IEEE Trans. Control Netw. Syst. 4 (1), 82–92.

Pajic, M., Weimer, J., Bezzo, N., Sokolsky, O., Pappas, G.J., Lee, I., 2017. Design and implementation of attack-resilient cyberphysical systems: with a focus on attack-resilient state estimators. IEEE Control Syst. 37 (2), 66–81.

Pajic, M., Weimer, J., Bezzo, N., Tabuada, P., Sokolsky, O., Lee, I., Pappas, G., 2014. Robustness of attack-resilient state estimators. In: Proceedings of the ACM/IEEE 5th International Conference on Cyber-Physical Systems (with CPS Week 2014). IEEE, New York, NY, pp. 163–174.

Pan, Y., White, J., Schmidt, D.C., Elhabashy, A., Sturm, L., Camelio, J., Williams, C., 2017. Taxonomies for reasoning about cyber-physical attacks in iot-based manufacturing systems.. Int. J. Interact. Multimedia Artif. Intell. 4 (3).

Pang, Y., Xia, H., Grimble, M.J., 2018. Resilient nonlinear control for attacked cyber–physical systems. IEEE Trans. Syst. Man Cybern.: Systems.

Pang, Z.-H., Liu, G.-P., Zhou, D., Hou, F., Sun, D., 2016. Two-channel false data injection attacks against output tracking control of networked systems. IEEE Trans. Ind. Electron. 63 (5), 3242–3251.

Paridari, K., O'Mahony, N., Mady, A.E.-D., Chabukswar, R., Boubekeur, M., Sandberg, H., 2018. A framework for attack-resilient industrial control systems: attack detection and controller reconfiguration. Proc. IEEE 106 (1), 113–128.

Pasqualetti, F., Bicchi, A., Bullo, F., 2012. Consensus computation in unreliable networks: asystem theoretic approach. IEEE Trans. Autom. Control 57 (1), 90–104.

Pasqualetti, F., Dörfler, F., Bullo, F., 2012. Cyber-physical security via geometric control: distributed monitoring and malicious attacks. In: Proceedings of the 51st Annual Conference on Decision and Control. IEEE, New York, NY, pp. 3418–3425.

Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M., 2008. Systematic mapping studies in software engineering. In: Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering. British Computer Society, Swinton, UK, pp. 68–77.

Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M., 2008. Systematic mapping studies in software engineering. In: Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering. British Computer Society, Swinton, UK, pp. 68–77.

Petersen, K., Vakkalanka, S., Kuzniarz, L., 2015. Guidelines for conducting systematic mapping studies in software engineering: an update. Inf. Softw. Technol. 64, 1–18.

PETTICREW, M., ARAI, L., ROBERTS, H., BRITTEN, N., POPAY, J., 2009. Testing methodological guidance on the conduct of narrative synthesis in systematic reviews. Evaluation 15, 1.

Poovendran, R., 2010. Cyber-physical systems: Close encounters between two parallel worlds [Point of View]. Proc. IEEE 98 (8), 1363–1366.

Popay, J., Roberts, H., Sowden, A., Petticrew, M., Arai, L., Rodgers, M., Britten, N., Roen, K., Duffy, S., 2006. Guidance on the conduct of narrative synthesis in systematic reviews. A product from the ESRC methods programme Version 1, b92.

Rahman, M.S., Mahmud, M.A., Oo, A.M.T., Pota, H.R., 2017. Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems. IEEE Trans. Ind. Inf. 13 (2), 436–447.

Rajkumar, R.R., Lee, I., Sha, L., Stankovic, J., 2010. Cyber-physical systems: the next computing revolution. In: Proceedings of the 47th Design Automation Conference. ACM, New York, NY, pp. 731–736.

Rao, S.S., 2009. Engineering Optimization: Theory and Practice, 4th Wiley, Hoboken, NJ.

Ricker, N.L., 1993. Model predictive control of a continuous, nonlinear, two-phase reactor. J. Process Control 3 (2), 109–123.

Rushanan, M., Rubin, A.D., Kune, D.F., Swanson, C.M., 2014. Sok: Security and privacy in implantable medical devices and body area networks. In: 2014 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 524–539.

Sandberg, H., Teixeira, A., Johansson, K.H., 2010. On security indices for state estimators in power networks. In: Proceedings of the First Workshop on Secure Control Systems, CPS Week 2010. KTH, Stockholm, Sweden, pp. 63–68.

Sanjab, A., Saad, W., 2016. Data injection attacks on smart grids with multiple adversaries: a game-theoretic perspective. IEEE Trans. Smart Grid 7 (4), 2038–2049.

Satchidanandan, B., Kumar, P.R., 2017. Dynamic watermarking: active defense of networked cyber–physical systems. Proc. IEEE 105 (2), 219–240.

Sauer, P., Pai, M., 1997. Power System Dynamics and Stability. Stipes Publishing, Champaign, IL.

Senejohnny, D., Tesi, P., De Persis, C., 2017. A jamming-resilient algorithm for self-triggered network coordination. IEEE Trans. Control Netw. Syst.

Shi, D., Elliott, R.J., Chen, T., 2017. On finite-state stochastic modeling and secure estimation of cyber-physical systems. IEEE Trans. Autom. Control 62 (1), 65–80.

Shi, D., Guo, Z., Johansson, K.H., Shi, L., 2018. Causality countermeasures for anomaly detection in cyber-physical systems. IEEE Trans. Autom. Control 63 (2), 386–401.

Shoukry, Y., Chong, M., Wakaiki, M., Nuzzo, P., Sangiovanni-Vincentelli, A., Seshia, S.A., Hespanha, J.P., Tabuada, P., 2018. SMT-based observer design for cyber-physical systems under sensor attacks. ACM Trans. Cyber-Phys. Syst. 2 (1), 5:1–5:27.

