Resilient Control in Cyber-Physical Systems

Countering Uncertainty, Constraints, and Adversarial Behavior

Other titles in Foundations and Trends® in Systems and Control

On the Control of Multi-Agent Systems: A Survey
Fei Chen and Wei Ren
ISBN: 978-1-68083-582-3

Analysis and Synthesis of Reset Control Systems
Christophe Prieur, Isabelle Queinnec, Sophie Tarbouriech and Luca Zaccarian
ISBN: 978-1-68083-522-9

Control and State Estimation for Max-Plus Linear Systems
Laurent Hardouin, Bertrand Cottenceau, Ying Shang and Jorg Raisch
ISBN: 978-1-68083-544-1

Resilient Control in Cyber-Physical Systems

Countering Uncertainty, Constraints, and Adversarial Behavior

Sean Weerakkody
Carnegie Mellon University
sweerakk@andrew.cmu.edu

Omur Ozel
George Washington University
ozel@gwu.edu

Yilin Mo
Tsinghua University
ylmo@tsinghua.edu.cn

Bruno Sinopoli
Carnegie Mellon University
brunos@andrew.cmu.edu

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Systems and Control

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

S. Weerakkody and O. Ozel and Y. Mo and B. Sinopoli. *Resilient Control in Cyber-Physical Systems*. Foundations and Trends® in Systems and Control, vol. 7, no. 1-2, pp. 1–252, 2020.

ISBN: 978-1-68083-586-1

Foundations and Trends® in Systems and Control

Volume 7, Issue 1-2, 2020

Editorial Scope

Topics

Foundations and Trends® in Systems and Control publishes survey and tutorial articles in the following topics:

- Control of:
  - Hybrid and Discrete Event Systems
  - Nonlinear Systems
  - Network Systems
  - Stochastic Systems
  - Multi-agent Systems
  - Distributed Parameter Systems
  - Delay Systems
- Filtering, Estimation, Identification
- Optimal Control
- Systems Theory
- Control Applications

Information for Librarians

Foundations and Trends® in Systems and Control, 2020, Volume 7, 4 issues. ISSN paper version 2325-6818. ISSN online version 2325-6826. Also available as a combined paper and online subscription.

Contents

Resilient Control in Cyber-Physical Systems

Sean Weerakkody [1], Omur Ozel[2], Yilin Mo[3] and Bruno Sinopoli[4]

[1] *Carnegie Mellon University; sweerakk@andrew.cmu.edu*
[2] *George Washington University; ozel@gwu.edu*
[3] *Tsinghua University; ylmo@tsinghua.edu.cn*
[4] *Carnegie Mellon University; brunos@andrew.cmu.edu*

ABSTRACT

Cyber-Physical Systems (CPS), the amalgamation of sophisticated sensing, communication, and computing technologies, applied to physical spaces, have become intrinsically linked to society's critical infrastructures. Indeed, CPS find applications in energy delivery systems, intelligent transportation, smart buildings and health care. Within these systems, technological advances have enabled mankind to improve their ability to both accurately monitor large scale systems and precisely manipulate their behavior in order to achieve complex local and global objectives. Nonetheless, the opportunities created by CPS are met with significant burdens and challenges, threatening the resilience of these systems to both benign failures and malicious attacks.

In this monograph, we provide a comprehensive survey of intelligent tools for analysis and design that take fundamental steps towards achieving resilient operation in CPS. Here, we investigate the challenges of achieving reliable control and estimation over networks, particularly in the face of uncertainty and resource constraints. Additionally, we examine the threat of bad actors, formulating realistic models

Sean Weerakkody, Omur Ozel, Yilin Mo and Bruno Sinopoli (2020), "Resilient Control in Cyber-Physical Systems", Foundations and Trends® in Systems and Control: Vol. 7, No. 1-2, pp 1–252. DOI: 10.1561/2600000018.

to characterize adversaries as well as systematic tools to detect and respond to attacks. Finally, we include a brief introduction to the problem of privacy in CPS, providing both measures to describe and techniques to preserve the confidentiality of sensitive information.

1

Introduction

Cyber-physical systems (CPS) are computationally capable systems that directly interact with a physical environment and allow people to intelligently and efficiently manage physical processes. CPS are the foundation of key infrastructures such as the smart grid, water distribution systems, and waste management. Their role in transportation, smart buildings, and medical technologies are also burgeoning as new application areas are discovered. We refer the reader to Lee (2008), Rajkumar *et al.* (2010), Poovendran (2010), Kim and Kumar (2012), and Johansson *et al.* (2014) for additional information on the reach of CPS in today's applications.

CPS are enabled by technologies which perform sensing, computing, and communication. In particular, CPS leverage sensing technologies to gather relevant data about physical systems. In transportation this could for instance be the position and velocity of vehicles. Alternatively, in medical technologies, this may be the heart rate or blood pressure of a patient. Combined with a mathematical model of a system's physical dynamics, sensing can enable accurate state estimation and prediction. This in turn allows the monitoring of physical processes. Sensing technologies have significantly improved. We can sample systems more frequently and with less delay. Additionally, sensing devices are in many cases cheap and economically viable. The availability of cheap and accurate sensing allows the designer to better understand physical processes by obtaining larger numbers of spatial and temporal samples. An example in this regard is the increased presence of phasor measurement units (PMUs) in the power grid (Abur and Exposito, 2004). We note that modern PMU technology has significantly changed the operation of the electricity grid. In particular, the high sampling rates and accuracy of voltage phasor measurements have changed state estimation from a static problem to a dynamic problem.

In addition to monitoring physical processes, it is typically desirable to physically manipulate a system to achieve some objective. In a waste management system, a relevant task would be to treat and purify the wastewater. Alternatively, in smart buildings we wish to regulate the environment (i.e. using HVAC systems) in an energy efficient manner. Cyber-physical systems allow us in many cases to automate this process using computing technologies. The intelligent control of physical systems is generally a time sensitive task. Thus, a key to incorporating CPS is improvement in the processing speed of our computers. Today, programmable logic controllers (PLCs) and microcontrollers are able to quickly process sensory information and automatically implement an intelligent algorithm for control. The speed at which this can be done has allowed humans to explore new frontiers. As an example, the ability to safely incorporate safe driving cars to transportation systems is in part a result of the vast computational abilities of the embedded systems in today's vehicles.

Finally, a sophisticated communication infrastructure allows operators to control cyber-physical systems remotely while also enabling them to reliably control large scale systems. Many systems have transitioned from wired to wireless communication technologies, which allows for ease of maintenance and installation, lower costs, as well as automation in geographically disparate systems. As an example, wireless communication technologies play a major role in supervisory control and data acquisition (SCADA) systems, see, e.g., Cardenas *et al.* (2009). A SCADA system is a hierarchical system, which enables the supervisory management of a control system. The lowest layer consists of field devices such as sensors and actuators, which directly interact with the physical environment. Remote terminal units (RTUs) and PLCs are often used to implement autonomous local control. These units typically interface with both field devices such as pumps, valves, and switches as well as a centralized supervisory control layer which monitors the system. SCADA systems are regularly seen in the smart grid as well as water distribution and waste management systems. Communication technologies allows RTUs to interface with human operators at SCADA systems in real time. This allows operators to make high level control decisions remotely in a timely fashion. This capability is especially important when monitoring at the supervisory layer raises an alarm, which requires immediate operator attention. Communication technologies not only allow devices and components to interface with central operators, but also each other. Local communication among field devices can enable distributed control. Here, autonomous controllers/agents share information and act to achieve a larger task. Distributed control can be used to achieve formations in aerial vehicles and platoons in ground transport.

Unexpected challenges arise when accounting for the tight interaction of computing elements with the physical plant in CPS. Unlike normal IT infrastructures, the operations of CPS are often safety critical (Lee, 2008; Rajkumar *et al.*, 2010; Giani *et al.*, 2008). For example, malfunctioning teleoperated robots in surgery may harm or possibly kill patients. Likewise, blackouts on the electricity grid may disrupt vital services. Thus, operators are obligated to ensure these systems perform resiliently. Complicating the matter is the time sensitive nature of CPS. To ensure that the dynamics of a physical process are well regulated, CPS must be monitored and acted upon frequently. In this monograph, we aspire to identify significant challenges, which hinder the successful operation of cyber-physical systems. To this end, we consider several proposed tools and methodologies aimed towards addressing these fundamental problems.

First, in section 2 we consider the problem of modeling CPS.In control systems, an accurate numerical representation of a plant is often a crucial component to developing intelligent algorithms for automation, with provable mathematical properties. These models can be developed from first principles. For instance, Newton's laws can be used to describe the dynamics of vehicles while Maxwell's equations can be used to derive dynamical equations associated with mathematical generators. Alternatively, we can utilize big data and in particular system identification/machine learning techniques to obtain effective models of our systems. We briefly discuss system identification in subsection 2.1. Cyber-physical systems pose a particular challenge due to the inherent diversity of the systems being considered (Derler *et al.*, 2012). They not only contain a physical plant, which needs to be modeled like a traditional control system, but also have heterogeneous hardware and software systems which enable computing and data transfer. The challenges of modeling CPS are detailed in subsection 2.2. We then look at specific classes of models. In addition to examining traditional state space, LTI, and stochastic systems in subsection 2.3, we will address modeling CPS through a brief discussion of hybrid systems in subsection 2.4.