Shoukry, Y., Nuzzo, P., Puggelli, A., Sangiovanni-Vincentelli, A.L., Seshia, S.A., Tabuada, P., 2017. Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach. IEEE Trans. Autom. Control 62 (10), 4917–4932.
Shoukry, Y., Puggelli, A., Nuzzo, P., Sangiovanni-Vincentelli, A.L., Seshia, S.A., Tabuada, P., 2015. Sound and complete state estimation for linear dynamical systems under sensor attack using satisfiability modulo theory solving. In: Proceedings of the 2015 American Control Conference. IEEE, New York, NY, pp. 3818–3823.
Shoukry, Y., Tabuada, P., 2016. Event-triggered state observers for sparse sensor noise/attacks. IEEE Trans. Autom. Control 61 (8), 2079–2091.
Smarra, F., Jain, A., de Rubeis, T., Ambrosini, D., D'Innocenzo, A., Mangharam, R., 2018. Data-driven model predictive control using random forests for building energy optimization and climate control. Applied Energy.
Spencer, D., 2009. Card sorting: Designing usable categories. Rosenfeld Media.
Sridhar, S., Hahn, A., Govindarasu, M., 2012. Cyber-physical system security for the electric power grid. Proc. IEEE 100 (1), 210–224.
Srikantha, P., Kundur, D., 2016. A DER attack-mitigation differential game for smart grid security analysis. IEEE Trans. Smart Grid 7 (3), 1476–1485.
Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A., 2015. Guide to Industrial Control Systems (ICS) Security. Technical Report. NIST, Gaithersburg, MD.
Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A., 2015. NIST SP 800-82 Rev. 2. Guide to Industrial Control Systems (ICS) Security. Technical Report. NIST.
Sun, H., Peng, C., Zhang, W., Yang, T., Wang, Z., 2018. Security-based resilient event-triggered control of networked control systems under denial of service attacks. J. Franklin Institute.
Sundaram, S., Hadjicostis, C.N., 2011. Distributed function calculation via linear iterative strategies in the presence of malicious agents. IEEE Trans. Autom. Control 56 (7), 1495–1508.
Taati, B., Tahmasebi, A.M., Hashtrudi-Zaad, K., 2008. Experimental identification and analysis of the dynamics of a PHANToM Premium 1.5A Haptic Device. Presence: Teleoperators and Virtual Environ. 17 (4), 327–343.
Taha, A.F., Qi, J., Wang, J., Panchal, J.H., 2018. Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs. IEEE Trans. Smart Grid 9 (2), 886–899.
Tan, R., Nguyen, H.H., Foo, E.Y., Yau, D.K., Kalbarczyk, Z., Iyer, R.K., Gooi, H.B., 2017. Modeling and mitigating impact of false data injection attacks on automatic generation control. IEEE Transactions on Information Forensics and Security 12 (7), 1609–1624.
Teixeira, A., Sou, K.C., Sandberg, H., Johansson, K.H., 2015. Secure control systems: a quantitative risk management approach. IEEE Control Syst. 35 (1), 24–45.
Teixeira, A.M., Araújo, J., Sandberg, H., Johansson, K.H., 2017. Distributed sensor and actuator reconfiguration for fault-tolerant networked control systems. IEEE Trans. Control Netw. Syst.
Tiri, K., 2007. Side-channel attack pitfalls. In: Proceedings of the 44th Annual Design Automation Conference. ACM, New York, NY, pp. 15–20.
Tsiamis, A., Gatsis, K., Pappas, G.J., 2017. State estimation with secrecy against eavesdroppers. IFAC-PapersOnLine 50 (1), 8385–8392.
Urbina, D., Giraldo, J., Cárdenas, A.A., Valente, J., Faisal, M., Tippenhauer, N.O., Ruths, J., Candell, R., Sandberg, H., 2016. NIST GCR 16-010. Survey and new directions for physics-based attack detection in control systems. Technical Report. NIST.
Urbina, D.I., Giraldo, J.A., Cárdenas, A.A., Tippenhauer, N.O., Valente, J., Faisal, M., Ruths, J., Candell, R., Sandberg, H., 2016. Limiting the impact of stealthy attacks on industrial control systems. In: Computer and Communications Security (CSS), 2016 ACM 23rd Conference on. ACM, pp. 1092–1105.
Walsh, G.C., Ye, H., Bushnell, L.G., 2002. Stability analysis of networked control systems. IEEE Trans. Control Syst. Technol. 10 (3), 438–446.
Wang, D., Wang, Z., Shen, B., Alsaadi, F.E., 2017. Security-guaranteed filtering for discrete-time stochastic delayed systems with randomly occurring sensor saturations and deception attacks. Int. J. Robust Nonlinear Control 27 (7), 1194–1208.
Weerakkody, S., Liu, X., Son, S.H., Sinopoli, B., 2017. A graph-theoretic characterization of perfect attackability for secure design of distributed control systems. IEEE Trans. Control Netw. Syst. 4 (1), 60–70.
Weerakkody, S., Mo, Y., Sinopoli, B., 2014. Detecting integrity attacks on control systems using robust physical watermarking. In: Proceedings of the 53rd Annual Conference on Decision and Control. IEEE, New York, NY, pp. 3757–3764.
Weerakkody, S., Sinopoli, B., 2016. A moving target approach for identifying malicious sensors in control systems. In: Communication, Control, and Computing (Allerton), 2016 54th Annual Allerton Conference on. IEEE, pp. 1149–1156.
Weerakkody, S., Sinopoli, B., Kar, S., Datta, A., 2016. Information flow for security in control systems. In: Decision and Control (CDC), 2016 IEEE 55th Conference on, pp. 5065–5072.
Wei, L., Sarwat, A., Saad, W., Biswas, S., 2018. Stochastic games for power grid protection against coordinated cyber-physical attacks. IEEE Trans. Smart Grid 9 (2), 684–694.
Wells, L.J., Camelio, J.A., Williams, C.B., White, J., 2014. Cyber-physical security challenges in manufacturing systems. Manuf. Lett. 2 (2), 74–77.
Wieringa, R., Maiden, N., Mead, N., Rolland, C., 2006. Requirements engineering paper classification and evaluation criteria: a proposal and a discussion. Requir. Eng. 11 (1), 102–107.
Wohlin, C., 2014. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering. ACM, New York, NY, pp. 38:1–38:10.
Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B., Wesslén, A., 2012. Experimentation in Software Engineering. Computer Science, Springer, Berlin, Germany.
Wood, A., Wollenberg, B., 1996. Power generation, operation and control, 2nd Wiley, Hoboken, NJ.
Xiang, Y., Ding, Z., Zhang, Y., Wang, L., 2017. Power system reliability evaluation considering load redistribution attacks. IEEE Trans. Smart Grid 8 (2), 889–901.
Yampolskiy, M., Horvath, P., Koutsoukos, X., Xue, Y., Sztipanovits, J., 2013. Taxonomy for description of cross-domain attacks on CPS. In: Proceedings of the 2Nd ACM International Conference on High Confidence Networked Systems. ACM, New York, NY, pp. 135–142.
Yang, Q., An, D., Min, R., Yu, W., Yang, X., Zhao, W., 2017. On optimal PMU placement-based defense against data integrity attacks in smart grid. IEEE Trans. Inf. Forensics Secur. 12 (7), 1735–1750.
Yang, Q., Li, D., Yu, W., Liu, Y., An, D., Yang, X., Lin, J., 2017. Toward data integrity attacks against optimal power flow in smart grid. IEEE Internet Things J. 4 (3).
Ye, H., Ge, Y., Liu, X., Li, Z., 2016. Transmission line rating attack in two-settlement electricity markets. IEEE Trans. Smart Grid 7 (3), 1346–1355.
Yuan, E., Esfahani, N., Malek, S., 2014. A systematic survey of self-protecting software systems. ACM Trans. Auton. Adapt. Syst 8 (4), 17:1–17:41.
Yuan, Y., Sun, F., Liu, H., 2016. Resilient control of cyber-physical systems against intelligent attacker: a hierarchal Stackelberg game approach. Int. J. Syst. Sci. 47 (9), 2067–2077.
Zacchia Lun, Y., D'Innocenzo, A., Abate, A., Di Benedetto, M.D., 2017. Optimal robust control and a separation principle for polytopic time-inhomogeneous Markov jump linear systems. In: 56th IEEE Conference on Decision and Control (CDC). IEEE, pp. 6525–6530.
Zacchia Lun, Y., D'Innocenzo, A., Di Benedetto, M.D., 2016. On stability of time-inhomogeneous Markov jump linear systems. In: 55th IEEE Conference on Decision and Control (CDC). IEEE, pp. 5527–5532.
Zeltmann, S.E., Gupta, N., Tsoutsos, N.G., Maniatakos, M., Rajendran, J., Karri, R., 2016. Manufacturing and security challenges in 3d printing. JOM 68 (7), 1872–1881.
Zhang, H., Ali Babar, M., Tell, P., 2011. Identifying relevant studies in software engineering. Inf. Softw. Technol. 53 (6), 625–637.
Zhang, H., Cheng, P., Shi, L., Chen, J., 2016. Optimal DoS attack scheduling in wireless networked control system. IEEE Trans. Control Syst. Technol. 24 (3), 843–852.
Zhang, H., Qi, Y., Wu, J., Fu, L., He, L., 2018. DoS attack energy management against remote state estimation. IEEE Trans. Control Netw. Syst. 5 (1), 383–394.
Zhang, J., Sankar, L., 2016. Physical system consequences of unobservable state-and–topology cyber-physical attacks. IEEE Trans. Smart Grid 7 (4), 106–117.
Zhang, X., Yang, X., Lin, J., Xu, G., Yu, W., 2017. On data integrity attacks against real–time pricing in energy-based cyber-physical systems. IEEE Trans Parallel Distrib Syst. 28 (1), 170–187.
Zhang, Y., Wang, L., Sun, W., Green, R., Alam, M., 2011. Distributed intrusion detection system in a multi-layer network architecture of smart grids. Smart Grid, IEEE Trans. 2 (4), 796–808.
Zhao, C., He, J., Cheng, P., Chen, J., 2017. Analysis of consensus-based distributed economic dispatch under stealthy attacks. IEEE Trans. Ind. Electron. 64 (6), 5107–5117.
Zhao, J., Zhang, G., La Scala, M., Dong, Z.Y., Chen, C., Wang, J., 2017. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks. IEEE Trans. Smart Grid 8 (4), 1580–1590.
Zheng, B., Deng, P., Anguluri, R., Zhu, Q., Pasqualetti, F., 2016. Cross-layer codesign for secure cyber-physical systems. IEEE Trans. Comput.-Aided Des. Integr. Circ. Syst. 35 (5), 699–711.
Zimmerman, R., Murillo-Sánchez, C., Thomas, R.J., 2011. MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans. Power Syst. 26 (1), 12–19.
Zimmerman, R. D., Murillo-Sánchez, C. E., 2016. Matpower 6.0 User's Manual.