Even with a precise and accurate model of CPS, operators must account for sources of uncertainty and how they impact subsequent analysis and design. As an example, in section 3 we will study networked control systems, focusing on achieving feedback control over stochastic, resource constrained, communication networks. While transitioning from wired to wireless communication technologies can reduce costs and improve efficiency, reliability may be sacrificed. Packets containing sensory or control data may be delayed or dropped over the communication network. In a cyber-physical system, the availability of real-time data is often essential for correct and reliable operation. Sensor packet drops leads to inadequate monitoring and feedback control. Input packet drops prevent corrective commands from being delivered to the plant. As communication failures can significantly affect the functionality of CPS, operators must carefully model and account for their presence through robust analysis and design. We will discuss the design of robust feedback controllers in CPS with sensor and input drops respectively in subsection 3.1 and 3.2. In these cases, we will additionally arrive at fundamental conditions on network reliability, which allow the aforementioned algorithms to successfully stabilize CPS.

Improvements in automation and efficiency are often cited as benefits of incorporating cyber-physical systems to our long standing infrastructures. Even then, operators must be careful to ensure the economic viability of these tasks. A traditional goal is to maximize the performance of a system subject to a constraint on available resources. For example, in subsection 3.3, we will briefly investigate resource constraints as it applies to sensors. Sensors in CPS are generally small heterogeneous devices, which are subject to power constraints, bandwidth constraints, and topology constraints. We will consider problems of sensor scheduling and event triggered estimation with the objective of maximizing system performance while meeting these constraints. In addition to event triggered estimation, in subsection 3.4, we will explore the dual problem of event based control.

At the heart of this monograph, in section 4, we will consider the security of cyber-physical systems. While it is important to achieve resilience to systematic and benign failures, which for instance can occur due to operator error, normal wear and tear, or environmental conditions, the bulk of our attention will be placed on malicious adversarial scenarios. As cyber-physical systems are intrinsically linked to our critical infrastructures, there exist ample motivation to target them. Attacks on transportation CPS can lead to car accidents while attacks on CPS associated with water treatment and management could damage the environment or contaminate the water supply. Additionally, attacks on the grid can disrupt vital services due to blackouts and attacks on medical CPS can cause injury or even death to patients.

Next generation cyber-physical systems also create opportunities for adversaries. Introducing wireless technologies into control systems allow remote attackers to perform man in the middle attacks. Moreover, the incorporation of heterogeneous subsystems and components provides numerous attack surfaces for adversaries. The internet of things (IoT), creates additional advantages for an attacker. CPS which leverage the IoT utilize existing (and possibly insecure) networking infrastructures, particularly the internet, to enable communication and remote processing (for instance through cloud computing). Finally, there exists precedence for attacks. Perhaps, the best known attack on a cyber-physical system is the Stuxnet attack, which was a malicious worm which targeted uranium enrichment facilities in Iran and was able to disable approximately one thousand centrifuges (Langner, 2011). In subsection 4.1, we go into deeper detail regarding the motivation for studying cyber-physical system security.

Next, in subsection 4.2, we will discuss common adversarial models in CPS, describing potential attacker's in terms of their knowledge, capabilities, and potential strategies. Here, we pay special attention to stealthy attack strategies, which allow an attacker to act on a system without being recognized, thus eliminating reactive defensive countermeasures. After, we describe potential mechanisms for achieving security in CPS. The ultimate goal is for the system to remain operational, even in the presence of an attacker. We argue the first step of this process is detection. As an example, in subsection 4.3, we will evaluate how sensor and link placement can be used structurally to ensure properties of attack detectability and identifiability. Additionally, in subsection 4.4, we will introduce tools for active detection, which enable operators to recognize and isolate classes of harmful and stealthy attacks, by intelligently perturbing the system.

Beyond detection, we wish to recover from and resiliently respond to attacks on our control system so that we can achieve graceful degradation of system performance under attack. We remark that directly designing resilient control laws to counter attacks is application dependent. Instead, we argue that a necessary step to achieve desirable system performance in the presence of an attacker is to perform resilient state estimation, the subject of subsection 4.5. Indeed, resilient state estimation allows a remote defender to maintain understanding of the system state under attack, even when a subset of inputs and outputs are compromised. This ability to perform resilient estimation in turn enables resilient control. Specifically, a defender can incorporate reliable state information when designing appropriate countermeasures (including a resilient feedback control law) to remedy a cyber-physical system.

Finally, as noted in the title of this monograph, we aim to counter adversarial behavior in CPS. While section 4 considers methods to counter attacks which actively affect the operations of a control system, passive adversaries in a CPS can also cause significant harm to society. In particular, in the age of big data, copious amounts of information, much of which can be sensitive, is used to efficiently and effectively control CPS. For instance, power consumption data aids in demand prediction, transportation data reveals information about traffic patterns, and medical information can enable preventive treatments. However, in the wrong hands this type of data can reveal sensitive information about a user's routines, travel habits, and preexisting conditions. As a result, in order to truly consider the impact of adversarial behavior in CPS, we argue that one must also pay close attention to notions of privacy. An introduction to some concepts in privacy is given in section 5. Here, we wish to provide some intuition about how important and useful data can be leveraged in a CPS without leaving citizens and users vulnerable to the actions of a passive, information collecting, attacker. To begin, we consider data privacy in subsection 5.1. We will discuss notions of differential privacy and inference privacy. In this respect, we will consider the problem of average consensus and discuss mechanisms that achieve these notions of privacy in subsection 5.2. Finally, in subsection 5.3, we will give a brief overview of cryptography based privacy.

We remark that this is far from the only monograph to examine cyber-physical systems. To date dozens of books on CPS have been published. Many of these texts are for more detailed in their discussion of applications, modeling, and specific architectures. Additionally, while not a focus of this monograph, several books have studied concepts of verification and validation in CPS. The main contribution of this text relative to most other works is the highly mathematical, model aware approach it takes to analysis and design when dealing with problems of robust and resilient control in CPS. Our aim is to provide readers with an introduction to challenges in this arena and discuss the basic tools that have been used to address these problems. Of course, not all concepts in resilient cyber-physical systems can be covered in this text. However, to aid the interested reader, several further reading subsections have been included to provide additional pointers to applicable and related research.

In the rest of this section, we discuss several applications of CPS in moderate detail. Here, we will emphasize application specific problems that highlight challenges for ensuring resilience in CPS.

1.1 Applications

In this subsection, we discuss several applications of cyber-physical systems, specifically the smart grid/energy management systems, medical technologies, transportation, and water treatment/distribution. While a comprehensive analysis of each infrastructure is out of scope, we aim to highlight the role cyber-physical technologies play in these systems and summarize key challenges which can threaten resilience.

1.1.1 Smart Grid and Energy Management CPS

The electric grid is a massive infrastructure, composed of a variety of subsystems with different owners and a diverse range of regulators. This large and complex system is inevitably prone to key challenges and vulnerabilities. This includes withstanding the failure of components and transmission lines, matching generation to demand, and preserving the environment.

The development of a smart grid in particular aims to address the major challenges and inefficiencies that exist in the current infrastructure through the use of advanced information, computing, and communication technologies, smarter devices, and economically viable renewable resources (Farhangi, 2010; Amin and Wollenberg, 2005; Fang *et al.*, 2012). For instance, the introduction of an advanced metering infrastructure (Mohassel *et al.*, 2014) and dynamic pricing will enable demand response (Albadi and El-Saadany, 2008). This along with distributed generation can reduce the cost of electricity for consumers as well as decrease peak demand. Additionally, the widespread use of phasor measurement units (PMUs) allows for wide area monitoring via dynamic state estimation as well as automatic control to improve real time efficiency. Furthermore, increased information and better predictive tools will help society in leveraging clean renewable resources such as wind and solar power. The smart grid is a preeminent example of a CPS where generation, transmission, and distribution subsystems comprise the physical system, while sensors collecting data, networks routing data, and computers processing data constitute the cyber system.

At a smaller scale, we consider energy management systems in buildings. Kleissl and Agarwal (2010) note that 70% of our total energy consumption is spent in buildings, which also generate 40% of greenhouse gases. Hence the application of information and communication technologies to achieve smart buildings has significant potential. Modern buildings could be viewed as cyber-physical systems that consist of heat control, water distribution, airflow, and security subsystems interacting closely via the usage of embedded sensing and control systems. Kleissl and Agarwal (2010) in particular examine opportunities to optimize energy consumption by both occupants and information processing equipment and provides recommendations for buildings to achieve zero net energy usage. The role of humans, especially in residential buildings can not be underestimated. Information technologies can allow humans to make better decisions in smart buildings. For instance Aksanli and Rosing (2017), after obtaining a model to capture the relationship between activities of residents in a house and total power consumption, use a human-behavior-centric scheduling method to achieve significant energy savings and peak demand reduction in residential CPS.

As an aside, cyber-physical technologies play an important role in managing energy usage in data centers. Data centers have shown rapid growth in energy consumption (Koomey, 2011). With data collection and storage only increasing, special care must be taken to efficiently manage electricity usage in data centers. Parolini *et al.* (2012) considers the problem of energy management in data centers using a cyber-physical system approach. In particular, the authors provide a coordinated strategy leveraging cooling and information technologies to achieve both energy efficiency and a high quality of service.

Unfortunately their exists ample motivation for attackers to target the smart grid. First, there exists economic benefits for potential attackers. On one hand, an adversary can physically tamper with smart meters in order to reduce electricity bills. Alternatively, attacker's who participate in the electricity market can elicit a profit by intelligently compromising sensor measurements (Xie *et al.*, 2010). Attackers may also perturb the grid as a prank or for far more nefarious reasons including terrorism. In particular, an attacker targeting the smart grid will affect critical life-saving resources.

There exists a precedent for attacks on the grid, perhaps most notably the attack on the Ukraine power grid in 2015 (Pultarova, 2016). Here, hackers were able to deliver the BlackEnergy3 malware to a SCADA system operating the grid months before commencing a physical attack. The attackers were able to harvest valid credentials and perform reconnaissance to ascertain appropriate targets. Finally, on December 23, 2015, attackers remotely carried out an attack on the grid, tripping breakers and blocking remote access from system operators. As a result tens of thousands of customers lost power over a period of several hours. The attackers also performed a telephone denial of service to cut off communication between consumers and providers and used the KillDisk malware to destroy data.