Selected Primary Studies

Amin, S., Cáardenas, Á.A., Sastry, S.S., 2009. Safe and secure networked control systems under Denial-of-Service attacks. In: Majumdar, R., Tabuada, P. (Eds.), Hybrid Systems: Computation and Control (HSCC). Springer, Berlin, Germany, pp. 31–45.
Amin, S., Litrico, X., Sastry, S.S., Bayen, A.M., 2010. Stealthy deception attacks on water SCADA systems. In: 13th International Conference on Hybrid Systems: Computation and Control (HSCC). ACM, pp. 161–170.
Amini, S., Mohsenian-Rad, H., Pasqualetti, F., 2015. Dynamic load altering attacks in smart grid. In: Innovative Smart Grid Technologies (ISGT). IEEE, pp. 1–5.
Anwar, A., Mahmood, A.N., Tari, Z., 2015. Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid. Inf. Syst. 53, 201–212.
Bai, C.Z., Pasqualetti, F., Gupta, V., 2015. Security in stochastic control systems: Fundamental limitations and performance bounds. In: American Control conference (ACC). IEEE, pp. 195–200.
Barreto, C., Cárdenas, A.A., Quijano, N., 2013. Controllability of dynamical systems: Threat models and reactive security. In: Das, S.K., Nita-Rotaru, C., Kantarcioglu, M. (Eds.), Decision and Game Theory for Security (GameSec). Lecture Notes in Computer Science, (8252). Springer, Cham, Switzerland, pp. 45–64.
Befekadu, G.K., Gupta, V., Antsaklis, P.J., 2015. Risk-sensitive control under Markov modulated Denial-of-Service (DoS) attack strategies. IEEE Trans. Autom. Control 60 (12), 3299–3304.

Bezzo, N., Du, Y., Sokolsky, O., Lee, I., 2015. A Markovian approach for attack resilient control of mobile robotic systems. In: 2nd International Workshop on Robotic Sensor Networks (CPSWEEK), pp. 2:1–2:6.

Bezzo, N., Weimer, J., Pajic, M., Sokolsky, O., Pappas, G.J., Lee, I., 2014. Attack resilient state estimation for autonomous robotic systems. In: International Conference on Intelligent Robots and Systems (IROS). IEEE, pp. 3692–3698.