Mo *et al.* (2012a) mention confidentiality and privacy as another relevent issue that arises due to the use of information technologies. Energy use information stored in smart meters can leak personal information about consumer habits and activities (McDaniel and McLaughlin, 2009). For instance, it is possible to intuit general information such as when a user is at home or awake or even very specific information, such as when a consumer is watching television. As many consumers consider this information to be sensitive, we observe a critical tradeoff between the benefits provided by data collection (improved demand prediction, efficient use of resources), and the resulting loss in privacy (Le Ny and Pappas, 2014). Differentially private filtering as discussed by Le Ny and Pappas (2014) can help to address such tradeoffs by aggregating data in a manner which provides strong privacy guarantees.

1.1.2 Medical CPS

Cyber-physical technologies have had a direct impact on medical systems. The management and operation of medical cyber-physical systems have been positively influenced by miniaturized sensing implants and actuating platforms, energy harvesting, in-body and on-body networks and new fabrication methods such as 3D printing. Additionally, improvements in communication and computing allow autonomous coordination of medical devices, both microscopically via nanorobots and macroscopically in the operating room. Precise control also has enabled new methods for device placement and drug delivery. We expand upon these topics below.

Traditionally, intelligent sensing and actuation has found applications in scenarios that involve wearable devices and implantable devices such as pacemakers and defibrillators. In particular, mobile monitoring of vital signals and physical activities obviate the need of doctors to be physically present to diagnose the health of individual patients. Schirner *et al.* (2013) suggests that embedded sensors which measure human cognitive activity are enablers of human in the loop CPS. Specifically, the development of human and machine interfaces can improve interactions with assistive robots, which perform actions for the benefit of a person with a disability and allow for enhancements in intelligent prostheses, restoring function to amputees.

Similarly, there is now also growing interest towards in-body and on-body sensor networks that can measure activity and athletic performance based on body state indicators such as heart and breathing rate, blood-sugar level and skin temperature. In this respect, developing energy harvesting technologies (such as RF energy harvesting or thermoelectric energy harvesting using body heat) enable battery free operation and ease of implementation in various types of body sensor applications. RF energy harvesting is a well known technique for increasing the lifetime of implantable devices (Ho *et al.*, 2014). In addition, thermoelectric generators, kinetic harvesters and solar technology are also being used in body sensor networks to harvest energy in wireless bio-sensor devices (Mitcheson, 2010).

It is argued by Lee and Sokolsky (2010) that monitoring and control in medicine could greatly benefit from newly developed cyber-physical technologies. Real time embedded closed-loop control could facilitate immediate diagnostic evaluation of vital signals and make constant care possible. For example, Lee and Sokolsky (2010) discuss how intelligent coordination between x-ray machines and ventilators during an operation can save patient lives. Specifically, to currently obtain good images (without patient motion) during an operation, a ventilator must be paused, thus preventing lung movement. However, patients have died in cases where the ventilator would not restart. An intelligent alternative involving precise control would be to enable automatic coordination between the x-ray and the ventilator. The x-ray would take images when it detects the end of a breathing cycle. As a result, the ventilator does not need to be turned off.

Additionally, the use of computing, sensing, and communication technologies can reduce humans erros. Cyber-physical technologies promise to minimize human mistakes by automating various medical tasks both in clinical scenarios and operation room practice. For instance, Lee and Sokolsky (2010) consider patient-controlled analgesia and argues that it can benefit from feedback control. In this process, infusion pumps are commonly used to deliver opioids for pain management before and after surgery. Current technological safeguards suchs as drug libraries and programmable limits can be insufficient in safely addressing pain management. The authors propose a closed-loop control system with a supervisor to monitor patient data for the early signs of respiratory failure. The automated supervisor can stop infusions and sound an alarm in case of an adverse event. We also remark the role of nanorobots in the development of new drug delivery methods, see, e.g., Douglas *et al.* (2012). This technology promises to deliver drugs to a targeted region in the body and hence minimize the risks and possible side effects caused by its use.

Unfortunately, without proper care, cyber physical technologies can negatively impact the security and reliability of medical devices. First, medical devices may be subject to a significant failure risk with potentially catastrophic impacts on patients. Alemzadeh *et al.* (2012) argue that faulty monitoring devices could cause serious injury and death. An over reliance on autonomous monitoring and treatment in a faulty scenario could result in harm to a patient, which could have otherwise been prevented with a doctor in the loop. In addition, the dependence of cyber-physical systems on information technology make them more vulnerable to cyber attacks. Alemzadeh *et al.* (2013) report that teleoperated robots are vulnerable to malicious adversaries. In particular, this work considers attackers who install malware to strategically affect robots during surgery. To detect and mitigate such attacks, Alemzadeh *et al.* (2013) devises a model-based analysis framework using the dynamics of the surgical robot. This framework is utilized to determine if a command is trustworthy before execution.

An enhanced information technology infrastructure also creates significant privacy concerns. Patients often wish to keep medical information private often due to a perceived stigma associated with various health conditions. A release of such information can violate the trust patients have in medical professionals and the system as a whole. As such, the privacy of an individuals mental/physical health along with the treatment they receive is mandated by law through the Health Insurance Portability and Accountability Act (HIPPA). Unfortunately, increased data collection in next generation and state of the art medical systems have made personal medical information more vulnerable. The research community has been active in attempting to prevent medical information from leaking. As an example, Kocabas *et al.* (2016) provides a detailed survey of encryption schemes to enable privacy at data collection, data aggregation, cloud storage, and action layers of medical CPS.

1.1.3 Transportation related CPS

Transportation infrastructures, including both terrestrial and aerial systems have been heavily influenced by CPS. Most obviously, improvements in embedded sensing and control have allowed self driving cars and unmanned aircrafts to surface. In addition, advanced wireless communication methods made in-vehicle and vehicle-to-vehicle coordination possible. This enhanced networking along with improvements in cloud computing and cellular wireless technologies has opened up the possibility of intelligent city wide and highway traffic control. With global travel now a common necessity, the problem of intelligent aerial traffic management has become increasingly important. On a smaller scale, as advances are being made in drone technology, city wide aerial traffic control may also pose a significant challenge.

Qu *et al.* (2010) argue that cyber-physical technologies have created opportunities for intelligent transportation systems which reduce traffic, improve safety, and increase sustainability. The authors envision a unified platform which integrates pedestrians, vehicles, roadside infrastructures, traffic management centers, sensors, and satellites to achieve safety and efficiency. Noting the capability of wireless communication technology to transfer information rapidly in mobile systems, Qu *et al.* (2010) analyze several candidate technologies for intra-vehicle communication as well as vehicle-to-vehicle and vehicle-to-infrastructure communication. Additionally, the future of transportation faces the challenge of integrating self-driving cars to traditional traffic. Self-driving vehicles leverage precise sensing technologies such light detection and radar (LIDAR) and GPS/INS and intelligent algorithms which perform simultaneous localization and mapping (SLAM) (Wolcott and Eustice, 2014). Autonomous vehicles have the potential to improve safety and increase efficiency.

Work and Bayen (2008) consider the role of mobile phones in the way transportation CPS is evolving. It is argued in Work and Bayen (2008) that cell phones can be used as traffic sensors in dynamic environments. The utility of mobile devices is propelled by their ubiquity, built infrastructure, and diverse capabilities. In particular, visualization and computation platforms in cellphones enable crucial feedback in the operation of transportation CPS. In Work *et al.* (2008), automotive CPS are considered and in-vehicle and among vehicles data collection and processing opportunities are set forth including forms of social networking and environmental monitoring. Possible benefits expected to be gained by such integration opportunities, including more energy efficient and human-centric operation, which remove a human from information acquisition tasks and leave them with higher lever decisions.

Sampigethaya and Poovendran (2013) propose an aviation CPS framework consisting of aircrafts, passengers, air traffic management, and airports. The authors observe that advances and innovations recorded in aviation design, flight operation, and airport management, which mainly rely on information and computational capabilities on the ground and during flight, will enable a new frontier for this infrastructure. As an example, aircrafts are beginning to employ integrated modular avionics (IMA)-based architecture, which yield software systems with lower power consumption and higher integration. Moreover, coupling higher level flight management systems with flight control enables route optimization in the presence of uncertainty and constraints while providing decision support for pilots. Improvements in air traffic management will improve air-to-ground interactions. For instance weather information can be collected by an aircraft, processed on the ground, and delivered to other planes which will travel through the same airspace. Tactical decisions can be made by the pilots of these aircrafts accordingly. Finally, at airports, cyber-physical technologies will improve surface operations, turnaround time at gates, and passage/baggage flow.

The resilience of transportation systems to failures and attacks is critical for the safety of the public. To achieve widespread adoption of next generation technologies (for instance autonomous vehicles that leverage both vehicle to vehicle and vehicle to infrastructure communication), resilient architectures must be developed which can withstand benign faults as well as malicious attacks. To investigate this matter further, we consider the example of vehicular platoons. In a vehicle platoon, several closely spaced vehicles follow a leader. The vehicles leverage radar technology and (in certain cases) vehicle to vehicle communication to share relative distances and velocities, as well as planned accelerations. By autonomously reducing inter-vehicle distance and relative velocities, platoons increase throughput and save fuel.