Bi, S., Zhang, Y.J., 2013. False-data injection attack to control real-time price in electricity market. In: Global Communications Conference (GLOBECOM). IEEE, pp. 772–777.

Bi, S., Zhang, Y.J., 2014. Using covert topological information for defense against malicious attacks on DC state estimation. IEEE J. Select. Areas Commun. 32 (7), 1471–1485.

Bobba, R.B., Rogers, K.M., Wang, Q., Khurana, H., Nahrstedt, K., Overbye, T.J., 2010. Detecting false data injection attacks on DC state estimation. In: 1st Workshop on Secure Control Systems, CPS Week, pp. 18–26.

Bopardikar, S.D., Speranzon, A., 2013. On analysis and design of stealth-resilient control systems. In: 6th International Symposium on Resilient Control Systems (ISRCS). IEEE, pp. 48–53.

Cáardenas, Á.A., Amin, S., Lin, Z.S., Huang, Y.L., Huang, C.Y., Sastry, S.S., 2011. Attacks against process control systems: Risk assessment, detection, and response. In: 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS), pp. 355–366.

Cetinkaya, A., Ishii, H., Hayakawa, T., 2015. Event-triggered control over unreliable networks subject to jamming attacks. In: 54th IEEE Conference on Decision and Control (CDC). IEEE, pp. 4818–4823.

Chakhchoukh, Y., Ishii, H., 2015. Coordinated cyber-attacks on the measurement function in hybrid state estimation. IEEE Trans. Power Syst. 30 (5), 2487–2497.

Chen, J., Shi, L., Cheng, P., Zhang, H., 2015. Optimal Denial-of-Service attack scheduling with energy constraint. IEEE Trans. Autom. Control 60 (11), 3023–3028.

Chen, Y., Kar, S., Moura, J.M., 2015. Cyber-physical systems: Dynamic sensor attacks and strong observability. In: International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, pp. 1752–1756.

Choi, D.H., Xie, L., 2013. Ramp-induced data attacks on look-ahead dispatch in real–time power markets. IEEE Trans. Smart Grid 4 (3), 1235–1243.

Davis, K.R., Morrow, K.L., Bobba, R., Heine, E., 2012. Power flow cyber attacks and perturbation-based defense. In: International Conference on Smart Grid Communications (SmartGridComm). IEEE, pp. 342–347.

De Persis, C., Tesi, P., 2015. Input-to-State stabilizing control under Denial-of-Service. IEEE Trans. Autom. Control 60 (11), 2930–2944.

Deka, D., Baldick, R., Vishwanath, S., 2014. Optimal hidden SCADA attacks on power grid: a graph theoretic approach. In: International Conference on Computing, Networking and Communications (ICNC). IEEE, pp. 36–40.

Deka, D., Baldick, R., Vishwanath, S., 2015. One breaker is enough: hidden topology attacks on power grids. In: Power & Energy Society General Meeting. IEEE, pp. 1–5.

Deka, D., Baldick, R., Vishwanath, S., 2015. Optimal data attacks on power grids: leveraging detection & measurement jamming. In: International Conference on Smart Grid Communications (SmartGridComm). IEEE, pp. 392–397.

D'Innocenzo, A., Smarra, F., DiBenedetto, M.D., 2015. Further results on fault detection and isolation of malicious nodes in Multi-hop Control Networks. In: European Control Conference (ECC). IEEE, pp. 1860–1865.

Djouadi, S.M., Melin, A.M., Ferragut, E.M., Laska, J.A., Dong, J., 2015. Finite energy and bounded attacks on control system sensor signals. In: American Control Conference (ACC). IEEE, pp. 1716–1722.

Do, V.L., Fillatre, L., Nikiforov, I., 2015. Sequential monitoring of SCADA systems against cyber/physical attacks. In: 9th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS), IFAC-PapersOnLine, Vol. 48, pp. 746–753.

Esmalifalak, M., Han, Z., Song, L., 2012. Effect of stealthy bad data injection on network congestion in market based power system. In: Wireless Communications and Networking Conference (WCNC). IEEE, pp. 2468–2472.

Esmalifalak, M., Nguyen, H., Zheng, R., Han, Z., 2011. Stealth false data injection using independent component analysis in smart grid. In: International Conference on Smart Grid Communications (SmartGridComm). IEEE, pp. 244–248.

Esmalifalak, M., Shi, G., Han, Z., Song, L., 2013. Bad data injection attack and defense in electricity market using game theory study. IEEE Trans. Smart Grid 4 (1), 160–169.

Eyisi, E., Koutsoukos, X., 2014. Energy-based attack detection in networked control systems. In: 3rd International Conference on High Confidence Networked Systems (HiCoNS). ACM, pp. 115–124.

Fawzi, H., Tabuada, P., Diggavi, S., 2014. Secure estimation and control for cyber–physical systems under adversarial attacks. IEEE Trans. Autom. Control 59 (6), 1454–1467.

Foroush, H.S., Martínez, S., 2013. On multi-input controllable linear systems under unknown periodic DoS jamming attacks. In: Conference on Control and its Applications. SIAM, pp. 222–229.

Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P., Poolla, K., 2013. Smart grid data integrity attacks. IEEE Trans. Smart Grid 4 (3), 1244–1253.

Gu, C., Jirutitijaroen, P., Motani, M., 2015. Detecting false data injection attacks in AC state estimation. IEEE Trans. Smart Grid 6, 5, 2476–2483.

Gupta, A., Langbort, C., Başar, T., 2010. Optimal control in the presence of an intelligent jammer with limited actions. In: 49th IEEE Conference on Decision and Control (CDC), pp. 1096–1101.

Hammad, E., Farraj, A.K., Kundur, D., 2015. A resilient feedback linearization control scheme for smart grids under cyber-physical disturbances. In: Innovative Smart Grid Technologies (ISGT). IEEE, pp. 1–5.

Hammad, E., Khalil, A.M., Farraj, A., Kundur, D., Iravani, R., 2015. Tuning out of phase: resonance attacks. In: International Conference on Smart Grid Communications (SmartGridComm). IEEE, pp. 491–496.

Hao, J., Piechocki, R.J., Kaleshi, D., Chin, W.H., Fan, Z., 2015. Sparse malicious false data injection attacks and defense mechanisms in smart grids. IEEE Trans. Ind. Inf. 11 (5), 1–12.

Hendrickx, J.M., Johansson, K.H., Jungers, R.M., Sandberg, H., Sou, K.C., 2014. Efficient computations of a security index for false data attacks in power networks. IEEE Trans. Autom. Control 59 (12), 3194–3208.

Huang, Y., Li, H., Campbell, K.A., Han, Z., 2010. Defending false data injection attack on smart grid network using adaptive CUSUM test. In: 45th Annual Conference on Information Sciences and Systems (CISS). IEEE, pp. 1–6.

Hug, G., Giampapa, J.A., 2012. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans. Smart Grid 3 (3), 1362–1370.

Jia, L., Kim, J., Thomas, R.J., Tong, L., 2014. Impact of data quality on real-time locational marginal price. IEEE Trans. Power Syst. 29 (2), 627–636.

Jones, A., Kong, Z., Belta, C., 2014. Anomaly detection in cyber-physical systems: a formal methods approach. In: 53rd IEEE Conference on Decision and Control (CDC). IEEE, pp. 848–853.

Kim, J., Tong, L., 2013. On topology attack of a smart grid: undetectable attacks and countermeasures. IEEE J. Select. Areas Commun. 31 (7), 1294–1305.

Kim, J., Tong, L., Thomas, R.J., 2014. Data framing attack on state estimation. IEEE J. Select. Areas Commun. 32 (7), 1460–1470.

Kim, J., Tong, L., Thomas, R.J., 2014. Dynamic attacks on power systems economic dispatch. In: Asilomar Conference on Signals, Systems, and Computers, 2014. IEEE, pp. 345–349.

Kim, J., Tong, L., Thomas, R.J., 2015. Subspace methods for data attack on state estimation: A data driven approach. IEEE Trans. Signal Process. 63 (5), 1102–1114.

Kim, T.T., Poor, H.V., 2011. Strategic protection against data injection attacks on power grids. IEEE Trans. Smart Grid 2 (2), 326–333.

Kogiso, K., Fujita, T., 2015. Cyber-security enhancement of networked control systems using homomorphic encryption. In: 54th IEEE Conference on Decision and Control (CDC). IEEE, pp. 6836–6843.

Kontouras, E., Tzes, A., Dritsas, L., 2015. Covert attack on a discrete-time system with limited use of the available disruption resources. In: European Control Conference (ECC). IEEE, pp. 812–817.

Kosut, O., Jia, L., Thomas, R.J., Tong, L., 2011. Malicious data attacks on the smart grid. IEEE Trans. Smart Grid 2 (4), 645–658.

Kwon, C., Hwang, I., 2013. Analytical analysis of cyber attacks on unmanned aerial systems. In: Guidance, Navigation, and Control Conference (GNC). AIAA, pp. 1–12.

Kwon, C., Hwang, I., 2013. Hybrid robust controller design: cyber attack attenuation for cyber-physical systems. In: 52nd IEEE Conference on Decision and Control (CDC), pp. 188–193.

Kwon, C., Liu, W., Hwang, I., 2014. Analysis and design of stealthy cyber attacks on unmanned aerial systems. J. Aerospace Inf. Syst. 11 (8), 525–539.

Lee, C., Shim, H., Eun, Y., 2015. Secure and robust state estimation under sensor attacks, measurement noises, and process disturbances: Observer-based combinatorial approach. In: European Control Conference (ECC). IEEE, pp. 1872–1877.

Li, S., Yilmaz, Y., Wang, X., 2015. Quickest detection of false data injection attack in wide-area smart grids. IEEE Trans. Smart Grid 6 (6), 2725–2735.

Li, Y., Wan, Y., 2014. State summation for detecting false data attack on smart grid. Int. J. Electr. Power Energy Syst. 57, 156–163.

Li, Y., Shi, L., Cheng, P., Chen, J., Quevedo, D.E., 2015. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. IEEE Trans. Autom. Control 60 (10), 2831–2836.

Li, Y., Voos, H., Darouach, M., Hua, C., 2015. An algebraic detection approach for control systems under multiple stochastic cyber-attacks. IEEE/CAA J. Autom. Sin. 2 (3), 258–266.

Liang, J., Kosut, O., Sankar, L., 2014. Cyber attacks on AC state estimation: Unobservability and physical consequences. In: Power & Energy Society General Meeting. IEEE, pp. 1–5.

Liu, L., Esmalifalak, M., Ding, Q., Emesih, V.A., Han, Z., 2014. Detecting false data injection attacks on power grid by sparse optimization. IEEE Trans. Smart Grid 5 (2), 612–621.

Liu, S., Chen, B., Zourntos, T., Kundur, D., Butler-Purry, K., 2014. A coordinated multi--switch attack for cascading failures in smart grid. IEEE Trans. Smart Grid 5 (3), 1183–1195.

Liu, S., Liu, P.X., El Saddik, A., 2014. A stochastic game approach to the security issue of networked control systems under jamming attacks. J. Franklin Inst. 351 (9), 4570–4583.

Liu, T., Sun, Y., Liu, Y., Gui, Y., Zhao, Y., Wang, D., Shen, C., 2015. Abnormal traffic-indexed state estimation: a cyber-physical fusion approach for smart grid attack detection. Future Gener. Comput. Syst. 49, 94–103.

Liu, X., Bao, Z., Lu, D., Li, Z., 2015. Modeling of local false data injection attacks with reduced network information. IEEE Trans. Smart Grid 6 (4), 1686–1696.

Liu, Y., Ning, P., Reiter, M.K., 2011. False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. 14 (1), 13:1–13:33.

Lo, C.H., Ansari, N., 2013. CONSUMER: a novel hybrid intrusion detection system for distribution networks in smart grid. IEEE Trans. Emerg. Topics Comput. 1 (1), 33–44.

Ma, J., Liu, Y., Song, L., Han, Z., 2015. Multiact dynamic game strategy for jamming attack in electricity market. IEEE Trans. Smart Grid 6 (5), 2273–2282.