Nonetheless, platoons are vulnerable to attacks. Amoozadeh *et al.* (2015) notes that messages between vehicles can be falsified, spoofed or replayed by attackers while jamming attacks can disrupt communication entirely. System level attacks can also tamper with vehicle hardware or software. This can be done both at the manufacturing state or remotely (Miller and Valasek, 2015). Gerdes *et al.* (2013) demonstrates how such attacks can be subtly used to increase energy expenditures of vehicles from anywhere between $20 - 300\%$. More malicious adversaries can use control of a single vehicle to manipulate the actions of all other vehicles in a stream and destabilize a platoon (Dadras *et al.*, 2015). DeBruhl *et al.* (2015) for instance demonstrates a particularly powerful attack where a vehicle communicates that it is going to accelerate to the vehicle behind it, only to brake suddenly. The authors demonstrate that careful model-based detection and control schemes are needed to detect and respond to such an attack safely while simultaneously benefiting from the typical advantages of platooning in the absence of an attack.

The privacy of location data has been frequently emphasized in the context of transportation CPS (Qu *et al.*, 2010; Work and Bayen, 2008; Work *et al.*, 2008; Sampigethaya and Poovendran, 2013; Amoozadeh *et al.*, 2015; Hoh *et al.*, 2006). Hoh *et al.* (2006) for instance notes that location monitoring services in next generation traffic systems can allow drivers to be be tracked. Privacy can be corrupted by eavesdroppers on the network, attackers who install spyware, or malicious insiders with access to a traffic monitoring server. Significant information can be gleaned from tracking a user. As noted by Hoh *et al.* (2006) , one can learn about the health of a driver if they frequently visit a doctor/specialist or political leanings from visits to activist organizations. Perhaps more worrisome is the home identification of particular drivers. As such, the privacy of transportation data requires significant attention.

1.1.4 Water Based CPS

Sewage or wastewater treatment allows communities to remove contaminants from wastewater, enabling this water to be returned to nature with minimal environmental consequence or in some cases, be reused. A cyber-physical approach to water treatment improves automation in this system (Department-of-Homeland-Security, 2015). Enhanced sensing and monitoring will allow operators to anticipate failures and thus increase reliability. Moreover, it will enable real time feedback control at collection stations and pumping stations. As an example, intelligent sensing and control can be utilized to monitor and finely tune the environment of rotating biological contactors. Rotating biological contactors consist of bacteria which can break down contaminants in water, but require very specific environmental conditions (which can be managed by SCADA systems) to function properly. Additionally, Konig *et al.* (2015) discuss how SCADA and IoT based technologies will allow cities to implement decentralized wastewater treatment, an initiative which will significantly reduce energy consumption, decrease long term costs, and increase the recycling of water.

Water distribution has also benefited from improvements in sensing, computing, and control (Mutchek and Williams, 2014). Smart water meters can monitor real time pressure and flow. This enables these sensors to automatically detect costly leaks/breakages. Moreover, smart meters enable consumers to control their water habits in much the way that demand response has been considered in the smart grid. This can be highly useful during droughts. Contamination sensors can additionally be used detect impurities, which decay the quality of water. In addition smart valves and pumps can control the flow of water in response to environmental conditions. For instance, smart valves can reduce harmful fluctuations in water pressure (Mistry, 2011) and isolate contaminated water while smart pumps can detect and respond to clogs in pipes.

The resilience of smart water technologies, however, has been brought to question. For instance, Amin *et al.* (2013) discuss relevant adversarial models against an automated canal system. The authors also perform tests on the Gignac canal system to demonstrate the effectiveness of potential attacks. These attacks can occur at various levels of a hierarchical SCADA system. For instance, attacks may occur on the physical infrastructure, the regulatory control layer (which interacts with the canal network through sensing and actuation devices), the communication network, the supervisory control layer (which performs tasks such state estimation/fault diagnosis/selection of control parameters), or the corporate network. In water distribution systems, Laszka *et al.* (2017) considers a cyber-physical attack model where the attacker introduces contaminants into the water supply and disables a subset of sensors. The authors recommend that operators intelligently add redundant sensors, introduce diverse sensing devices, and increase device security to achieve resilience.

The examination of the resilience of water based CPS has been in part motivated by a precedent for attacks. Most notably, one can consider the Maroochy Shire incident (Slay and Miller, 2007; Abrams and Weiss, 2008) an attack on a sewage treatment SCADA system in Queensland, Australia. The system contained 142 pumping stations monitored by two monitoring workstations. Radio communication was enabled between pumping stations and central computers. An attack on this system was carried out by a disgruntled former employee over a period of 2 months in the year 2000. The attack, which was done remotely using a laptop and radio transmitter, led to communication failures among the pumping stations and the central computer, unexpected pump behavior, and a malfunctioning alarm system. Moreover, as a result of the attack, 800,000 liters of raw sewage spilled into the community. The attack demonstrated the power of a malicious insider. Moreover, it revealed the vulnerability of remote control and sensing technologies when they are used without adequate security defenses.

Privacy must also be accounted for in water distribution systems. While water consumption may not release as much sensitive information about users as electricity consumption, there exist avenues for adversary's to learn about the user. For instance Rottondi and Verticale (2016) discuss how information can be leaked in gaming scenarios where users are incentivized by operators to alter their water consumption habits. In particular, it is argued that game actions can be related to physical, social, and mental characteristics of the user. Thus, while cyber-physical technologies such as smart water meters provide operators the ability to increase efficiency by influencing resource consumption, collecting the necessary data raises significant privacy concerns.

References

Abrams, M. and J. Weiss. 2008. “Malicious control system cyber security attack case study–Maroochy Water Services, Australia”. *McLean, VA: The MITRE Corporation.*

Abur, A. and A. G. Exposito. 2004. *Power system state estimation: theory and implementation*. CRC press.

Aksanli, B. and T. S. Rosing. 2017. “Human Behavior Aware Energy Management in Residential Cyber-Physical Systems”. *IEEE Transactions on Emerging Topics in Computing*. PP(99): 1–1.

Albadi, M. H. and E. El-Saadany. 2008. “A summary of demand response in electricity markets”. *Electric Power Systems Research*. 78(11): 1989–1996.

Alemzadeh, H., C. D. Martino, Z. Jin, Z. T. Kalbarczyk, and R. K. Iyer. 2012. “Towards resiliency in embedded medical monitoring devices”. In: *Workshops of International Conference on Dependable Systems and Networks*. IEEE/IFIP. 1–6.

Alemzadeh, H., K. Ravishankar, Z. Kalbarczyk, and J. Raman. 2013. “Analysis of Safety-Critical Computer Failures in Medical Devices”. *Security & Privacy*. 11(4): 14–26.

Amin, S. M. and B. F. Wollenberg. 2005. “Toward a smart grid: power delivery for the 21st century”. *IEEE Power and Energy Magazine*. 3(5): 34–41.

Amin, S., A. A. Cárdenas, and S. Sastry. 2009. "Safe and Secure Networked Control Systems under Denial-of-Service Attacks". In: *International Workshop on Hybrid Systems: Computation and Control*. Vol. 5469. Springer. 31–45.

Amin, S., X. Litrico, S. Sastry, and A. M. Bayen. 2013. "Cyber security of water SCADA systems – Part I: Analysis and experimentation of stealthy deception attacks". *IEEE Transactions on Control Systems Technology*. 21(5): 1963–1970.

Amoozadeh, M., A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt. 2015. "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving". *IEEE Communications Magazine*. 53(6): 126–132.

Anta, A. and P. Tabuada. 2010. "To sample or not to sample: Self-triggered control for nonlinear systems". *IEEE Transactions on Automatic Control*. 55(9): 2030–2042.

Arulampalam, M. S., S. Maskell, N. Gordon, and T. Clapp. 2002. "A Tutorial on Particle Filters for Online Nonlinear/Non-Gaussian Bayesian Tracking". *IEEE Transactions on Signal Processing*. 50(2): 174–188.

Bai, C. Z., V. Gupta, and F. Pasqualetti. 2017a. "On Kalman Filtering with Compromised Sensors: Attack Stealthiness and Performance Bounds". *IEEE Transactions on Automatic Control*. 62(12): 6641–6648.

Bai, C. Z., F. Pasqualetti, and V. Gupta. 2015. "Security in stochastic control systems: Fundamental limitations and performance bounds". In: *American Control Conference*. IEEE. 195–200.

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

Bi, S. and Y. J. Zhang. 2014. "Graphical methods for defense against false-data injection attacks on power system state estimation". *IEEE Transactions on Smart Grid*. 5(3): 1216–1227.

Bobba, R. B., K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye. 2010. "Detecting false data injection attacks on DC state estimation". In: *Workshop on Secure Control Systems, CPSWEEK*.

Borgers, D. P. and M. W. Heemels. 2014. "Stability Analysis of Large-scale Networked Control Systems with Local Networks: A Hybrid Small-gain Approach". In: *International Conference on Hybrid Systems: Computation and Control*. ACM.

Boukhobza, T. and F. Hamelin. 2009. "State and input observability recovering by additional sensor implementation: A graph-theoretic approach". *Automatica*. 45(7): 1737–1742.

Boukhobza, T., F. Hamelin, and S. Martinez-Martinez. 2007. "State and input observability for structured linear systems: A graph-theoretic approach". *Automatica*. 43(7): 1204–1210.

Branicky, M. S., V. S. Borkar, and S. K. Mitter. 1998. "A unified framework for hybrid control: model and optimal control theory". *IEEE Transactions on Automatic Control*. 43(1): 31–45.

Candès, E. J., M. B. Wakin, and S. P. Boyd. 2008. "Enhancing Sparsity by Reweighted L1 Minimization". *Journal of Fourier Analysis and Applications*. 14(5-6): 877–905.

Cardenas, A. A., T. Roosta, and S. Sastry. 2009. "Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems". *Ad Hoc Networks*. 7(8): 1434–1447.

Censi, A. 2009. "On the performance of Kalman filtering with intermittent observations: A geometric approach with fractals". In: *American Control Conference*. IEEE. 3806–3812.

Censi, A. 2011. "Kalman Filtering With Intermittent Observations: Convergence for Semi-Markov Chains and an Intrinsic Performance Measure". *IEEE Transactions on Automatic Control*. 56(2): 376–381.

Chabukswar, R., Y. Mo, and B. Sinopoli. 2011. "Detecting Integrity Attacks on SCADA Systems". In: *IFAC World Congress*. 11239–11244.

Chaojun, G., P. Jirutitijaroen, and M. Motani. 2015. "Detecting false data injection attacks in AC state estimation". *IEEE Transactions on Smart Grid*. 6(5): 2476–2483.

Chen, Y., S. Kar, and J. M. F. Moura. 2017a. "Optimal Attack Strategies Subject to Detection Constraints Against Cyber-Physical Systems". *IEEE Transactions on Control of Network Systems*. PP(99): 1–1.

Chen, Y., S. Kar, and J. M. Moura. 2017b. "Dynamic attack detection in cyber-physical systems with side initial state information". *IEEE Transactions on Automatic Control*. 62(9): 4618–4624.

Chong, M. S., M. Wakaiki, and J. P. Hespanha. 2015. "Observability of linear systems under adversarial attacks". In: *American Control Conference*. IEEE. 2439–2444.

Cortes, J., G. E. Dullerud, S. Han, J. L. Ny, S. Mitra, and G. J. Pappas. 2016. "Differential privacy in control and network systems". In: *Conference on Decision and Control*. IEEE. 4252–4272.

Dadras, S., R. M. Gerdes, and R. Sharma. 2015. "Vehicular platooning in an adversarial environment". In: *Symposium on Information, Computer and Communications Security*. ACM. 167–178.

Dahleh, M. and I. J. Diaz-Bobillo. 1994. *Control of Uncertain Systems: A Linear Programming Approach*. Prentice-Hall, Inc.

Damgård, I., V. Pastro, N. Smart, and S. Zakarias. 2012. "Multiparty Computation from Somewhat Homomorphic Encryption". In: Springer, Berlin, Heidelberg. 643–662.

Davare, A., D. Densmore, L. Guo, R. Passerone, A. L. Sangiovanni-Vincentelli, A. Simalatsar, and Q. Zhu. 2013. "metroII: A design environment for cyber-physical systems". *ACM Transactions on Embedded Computing Systems*. 12(1s): 49.

DeBruhl, B., S. Weerakkody, B. Sinopoli, and P. Tague. 2015. "Is your commute driving you crazy?: A study of misbehavior in vehicular platoons". In: *Conference on Security & Privacy in Wireless and Mobile Networks*. ACM. 22:1–22:11.

Denning, D. E. 1976. "A lattice model of secure information flow". *Communications of the ACM*. 19(5): 236–243.

Department-of-Homeland-Security. 2015. "The future of smart cities: cyber-physical infrastructural risk". *Tech. rep.* Department of Homeland Security.

Derler, P., E. A. Lee, and A. S. Vincentelli. 2012. "Modeling Cyber-Physical Systems". *Proceedings of the IEEE*. 100(1): 13–28.

Dimarogonas, D. V., E. Frazzoli, and K. H. Johansson. 2012. "Distributed event-triggered control for multi-agent systems". *IEEE Transactions on Automatic Control*. 57(5): 1291–1297.

Dinic, E. A. 1970. "An algorithm for the solution of the max-flow problem with the polynomial estimation". *Doklady Akademii Nauk.* 194(4): 1277–1280.

Dion, J.-M., C. Commault, and J. Van Der Woude. 2003. "Generic properties and control of linear structured systems: a survey". *Automatica.* 39(7): 1125–1144.

Donkers, M. and W. Heemels. 2012. "Output-Based Event-Triggered Control With Guaranteed $\mathcal{L}_\infty$-Gain and Improved and Decentralized Event-Triggering". *IEEE Transactions on Automatic Control.* 57(6): 1362–1376.

Douglas, S. M., I. Bachelet, and G. M. Church. 2012. "A logic-gated nanorobot for targeted transport of molecular payloads". *Science.* 335(6070): 831–834.

Edwards, S. A. and E. A. Lee. 2007. "The case for the precision timed (PRET) machine". In: *Design Automation Conference.* ACM. 264–265.

Eker, J., J. W. Janneck, E. A. Lee, J. Liu, X. Liu, J. Ludvig, S. Neuendorffer, S. Sachs, and Y. Xiong. 2003. "Taming heterogeneity-the Ptolemy approach". *Proceedings of the IEEE.* 91(1): 127–144.

Eqtami, A., D. V. Dimarogonas, and K. J. Kyriakopoulos. 2010. "Event-triggered control for discrete-time systems". In: *American Control Conference.* IEEE. 4719–4724.

Even, S. and R. E. Tarjan. 1975. "Network flow and testing graph connectivity". *SIAM Journal on Computing.* 4(4): 507–518.

Fang, X., S. Misra, G. Xue, and D. Yang. 2012. "Smart Grid – The New and Improved Power Grid: A Survey". *IEEE Communications Surveys & Tutorials.* 14(4): 944–980.

Farhangi, H. 2010. "The path of the smart grid". *IEEE Power and Energy Magazine.* 8(1): 18–28.

Fawzi, H., P. Tabuada, and S. Diggavi. 2014. "Secure estimation and control for cyber-physical systems under adversarial attacks". *IEEE Transactions on Automatic Control.* 59(6): 1454–1467.

Forti, N., G. Battistelli, L. Chisci, and B. Sinopoli. 2016. "A Bayesian approach to joint attack detection and resilient state estimation". In: *Conference on Decision and Control.* IEEE. 1192–1198.

Fritzson, P. 2014. *Principles of object-oriented modeling and simulation with Modelica 3.3: A cyber-physical approach*. John Wiley & Sons.

Garcia, E. and P. J. Antsaklis. 2013. “Model-based event-triggered control for systems with quantization and time-varying network delays”. *IEEE Transactions on Automatic Control*. 58(2): 422–434.

Gentry, C. 2009. “A fully homomorphic encryption scheme”. *PhD thesis*. Stanford University. ISBN: 978-1-109-44450-6.

Gerdes, R. M., C. Winstead, and K. Heaslip. 2013. “CPS: An efficiency-motivated attack against autonomous vehicular transportation”. In: *Computer Security Applications Conference*. ACM. 99–108.

Giani, A., G. Karsai, T. Roosta, A. Shah, B. Sinopoli, and J. Wiley. 2008. “A testbed for secure and robust SCADA systems”. *ACM SIGBED Review*. 5(2): 4.

Giannakis, G. B. and E. Serpedin. 2001. “A bibliography on nonlinear system identification”. *Signal Processing*. 81(3): 533–580.

Giraldo, J., D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell. 2018. “A Survey of Physics-Based Attack Detection in Cyber-Physical Systems”. *ACM Computing Surveys (CSUR)*. 51(4): 76.

Goguen, J. A. and J. Meseguer. 1982. “Security policies and security models”. In: *IEEE Symposium on Security and Privacy*. 11–20.

Grebeck, M. 1998. “A comparison of controllers for the quadruple tank system”. *Department of Automatic Control, Lund Institute of Technology, Lund, Sweden, Tech. Rep.*

Guinaldo, M., D. V. Dimarogonas, K. H. Johansson, J. Moreno, and S. Dormido. 2011. “Distributed event-based control for interconnected linear systems”. In: *Conference on Decision and Control held jointly with the European Control Conference*. IEEE. 2553–2558.

Guinaldo, M., D. Lehmann, J. Sánchez, S. Dormido, and K. H. Johansson. 2012. “Distributed event-triggered control with network delays and packet losses”. In: *Conference on Decision and Control*. IEEE. 1–6.

Han, D., Y. Mo, J. Wu, S. Weerakkody, B. Sinopoli, and L. Shi. 2015. “Stochastic Event-Triggered Sensor Schedule for Remote State Estimation”. *IEEE Transactions on Automatic Control*. 60(10): 2661–2675.

Han, D., Y. Mo, and L. Xie. 2019. "Convex optimization based state estimation against sparse integrity attacks". *IEEE Transactions on Automatic Control*. 64(6): 2383–2395.

Han, D., J. Wu, H. Zhang, and L. Shi. 2017a. "Optimal sensor scheduling for multiple linear dynamical systems". *Automatica*. 75(Jan.): 260–270.

Han, S., U. Topcu, and G. J. Pappas. 2017b. "Differentially Private Distributed Constrained Optimization". *IEEE Transactions on Automatic Control*. 62(1): 50–64.

He, L., D. Han, X. Wang, and L. Shi. 2013. "Optimal linear state estimation over a packet-dropping network using linear temporal coding". *Automatica*. 49(4): 1075–1082.

Heemels, W. H., M. Donkers, and A. R. Teel. 2013. "Periodic event-triggered control for linear systems". *IEEE Transactions on Automatic Control*. 58(4): 847–861.

Heemels, W., K. H. Johansson, and P. Tabuada. 2012. "An introduction to event-triggered and self-triggered control". In: *Conference on Decision and Control*. IEEE. 3270–3285.

Henzinger, T., B. Horowitz, and C. Kirsch. 2001. "Giotto: A time-triggered language for embedded programming". In: *Embedded software*. Springer. 166–184.

Hespanhol, P., M. Porter, R. Vasudevan, and A. Aswani. 2017. "Dynamic Watermarking for General LTI Systems". In: *Conference on Decision and Control*. IEEE. 1834–1839.