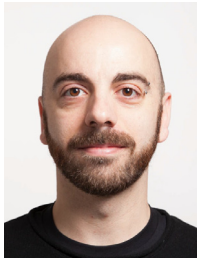
Manandhar, K., Cao, X., Hu, F., Liu, Y., 2014. Detection of faults and attacks including false data injection attack in smart grid using kalman filter. IEEE Trans. Control Netw. Syst. 1 (4), 370–379.
Miao, F., Zhu, Q., 2014. A moving-horizon hybrid stochastic game for secure control of cyber-physical systems. In: 53rd IEEE Conference on Decision and Control (CDC), pp. 517–522.
Miao, F., Zhu, Q., Pajic, M., Pappas, G.J., 2014. Coding sensor outputs for injection attacks detection. In: 53rd IEEE Conference on Decision and Control (CDC), pp. 5776–5781.
Mishra, S., Karamchandani, N., Tabuada, P., Diggavi, S., 2014. Secure state estimation and control using multiple (insecure) observers. In: 53rd IEEE Conference on Decision and Control (CDC). IEEE, pp. 1620–1625.
Mishra, S., Li, X., Kuhnle, A., Thai, M.T., Seo, J., 2015. Rate alteration attacks in smart grid. In: Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, pp. 2353–2361.
Mishra, S., Shoukry, Y., Karamchandani, N., Diggavi, S., Tabuada, P., 2015. Secure state estimation: optimal guarantees against sensor attacks in the presence of noise. In: International Symposium on Information Theory (ISIT). IEEE, pp. 2929–2933.
Mo, Y., Sinopoli, B., 2012. Integrity attacks on cyber-physical systems. In: 1st International Conference on High Confidence Networked Systems (HiCoNS). ACM, pp. 47–54.
Mo, Y., Sinopoli, B., 2015. Secure estimation in the presence of integrity attacks. IEEE Trans. Autom. Control 60 (4), 1145–1151.
Mo, Y., Weerakkody, S., Sinopoli, B., 2015. Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor outputs. IEEE Control Syst. 35 (1), 93–109.
Mohsenian-Rad, A.H., Leon-Garcia, A., 2011. Distributed internet-based load altering attacks against smart power grids. IEEE Trans. Smart Grid 2 (4), 667–674.
Naghnaeian, M., Hirzallah, N., Voulgaris, P.G., 2015. Dual rate control for security in cyber-physical systems. In: 54th IEEE Conference on Decision and Control (CDC). IEEE, pp. 1415–1420.
Nudell, T.R., Nabavi, S., Chakrabortty, A., 2015. A real-time attack localization algorithm for large power system networks using graph-theoretic techniques. IEEE Trans. Smart Grid 6 (5), 2551–2559.
Ozay, M., Esnaola, I., Vural, F.T.Y., Kulkarni, S.R., Poor, H.V., 2013. Sparse attack construction and state estimation in the smart grid: Centralized and distributed models. IEEE J. Select. Areas Commun. 31 (7), 1306–1318.
Pajic, M., Tabuada, P., Lee, I., Pappas, G.J., 2015. Attack-resilient state estimation in the presence of noise. In: 54th IEEE Conference on Decision and Control (CDC), pp. 5827–5832.
Park, P., Khadilkar, H., Balakrishnan, H., Tomlin, C.J., 2014. High confidence networked control for next generation air transportation systems. IEEE Trans. Autom. Control 59 (12), 3357–3372.
Pasqualetti, F., Carli, R., Bullo, F., 2011. A distributed method for state estimation and false data detection in power networks. In: International Conference on Smart Grid Communications (SmartGridComm). IEEE, pp. 469–474.
Pasqualetti, F., Dörfler, F., Bullo, F., 2013. Attack detection and identification in cyber-physical systems. IEEE Trans. Autom. Control 58 (11), 2715–2729.
Qi, Y., Cheng, P., Shi, L., Chen, J., 2015. Event-based attack against remote state estimation. In: 54th IEEE Conference on Decision and Control (CDC). IEEE, pp. 6844–6849.
Qin, Z., Li, Q., Chuah, M.C., 2013. Defending against unidentifiable attacks in electric power grids. IEEE Trans. Parallel Distrib. Syst. 24 (10), 1961–1971.
Rahman, M.A., Al-Shaer, E., Bobba, R.B., 2014. Moving target defense for hardening the security of the power system state estimation. In: 1st ACM Workshop on Moving Target Defense (MTD), pp. 59–68.
Rahman, M.A., Mohsenian-Rad, H., 2012. False data injection attacks with incomplete information against smart power grids. In: Global Communications Conference (GLOBECOM). IEEE, pp. 3153–3158.
Rawat, D.B., Bajracharya, C., 2015. Detection of false data injection attacks in smart grid communication systems. IEEE Signal Process. Lett. 22 (10), 1652–1656.
Rhouma, T., Keller, J., Sauter, D., Chabir, K., Abdelkrim, M., 2015. Active GLR detector for resilient LQG controller in networked control systems. In: 9th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS), IFAC-PapersOnLine, Vol. 48, pp. 754–759.
Sajjad, I., Dunn, D. D., Sharma, R., Gerdes, R., 2015. Attack mitigation in adversarial platooning using detection-based sliding mode control. 43–53.
Sanandaji, B.M., Bitar, E., Poolla, K., Vincent, T.L., 2014. An abrupt change detection heuristic with applications to cyber data attacks on power systems. In: American Control Conference (ACC). IEEE, pp. 5056–5061.
Sanjab, A., Saad, W., 2015. Smart grid data injection attacks: to defend or not? In: International Conference on Smart Grid Communications (SmartGridComm). IEEE, pp. 380–385.
Sedghi, H., Jonckheere, E., 2015. Statistical structure learning to ensure data integrity in smart grid. IEEE Trans. Smart Grid 6 (4), 1924–1933.
Shoukry, Y., Araujo, J., Tabuada, P., Srivastava, M., Johansson, K.H., 2013. Minimax control for cyber-physical systems under network packet scheduling attacks. In: 2nd ACM International Conference on High Confidence Networked Systems (HiCoNS). ACM, pp. 93–100.
Shoukry, Y., Martin, P., Yona, Y., Diggavi, S., Srivastava, M., 2015. Pycra: physical challenge-response authentication for active sensors under spoofing attacks. In: 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 1004–1015.
Shoukry, Y., Nuzzo, P., Bezzo, N., Sangiovanni-Vincentelli, A.L., Seshia, S.A., Tabuada, P., 2015. Secure state reconstruction in differentially flat systems under sensor attacks using satisfiability modulo theory solving. In: 54th IEEE Conference on Decision and Control (CDC). IEEE, pp. 3804–3809.
Shoukry, Y., Tabuada, P., 2014. Event-triggered projected Luenberger observer for linear systems under sparse sensor attacks. In: 53rd IEEE Conference on Decision and Control (CDC). IEEE, pp. 3548–3553.
Smith, R.S., 2015. Covert misappropriation of networked control systems: Presenting a feedback structure. IEEE Control Syst. 35 (1), 82–92.
Soltan, S., Yannakakis, M., Zussman, G., 2015. Joint cyber and physical attacks on power grids: Graph theoretical approaches for information recovery. In: International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS). ACM, pp. 361–374.
Sou, K.C., Sandberg, H., Johansson, K.H., 2014. Data attack isolation in power networks using secure voltage magnitude measurements. IEEE Trans. Smart Grid 5 (1), 14–28.
Sundaram, S., Pajic, M., Hadjicostis, C.N., Mangharam, R., Pappas, G.J., 2010. The wireless control network: monitoring for malicious behavior. In: 49th IEEE Conference on Decision and Control (CDC), pp. 5979–5984.
Tajer, A., Kar, S., Poor, H.V., Cui, S., 2011. Distributed joint cyber attack detection and state recovery in smart grids. In: International Conference on Smart Grid Communications (SmartGridComm). IEEE, pp. 202–207.
Talebi, M., Wang, J., Qu, Z., 2010. Secure power systems against malicious cyber–physical data attacks: protection and identification. In: International Conference on Power Systems Engineering, WASET, pp. 112–119.
Tan, R., Krishna, V.B., Yau, D.K., Kalbarczyk, Z., 2015. Integrity attacks on real-time pricing in electric power grids. In: ACM Transactions on Information and System Security (TISSEC), Vol. 18, pp. 5:1–5:33.
Tan, S., Song, W.Z., Stewart, M., Tong, L., 2014. LPAttack: Leverage point attacks against state estimation in smart grid. In: Global Communications Conference (GLOBECOM). IEEE, pp. 643–648.
Tang, B., Alvergue, L.D., Gu, G., 2015. Secure networked control systems against replay attacks without injecting authentication noise. In: American Control Conference (ACC). IEEE, pp. 6028–6033.
Teixeira, A., Amin, S., Sandberg, H., Johansson, K.H., Sastry, S.S., 2010. Cyber security analysis of state estimators in electric power systems. In: 49th IEEE Conference on Decision and Control (CDC), pp. 5991–5998.
Teixeira, A., Paridari, K., Sandberg, H., Johansson, K.H., 2015. Voltage control for interconnected microgrids under adversarial actions. In: 20th Conference on Emerging Technologies & Factory Automation (ETFA). IEEE, pp. 1–8.
Teixeira, A., Shames, I., Sandberg, H., Johansson, K.H., 2012. Revealing stealthy attacks in control systems. In: 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton). IEEE, pp. 1806–1813.
Teixeira, A., Shames, I., Sandberg, H., Johansson, K.H., 2015. A secure control framework for resource-limited adversaries. Automatica 51, 135–148.
Tiwari, A., Dutertre, B., Jovanović, D., de Candia, T., Lincoln, P.D., Rushby, J., Sadigh, D., Seshia, S., 2014. Safety envelope for security. In: 3rd International Conference on High Confidence Networked Systems (HiCoNS). ACM, pp. 85–94.
Valenzuela, J., Wang, J., Bissinger, N., 2013. Real-time intrusion detection in power system operations. IEEE Trans. Power Syst. 28 (2), 1052–1062.
Vrakopoulou, M., Esfahani, P.M., Margellos, K., Lygeros, J., Andersson, G., 2015. Cyber-attacks in the automatic generation control. In: Khaitan, S.K., McCalley, J.D., Liu, C.C. (Eds.), Cyber Physical Systems Approach to Smart Electric Power Grid, Power Systems. Springer, Berlin, Germany, pp. 303–328.
Vuković, O., Dán, G., 2014. Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks. IEEE J. Select. Areas Commun. 32 (7), 1500–1508.
Vuković, O., Sou, K.C., Dán, G., Sandberg, H., 2012. Network-aware mitigation of data integrity attacks on power system state estimation. IEEE J. Select. Areas Commun. 30 (6), 1108–1118.
Wang, D., Guan, X., Liu, T., Gu, Y., Shen, C., Xu, Z., 2014. Extended distributed state estimation: A detection method against tolerable false data injection attacks in smart grids. Energies 7 (3), 1517–1538.
Wang, S., Ren, W., 2014. Stealthy attacks in power systems: limitations on manipulating the estimation deviations caused by switching network topologies. In: 53rd IEEE Conference on Decision and Control (CDC), pp. 217–222.
Weerakkody, S., Sinopoli, B., 2015. Detecting integrity attacks on control systems using a moving target approach. In: 54th IEEE Conference on Decision and Control (CDC). IEEE, pp. 5820–5826.
Wei, J., Kundur, D., 2015. Biologically inspired hierarchical cyber-physical multi-agent distributed control framework for sustainable smart grids. In: Khaitan, S.K., McCalley, J.D., Liu, C.C. (Eds.), Cyber Physical Systems Approach to Smart Electric Power Grid, Power Systems. Springer, Berlin, Germany, pp. 219–259.
Weimer, J., Bezzo, N., Pajic, M., Sokolsky, O., Lee, I., 2014. Attack-resilient minimum mean-squared error estimation. In: American Control Conference (ACC). IEEE, pp. 1114–1119.
Xie, L., Mo, Y., Sinopoli, B., 2011. Integrity data attacks in power market operations. IEEE Trans. Smart Grid 2 (4), 659–666.
Xu, Z., Zhu, Q., 2015. Secure and resilient control design for cloud enabled networked control systems. In: 1st ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (CPS-SPC), pp. 31–42.
Xue, M., Wang, W., Roy, S., 2014. Security concepts for the dynamics of autonomous vehicle networks. Automatica 50 (3), 852–857.
Yamaguchi, Y., Ogawa, A., Takeda, A., Iwata, S., 2014. Cyber security analysis of power networks by hypergraph cut algorithms. In: International Conference on Smart Grid Communications (SmartGridComm). IEEE, pp. 824–829.