Ho, J. S., A. J. Yeh, E. Neofytou, S. Kim, Y. Tanabe, B. Patlolla, R. E. Beygui, and A. S. Y. Poon. 2014. "Wireless power transfer to deep-tissue microimplants". *Proceedings of the National Academy of Sciences*. 111(22): 7974–7979.

Hoehn, A. and P. Zhang. 2016a. "Detection of covert attacks and zero dynamics attacks in cyber-physical systems". In: *American Control Conference*. IEEE. 302–307.

Hoehn, A. and P. Zhang. 2016b. "Detection of replay attacks in cyber-physical systems". In: *American Control Conference*. IEEE. 290–295.

Hoh, B., M. Gruteser, H. Xiong, and A. Alrabady. 2006. "Enhancing security and privacy in traffic-monitoring systems". *IEEE Pervasive Computing*. 5(4): 38–46.

Hosseini, M., T. Tanaka, and V. Gupta. 2016. "Designing optimal watermark signal for a stealthy attacker". In: *European Control Conference*. IEEE. 2258–2262.

Huang, Z., S. Mitra, and G. Dullerud. 2012. "Differentially private iterative synchronous consensus". In: *Proceedings of the 2012 ACM workshop on Privacy in the electronic society*. ACM. 81–90.

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

Jawaid, S. T. and S. L. Smith. 2015. "Submodularity and greedy algorithms in sensor scheduling for linear dynamical systems". *Automatica*. 61(Nov.): 282–288.

Johannessen, S. 2004. "Time synchronization in a local area network". *IEEE Control Systems*. 24(2): 61–69.

Johansson, K. H., G. J. Pappas, P. Tabuada, and C. J. Tomlin. 2014. "Guest Editorial Special Issue on Control of Cyber-Physical Systems". *IEEE Transactions on Automatic Control*. 59(12): 3120–3121.

Johansson, K. H. 2000. "The quadruple-tank process: A multivariable laboratory process with an adjustable zero". *IEEE Transactions on control systems technology*. 8(3): 456–465.

Joshi, S. and S. Boyd. 2009. "Sensor Selection via Convex Optimization". *IEEE Transactions on Signal Processing*. 57(2): 451–462.

Kar, S., B. Sinopoli, and J. M. F. Moura. 2012. "Kalman Filtering With Intermittent Observations: Weak Convergence to a Stationary Distribution". *IEEE Transactions on Automatic Control*. 57(2): 405–420.

Kilian, J. 1988. "Founding Cryptography on Oblivious Transfer". In: *ACM Symposium on Theory of Computing*. 20–31.

Kim, K. D. and P. R. Kumar. 2012. "Cyber-Physical Systems: A Perspective at the Centennial". *Proceedings of the IEEE*. 100: 1287–1308.

Kleissl, J. and Y. Agarwal. 2010. “Cyber-physical energy systems: Focus on smart buildings”. In: *Design Automation Conference*. ACM. 749–754.

Ko, W.-H., B. Satchidanandan, and P. Kumar. 2016. “Theory and implementation of dynamic watermarking for cybersecurity of advanced transportation systems”. In: *Conference on Communications and Network Security*. IEEE. 416–420.

Kocabas, O., T. Soyata, and M. K. Aktas. 2016. “Emerging Security Mechanisms for Medical Cyber Physical Systems”. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*. 13(3): 401–416.

Konig, M., J. Jacob, T. Kaddoura, and A. M. Farid. 2015. “The role of resource efficient decentralized waste water treatment in smart cities”. In: *International Smart Cities Conference*. IEEE. 1–5.

Koomey, J. 2011. “Growth in data center electricity use 2005 to 2010”. *A report by Analytical Press, completed at the request of The New York Times*. 9.

Kung, E., S. Dey, and L. Shi. 2017. “The Performance and Limitations of ϵ-Stealthy Attacks on Higher Order Systems”. *IEEE Transactions on Automatic Control*. 62(2): 941–947.

Kwon, C. and I. Hwang. 2017. “Reachability Analysis for Safety Assurance of Cyber-Physical Systems against Cyber Attacks”. *IEEE Transactions on Automatic Control*. PP(99): 1–1.

Kwon, C. and I. Hwang. 2016. “Recursive reachable set computation for on-line safety assessment of the Cyber-Physical System against stealthy cyber attacks”. In: *Allerton Conference on Communication, Control, and Computing*. IEEE. 1123–1128.

Langner, R. 2011. “Stuxnet: Dissecting a cyberwarfare weapon”. *IEEE Security & Privacy*. 9(3): 49–51.

Laszka, A., W. Abbas, Y. Vorobeychik, and X. Koutsoukos. 2017. “Synergic security for smart water networks: redundancy, diversity, and hardening”. In: *International Workshop on Cyber-Physical Systems for Smart Water Networks*. ACM. 21–24.

Le Ny, J. and G. J. Pappas. 2014. “Differentially private filtering”. *IEEE Transactions on Automatic Control*. 59(2): 341–354.

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

Lee, E. A. 2006. "Cyber-physical systems-are computing foundations adequate". In: *NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*. Vol. 2.

Lee, E. A. 2008. "Cyber physical systems: Design challenges". In: *International Symposium on Object Oriented Real-Time Distributed Computing*. IEEE. 363–369.

Lee, I. and O. Sokolsky. 2010. "Medical Cyber Physical Systems". In: *Design Automation Conference*. ACM/IEEE. 743–748.

Liao, J., L. Sankar, V. Y. F. Tan, and F. du Pin Calmon. 2018. "Hypothesis Testing Under Mutual Information Privacy Constraints in the High Privacy Regime". *IEEE Transactions on Information Forensics and Security*. 13(4): 1058–1071.

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

Liu, X., S. Weerakkody, and B. Sinopoli. 2016. "Sensor placement for reliable observability: a structured systems approach". In: *Conference on Decision and Control*. IEEE. 5414–5421.

Liu, X., Y. Mo, and E. Garone. 2017. "Secure Dynamic State Estimation by Decomposing Kalman Filter". *IFAC-PapersOnLine*. 50(1): 7351–7356.

Liu, Y., P. Ning, and M. K. Reiter. 2011. "False data injection attacks against state estimation in electric power grids". *ACM Transactions on Information and System Security*. 14(1): 13.

Ljung, L. 1998. *System Identification: Theory for the User*. Pearson Education.

Ljung, L., H. Hjalmarsson, and H. Ohlsson. 2011. "Four encounters with system identification". *European Journal of Control*. 17(5-6): 449–471.

Mazo, M. and P. Tabuada. 2009. "Input-to-state stability of self-triggered control systems". In: *Conference on Decision and Control*. IEEE. 928–933.

McDaniel, P. and S. McLaughlin. 2009. “Security and Privacy Challenges in the Smart Grid”. *IEEE Security Privacy*. 7(3): 75–77.

Mehra, R. 1974. “Optimal inputs for linear system identification”. *IEEE Transactions on Automatic Control*. 19(3): 192–200.

Menger, K. 1927. “Zur allgemeinen kurventheorie”. *Fundamenta Mathematicae*. 1(10): 96–115.

Miao, F., M. Pajic, and G. J. Pappas. 2013. “Stochastic game approach for replay attack detection”. In: *Conference on Decision and Control*. IEEE. 1854–1859.

Miao, F., Q. Zhu, M. Pajic, and G. J. Pappas. 2014. “Coding sensor outputs for injection attacks detection”. In: *Conference on Decision and Control*. IEEE. 5776–5781.

Miller, C. and C. Valasek. 2015. “Remote exploitation of an unaltered passenger vehicle”. *Black Hat USA*. 2015.

Mistry, P. 2011. “Pressure management to reduce water demand & leakage”. *Wide Bay Water Corporation, Australia.*

Mitcheson, P. D. 2010. “Energy harvesting for human wearable and implantable bio-sensors”. In: *International Conference on Engineering in Medicine and Biology Society*. IEEE. 3432–3436.

Mo, Y., E. Garone, and B. Sinopoli. 2014a. “On infinite-horizon sensor scheduling”. *Systems & Control Letters*. 67(May): 65–70.

Mo, Y., T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli. 2012a. “Cyber-Physical Security of a Smart Grid Infrastructure”. *Proceedings of the IEEE*. 100(1): 195–209.

Mo, Y., R. Ambrosino, and B. Sinopoli. 2011a. “Sensor selection strategies for state estimation in energy constrained wireless sensor networks”. *Automatica*. 47(7): 1330–1338.

Mo, Y., R. Chabukswar, and B. Sinopoli. 2014b. “Detecting integrity attacks on SCADA systems”. *IEEE Transactions on Control Systems Technology*. 22(4): 1396–1407.

Mo, Y., E. Garone, A. Casavola, and B. Sinopoli. 2010. “False data injection attacks against state estimation in wireless sensor networks”. In: *Conference on Decision and Control*. IEEE. 5967–5972.

Mo, Y., E. Garone, A. Casavola, and B. Sinopoli. 2011b. “Stochastic Sensor Scheduling for Energy Constrained Estimation in Multi-Hop Wireless Sensor Networks”. *IEEE Transactions on Automatic Control*. 56(10): 2489–2495.

Mo, Y., E. Garone, and B. Sinopoli. 2013. “LQG control with Markovian packet loss”. In: *European Control Conference*. IEEE. 2380–2385.

Mo, Y. and R. M. Murray. 2017. “Privacy Preserving Average Consensus”. *IEEE Transactions on Automatic Control*. 62(2): 753–765.

Mo, Y. and B. Sinopoli. 2009. “Secure control against replay attacks”. In: *Allerton Conference on Communication, Control, and Computing*. IEEE. 911–918.

Mo, Y. and B. Sinopoli. 2010. “False Data Injection Attacks in Control Systems”. In: *Workshop on Secure Control Systems*.