Yang, Q., Chang, L., Yu, W., 2016. On false data injection attacks against kalman filtering in power system dynamic state estimation. Secur. Commun. Netw. 9 (9), 833–849. [First published: 27 August 2013].
Yang, Q., Yang, J., Yu, W., An, D., Zhang, N., Zhao, W., 2014. On false data-injection attacks against power system state estimation: Modeling and countermeasures. IEEE Trans. Parallel Distrib. Syst. 25 (3), 717–729.
Yu, Z.H., Chin, W.L., 2015. Blind false data injection attack using PCA approximation method in smart grid. IEEE Trans. Smart Grid 6 (3), 1219–1226.
Yuan, Y., Li, Z., Ren, K., 2012. Quantitative analysis of load redistribution attacks in power systems. IEEE Trans. Parallel Distrib. Syst. 23 (9), 1731–1738.
Yuan, Y., Mo, Y., 2015. Security in cyber-physical systems: Controller design against known-plain text attack. In: 54th IEEE Conference on Decision and Control (CDC). IEEE, pp. 5814–5819.
Zhang, H., Cheng, P., Wu, J., Shi, L., Chen, J., 2014. Online deception attack against remote state estimation. In: 19th IFAC World Congress (IFAC), pp. 128–133.
Zhang, J., Sankar, L., 2015. Implementation of unobservable state-preserving topology attacks. In: North American Power Symposium (NAPS). IEEE, pp. 1–6.
Zhu, M., Martínez, S., 2014. On the performance analysis of resilient networked control systems under replay attacks. IEEE Trans. Autom. Control 59 (3), 804–808.
Zhu, Q., Başar, T., 2015. Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. IEEE Control Syst. 35 (1), 46–65.
Zhu, Q., Bushnell, L., Başar, T., 2018. Resilient distributed control of multi-agent cyber-physical systems. In: Tarraf, D.C. (Ed.), Control of Cyber-Physical Systems. Springer, Cham, Zug, Switzerland, pp. 301–316.
Zonouz, S., Rogers, K.M., Berthier, R., Bobba, R.B., Sanders, W.H., Overbye, T.J., 2012. SCPSE: security-oriented cyber-physical state estimation for power grid critical infrastructures. IEEE Trans. Smart Grid 3 (4), 1790–1799.