Mo, Y. and B. Sinopoli. 2011. “Kalman Filtering with Intermittent Observations: Critical Value for Second Order System”. *IFAC Proceedings Volumes*. 44(1): 6592–6597.

Mo, Y. and B. Sinopoli. 2012a. “Integrity attacks on cyber-physical systems”. In: *International Conference on High Confidence Networked Systems*. ACM. 47–54.

Mo, Y. and B. Sinopoli. 2012b. “Kalman filtering with intermittent observations: Tail distribution and critical value”. *IEEE Transactions on Automatic Control*. 57(3): 677–689.

Mo, Y. and B. Sinopoli. 2016. “On the performance degradation of cyber-physical systems under stealthy integrity attacks”. *IEEE Transactions on Automatic Control*. 61(9): 2618–2624.

Mo, Y., B. Sinopoli, L. Shi, and E. Garone. 2012b. “Infinite-horizon sensor scheduling for estimation over lossy networks”. In: *Conference on Decision and Control*. IEEE. 3317–3322.

Mo, Y., S. Weerakkody, and B. Sinopoli. 2015. “Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs”. *IEEE Control Systems*. 35(1): 93–109.

Mohassel, R. R., A. Fung, F. Mohammadi, and K. Raahemifar. 2014. “A survey on advanced metering infrastructure”. *International Journal of Electrical Power & Energy Systems*. 63: 473–484.

Mpitziopoulos, A., D. Gavalas, C. Konstantopoulos, and G. Pantziou. 2009. “A survey on jamming attacks and countermeasures in WSNs”. *IEEE Communications Surveys & Tutorials*. 11(4).

Mutchek, M. and E. Williams. 2014. “Moving towards sustainable and resilient smart water grids”. *Challenges*. 5(1): 123–137.

Nair, G. N., F. Fagnani, S. Zampieri, and R. J. Evans. 2007. “Feedback Control Under Data Rate Constraints: An Overview”. *Proceedings of the IEEE*. 95(1): 108–137.

Nakahira, Y. and Y. Mo. 2015. “Dynamic state estimation in the presence of compromised sensory data”. In: *Conference on Decision and Control*. IEEE. 5808–5813.

Narendra, K. S. and K. Parthasarathy. 1990. “Identification and control of dynamical systems using neural networks”. *IEEE Transactions on Neural Networks*. 1(1): 4–27.

Needham, R. M. and M. D. Schroeder. 1978. “Using encryption for authentication in large networks of computers”. *Communications of the ACM*. 21(12): 993–999.

Nelles, O. 2013. *Nonlinear system identification: from classical approaches to neural networks and fuzzy models*. Springer Science & Business Media.

Nemhauser, G. L., L. A. Wolsey, and M. L. Fisher. 1978. “An analysis of approximations for maximizing submodular set functions-I”. *Mathematical Programming*. 14(1): 265–294.

Nilsson, J. *et al.* 1998. “Real-time control systems with delays”. *Lund institute of Technology Lund, Sweden.*

Nozari, E., P. Tallapragada, and J. Cortés. 2017. “Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design”. *Automatica*. 81(July): 221–231.

Ozel, O., S. Weerakkody, and B. Sinopoli. 2017. “Physical Watermarking for Securing Cyber-Physical Systems via Packet Drop Injections”. In: *IEEE International Conference on Smart Grid Communications.*

Paillier, P. 1999. “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes”. In: *Advances in Cryptology – EUROCRYPT ’99*. Springer Berlin Heidelberg. 223–238.

Pajic, M., P. Tabuada, I. Lee, and G. J. Pappas. 2015. "Attack-resilient state estimation in the presence of noise". In: *Conference on Decision and Control*. IEEE. 5827–5832.

Pajic, M., J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas. 2014. "Robustness of attack-resilient state estimators". In: *International Conference on Cyber-Physical Systems*. ACM/IEEE. 163–174.

Paoletti, S., A. L. Juloski, G. Ferrari-Trecate, and R. Vidal. 2007. "Identification of hybrid systems a tutorial". *European Journal of Control*. 13(2-3): 242–260.

Parolini, L., B. Sinopoli, B. H. Krogh, and Z. Wang. 2012. "A Cyber-Physical Systems Approach to Data Center Modeling and Control for Energy Efficiency". *Proceedings of the IEEE*. 100(1): 254–268.

Parolini, L. 2012. "Models and Control Strategies for Data Center Energy Efficiency". *PhD thesis*. Carnegie Mellon University.

Pasqualetti, F., A. Bicchi, and F. Bullo. 2012. "Consensus Computation in Unreliable Networks: A System Theoretic Approach". *IEEE Transactions on Automatic Control*. 57(1): 90–104.

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

Pasqualetti, F., F. Dörfler, and F. Bullo. 2013. "Attack detection and identification in cyber-physical systems". *IEEE Transactions on Automatic Control*. 58(11): 2715–2729.

Peeters, B. and G. De Roeck. 1999. "Reference-based stochastic subspace identification for output-only modal analysis". *Mechanical systems and signal processing*. 13(6): 855–878.

Peng, T., C. Leckie, and K. Ramamohanarao. 2007. "Survey of network-based defense mechanisms countering the DoS and DDoS problems". *ACM Computing Surveys (CSUR)*. 39(1): 3.

Pin Calmon, F. du and N. Fawaz. 2012. "Privacy against statistical inference". In: *Allerton Conference on Communication, Control, and Computing*. IEEE. 1401–1408.

Poovendran, R. 2010. “Cyber-Physical Systems: Close Encounters Between Two Parallel Worlds [Point of View]”. *Proceedings of the IEEE*. 98(8): 1363–1366.

Pultarova, T. 2016. “Cyber security-Ukraine grid hack is wake-up call for network operators [News Briefing]”. *Engineering & Technology*. 11(1): 12–13.

Qu, F., F. Y. Wang, and L. Yang. 2010. “Intelligent transportation spaces: vehicles, traffic, communications, and beyond”. *IEEE Communications Magazine*. 48(11): 136–142.

Rajkumar, R. R., I. Lee, L. Sha, and J. Stankovic. 2010. “Cyber-physical systems: the next computing revolution”. In: *ACM Design Automation Conference*. 731–736.

Rigtorp, E. 2010. “Sensor Selection with Correlated Noise”. *PhD thesis*. KTH Royal Institute of Technology.

Rivest, R. L., A. Shamir, and L. Adleman. 1978. “A method for obtaining digital signatures and public-key cryptosystems”. *Communications of the ACM*. 21(2): 120–126.

Rottondi, C. and G. Verticale. 2016. “Enabling privacy in a gaming framework for smart electricity and water grids”. In: *IEEE International Workshop on Cyber-physical Systems for Smart Water Networks*. 25–30.

Ruan, M., H. Gao, and Y. Wang. 2019. “Secure and Privacy-Preserving Consensus”. *IEEE Transactions on Automatic Control*.

Rubio-Hernan, J., L. De Cicco, and J. Garcia-Alfaro. 2017. “On the use of watermark-based schemes to detect cyber-physical attacks”. *EURASIP Journal on Information Security*. 2017(1).

Sampigethaya, K. and R. Poovendran. 2013. “Aviation Cyber-Physical Systems: Foundations for Future Aircraft and Air Transport”. *Proceedings of the IEEE*. 101(8): 1834–1855.

Satchidanandan, B. and P. Kumar. 2017. “Dynamic Watermarking: Active Defense of Networked Cyber–Physical Systems”. *Proceedings of the IEEE*. 105(2): 219–240.

Schaeffer, S. E. 2007. “Survey: Graph Clustering”. *Comput. Sci. Rev.* 1(1): 27–64.

Schenato, L. 2008. "Optimal Estimation in Networked Control Systems Subject to Random Delay and Packet Drop". *IEEE Transactions on Automatic Control*. 53(5): 1311–1317.

Schenato, L., B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry. 2007. "Foundations of control and estimation over lossy networks". *Proceedings of the IEEE*. 95(1): 163–187.

Schirner, G., D. Erdogmus, K. Chowdhury, and T. Padir. 2013. "The Future of Human-in-the-Loop Cyber-Physical Systems". *Computer*. 46(1): 36–45.

Seyboth, G. S., D. V. Dimarogonas, and K. H. Johansson. 2013. "Event-based broadcasting for multi-agent average consensus". *Automatica*. 49(1): 245–252.

Shamaiah, M., S. Banerjee, and H. Vikalo. 2010. "Greedy sensor selection: Leveraging submodularity". In: *Conference on Decision and Control*. IEEE. 2572–2577.

Sharma, A. B., F. Ivančić, A. Niculescu-Mizil, H. Chen, and G. Jiang. 2014. "Modeling and analytics for cyber-physical systems in the age of big data". *ACM SIGMETRICS Performance Evaluation Review*. 41(4): 74–77.

Shi, E. and A. Perrig. 2004. "Designing secure sensor networks". *IEEE Wireless Communications*. 11(6): 38–43.

Shi, L., L. Xie, and R. M. Murray. 2009. "Kalman filtering over a packet-delaying network: A probabilistic approach". *Automatica*. 45(9): 2134–2140.

Shi, L. and H. Zhang. 2012. "Scheduling Two Gauss – Markov Systems: An Optimal Solution for Remote State Estimation Under Bandwidth Constraint". *IEEE Transactions on Signal Processing*. 60(4): 2038–2042.

Shoukry, Y., K. Gatsis, A. Alanwar, G. J. Pappas, S. A. Seshia, M. Srivastava, and P. Tabuada. 2016. "Privacy-aware quadratic optimization using partially homomorphic encryption". In: *Conference on Decision and Control*. IEEE. IEEE. 5053–5058.