Yuriy Zacchia Lun is Research Collaborator at the IMT School for Advanced Studies Lucca, Italy. His research focuses on automatic control of stochastic hybrid systems, formal methods and security in cyber-physical domain. He is a member of IEEE. He received his PhD in computer science from the Gran Sasso Science Institute, Italy, in 2017 and MEng in telecommunications engineering from University of LA'quila, Italy, in 2012.

Alessandro D'Innocenzo received the Laurea degree (cum laude) in electrical engineering, in 2000, and the Ph.D. degree in electrical and information engineering, 2007, from the University of LA'quila, Italy. He has been a Postdoctoral Researcher in the Department of Electrical and Information Engineering, University of LA'quila and in the Department of Electrical and Systems Engineering, University of Pennsylvania, US. Since January 2010, he has been an Assistant Professor in the Department of Information Engineering, Computer Science, and Mathematics, University of LA'quila. Prof. D'Innocenzo was recipient of the Fondazione Filauro award for Ph.D. students in 2005, and in 2015 of the Best Application Paper Award of the European Control Conference. His research focuses on control and formal verification of hybrid and networked embedded systems with applications to air traffic management, automation and communication systems.

Francesco Smarra is Postdoctoral researcher at the Department of Information Engineering, Computer Science and Mathematics at the University of LA'quila, Italy, where he also obtained his Ph.D. in April 2014. He accomplished the International Curriculum Option of Doctoral Studies in Networked, Embedded, and Hybrid Control Systems for Complex, Distributed and Heterogeneous Systems (ICO-NEH) in 2014. He was recipient of Fondazione F. Filauro award for PhD students in 2013 and of the Best Application Paper Award of the European Control Conference in 2015. He has held several visiting research positions at UC Berkeley and University of Pennsylvania, USA. His research interests are in control theory, wireless networked control systems, and data-driven approaches based on machine learning with application to building automation systems, structural monitoring, and power systems.



Ivano Malavolta is Assistant Professor at the Vrije Universiteit Amsterdam, the Netherlands. His research focuses on data-driven software engineering, software engineering for mobile development, software architecture, model-driven engineering (MDE), and robotics. He is program committee member and reviewer of international conferences and journals in software engineering. He authored more than 80 papers in international journals and peer-reviewed international conferences proceedings. He received a PhD in computer science from the University of L'Aquila in 2012. He is a member of ACM and IEEE, Amsterdam Data Science, and VERSEN (the Dutch National Association for Software Engineering). More information is available at http://www.ivanomalavolta.com.

Maria Domenica Di Benedetto has been Professor of Control Theory at University of LA'quila since 1994. From 1995 to 2002, she has been Adjunct Professor at the Department of EECS, University of California at Berkeley. In 1987, she was Visiting Scientist at MIT, in 1988, 1989 and 1992 Visiting Professor at the University of Michigan, Ann Arbor, in 1992 Chercheur Associé, C.N.R.S., Poste Rouge, Ecole Nationale Supérieure de Mécanique, Nantes, France, from 1990 to 1995 McKay Professor at the University of California Berkeley. She is the Director of the Center of Excellence for Research DEWS "Architectures and Design methodologies for Embedded controllers, Wireless interconnect and System-on-Chip". She has been President of the European Embedded Control Institute since 2009. Since 2010, she has been a Member of the International Advisory Board of the Lund Center for the Control of Complex engineering systems (LCCC). Since 2013, she has been President of the Italian Society of Researchers in Automatic Control (SIDRA). In 2002, she was elected IEEE Fellow. From 2007 to 2010, she has been member of the IEEE Control Systems Technical Fields Award Committee, IEEE Control Systems Society. From 2003 to 2007 she has been Chair of the Standing Committee on Fellow Nominations, IEEE Control Systems Society. From 1995 to 1999, she has been Associate Editor of the IEEE Transactions of Automatic Control. From 2006 to 2009, she has been Associate Editor at Large of the IEEE Transactions on Automatic Control. Since 1995 she is Subject Editor of the International Journal of Robust and Nonlinear Control. Since 2015, she is Editorial Board Member of the Annual Reviews in Control. From 2016 she is Associate Editor of the IFAC Journal Nonlinear Analysis: Hybrid Systems. Maria Domenica Di Benedetto is the PI and Director of the Center of Excellence for Research DEWS "Architectures and Design methodologies for Embedded controllers, Wireless interconnect and System-on-Chip", a member of the Technology District of the Abruzzo Region. Her research interests are centered about analysis and control of hybrid systems and networked control.