Shoukry, Y., P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada. 2017. "Secure state estimation for cyber physical systems under sensor attacks: a satisfiability modulo theory approach". *IEEE Transactions on Automatic Control*.

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

Sinopoli, B., L. Schenato, M. Franceschetti, K. Poolla, M. I. Jordan, and S. S. Sastry. 2004. "Kalman filtering with intermittent observations". *IEEE Transactions on Automatic Control*. 49(9): 1453–1464.

Slavakis, K., G. B. Giannakis, and G. Mateos. 2014. "Modeling and optimization for big data analytics:(statistical) learning tools for our era of data deluge". *IEEE Signal Processing Magazine*. 31(5): 18–31.

Slay, J. and M. Miller. 2007. "Lessons learned from the maroochy water breach". *Critical infrastructure protection*: 73–82.

Smith, G. 2009. "On the foundations of quantitative information flow". In: *International Conference on Foundations of Software Science and Computational Structures*. Springer. 288–302.

Smith, R. S. 2015. "Covert misappropriation of networked control systems: Presenting a feedback structure". *IEEE Control Systems*. 35(1): 82–92.

Sui, T., K. You, M. Fu, and D. Marelli. 2015. "Stability of MMSE state estimators over lossy networks using linear coding". *Automatica*. 51(Jan.): 167–174.

Sun, M. and W. P. Tay. 2017. "Inference and data privacy in IoT networks". In: *IEEE International Workshop on Signal Processing Advances in Wireless Communications*. 1–5.

Sundaram, S. and C. Hadjicostis. 2011. "Distributed Function Calculation via Linear Iterative Strategies in the Presence of Malicious Agents". *IEEE Transactions on Automatic Control*. 56(7): 1495–1508.

Tabuada, P. 2007. "Event-triggered real-time scheduling of stabilizing control tasks". *IEEE Transactions on Automatic Control*. 52(9): 1680–1685.

Tan, R., V. Badrinath Krishna, D. K. Yau, and Z. Kalbarczyk. 2013. "Impact of integrity attacks on real-time pricing in smart grids". In: *Conference on Computer & Communications Security*. ACM. 439–450.

Tariq, M. U., J. Florence, and M. Wolf. 2014. “Design Specification of Cyber-Physical Systems: Towards a Domain-Specific Modeling Language based on Simulink, Eclipse Modeling Framework, and Giotto.” In: *ACESMB@ MoDELS*. 6–15.

Teixeira, A., D. Pérez, H. Sandberg, and K. H. Johansson. 2012a. “Attack models and scenarios for networked control systems”. In: *International conference on High Confidence Networked Systems*. ACM. 55–64.

Teixeira, A., I. Shames, H. Sandberg, and K. H. Johansson. 2012b. “Revealing stealthy attacks in control systems”. In: *Allerton Conference on Communication, Control, and Computing*. IEEE. 1806–1813.

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

Trentelman, H., A. A. Stoorvogel, and M. Hautus. 2012. *Control theory for linear systems*. Springer Science & Business Media.

Tsatsanis, M. K. and G. B. Giannakis. 1993. “Time-varying system identification and model validation using wavelets”. *IEEE Transactions on Signal Processing*. 41(12): 3512–3523.

Van Der Schaft, A. J. and J. M. Schumacher. 2000. *An introduction to hybrid dynamical systems*. Vol. 251.

Van der Woude, J. 1999. “The generic number of invariant zeros of a structured linear system”. *SIAM Journal on Control and Optimization*. 38(1): 1–21.

Van der Woude, J. 1991. “A graph-theoretic characterization for the rank of the transfer matrix of a structured system”. *Mathematics of Control, Signals, and Systems (MCSS)*. 4(1): 33–40.

Van Trees, H. L. 1968. *Detection Estimation and Modulation Theory*. Vol. 1. New York: Wiley.

Volpano, D., C. Irvine, and G. Smith. 1996. “A sound type system for secure flow analysis”. *Journal of Computer Security*. 4(2-3): 167–187.

Wahlberg, B., H. Hjalmarsson, and M. Annergren. 2010. “On optimal input design in system identification for control”. In: *Conference on Decision and Control*. IEEE. 5548–5553.

Wang, W., L. Ying, and J. Zhang. 2016. “On the Relation Between Identifiability, Differential Privacy, and Mutual-Information Privacy”. *IEEE Transactions on Information Theory*. 62(9): 5018–5029.

Weerakkody, S., X. Liu, and B. Sinopoli. 2017a. “Robust Structural Analysis and Design of Distributed Control Systems to Prevent Zero Dynamics Attacks”. In: *Conference on Decision and Control*. IEEE.

Weerakkody, S., X. Liu, S. H. Son, and B. Sinopoli. 2016a. “A graph theoretic characterization of perfect attackability and detection in Distributed Control Systems”. In: *American Control Conference*. IEEE. 1171–1178.

Weerakkody, S., X. Liu, S. H. Son, and B. Sinopoli. 2017b. “A Graph Theoretic Characterization of Perfect Attackability for Secure Design of Distributed Control Systems”. *IEEE Transactions on Control of Network Systems*. 4(1): 60–70.

Weerakkody, S., Y. Mo, and B. Sinopoli. 2014. “Detecting Integrity Attacks on Control Systems using Robust Physical Watermarking”. In: *Conference on Decision and Control*. IEEE. 3757–3764.

Weerakkody, S., Y. Mo, B. Sinopoli, D. Han, and L. Shi. 2016b. “Multi-Sensor Scheduling for State Estimation With Event-Based, Stochastic Triggers”. *IEEE Transactions on Automatic Control*. 61(9): 2695–2701.

Weerakkody, S., O. Ozel, P. Griffioen, and B. Sinopoli. 2017c. “Active detection for exposing intelligent attacks in control systems”. In: *Conference on Control Technology and Applications*. IEEE. 1306–1312.

Weerakkody, S., O. Ozel, and B. Sinopoli. 2017d. “A Bernoulli-Gaussian watermark design for detecting integrity attacks in control systems”. In: *Allerton Conference on Communication, Control and Computing*. IEEE.

Weerakkody, S. and B. Sinopoli. 2015. “Detecting integrity attacks on control systems using a moving target approach”. In: *Conference on Decision and Control*. IEEE. 5820–5826.

Weerakkody, S. and B. Sinopoli. 2016. “A moving target approach for identifying malicious sensors in control systems”. In: *Allerton Conference on Communication, Control, and Computing*. IEEE. 1149–1156.

Weerakkody, S., B. Sinopoli, S. Kar, and A. Datta. 2016c. “Information flow for security in control systems”. In: *Conference on Decision and Control*. IEEE. 5065–5072.

Wolcott, R. W. and R. M. Eustice. 2014. “Visual localization within LIDAR maps for automated urban driving”. In: *International Conference on Intelligent Robots and Systems*. IEEE. 176–183.

Work, D. and A. Bayen. 2008. “Impacts of the mobile internet on transportation cyberphysical systems: traffic monitoring using smartphones”. In: *National Workshop for Research on High-Confidence Transportation Cyber-Physical Systems: Automotive, Aviation, & Rail*. 18–20.

Work, D., A. Bayen, and Q. Jacobson. 2008. “Automotive cyber physical systems in the context of human mobility”. In: *National Workshop for Research on High-Confidence Transportation Cyber-Physical Systems: Automotive, Aviation, & Rail*. 3–4.

Wu, D. and C. Zhou. 2011. “Fault-tolerant and scalable key management for smart grid”. *IEEE Transactions on Smart Grid*. 2(2): 375–381.

Wu, J., Q.-S. Jia, K. H. Johansson, and L. Shi. 2013. “Event-Based Sensor Data Scheduling: Trade-Off Between Communication Rate and Estimation Quality”. *IEEE Transactions on Automatic Control*. 58(4): 1041–1046.

Xie, L., Y. Mo, and B. Sinopoli. 2010. “False data injection attacks in electricity markets”. In: *International Conference on Smart Grid Communications*. IEEE. 226–231.

Xu, Y. and J. P. Hespanha. 2005. “Estimation under uncontrolled and controlled communications in networked control systems”. In: *Conference on Decision and Control jointly held with the European Control Conference*. IEEE. 842–847.

Yong, S. Z., M. Zhu, and E. Frazzoli. 2015. “Resilient state estimation against switching attacks on stochastic cyber-physical systems”. In: *Conference on Decision and Control*. IEEE. 5162–5169.

Yuan, Y. and Y. Mo. 2015. “Security in cyber-physical systems: Controller design against known-plaintext attack”. In: *Conference on Decision and Control*. IEEE. 5814–5819.

Yuan, Y., Q. Zhu, F. Sun, Q. Wang, and T. Başar. 2013. "Resilient control of cyber-physical systems against denial-of-service attacks". In: *International Symposium on Resilient Control Systems*. IEEE. 54–59.

Zhang, R. and P. Venkitasubramaniam. 2016. "Stealthy control signal attacks in vector LQG systems". In: *American Control Conference*. IEEE. 1179–1184.

Zheng, Y., O. Ozdemir, R. Niu, and P. K. Varshney. 2012. "New Conditional Posterior Cramér - Rao Lower Bounds for Nonlinear Sequential Bayesian Estimation". *IEEE Transactions on Signal Processing*. 60(10): 5549–5556.

Zhu, M. and S. Martinez. 2014. "On the performance analysis of resilient networked control systems under replay attacks". *IEEE Transactions on Automatic Control*. 59(3): 804–808.

Zuo, L., R. Niu, and P. K. Varshney. 2011. "Conditional Posterior Cramér - Rao Lower Bounds for Nonlinear Sequential Bayesian Estimation". *IEEE Transactions on Signal Processing*. 59(1): 1–14.