This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2787962, IEEE Internet of Things Journal

# Vulnerabilities of Control Systems in Internet of Things Applications

Verica Radisavljevic-Gajic, *Member, IEEE*, Seri Park, and Danai Chasaki, *Member, IEEE*

***Abstract*— In this paper, we present some initial results about vulnerability of control systems that can be used in Internet of Things (IoT) applications. Up to our best knowledge, this paper is the first study about vulnerability of applied control systems in general, and especially in the IoT environment. The purpose of this paper is to examine fundamentals of linear control systems and consider vulnerability of its main features and concepts used in Internet of Things applications under potential malicious attacks. We examine vulnerabilities of system stability, controllability, observability, design of feedback loops, and design and placement of sensors and controllers (actuators). The detailed study is limited to the most important vulnerability issues in time-invariant, unconstrained, deterministic, linear physical systems. Several interesting and motivating examples are provided. We have outlined also some basic vulnerability studies for time-invariant nonlinear unconstrained systems, and indicate that such a study is particularly needed for distributed parameter systems that are very prone to outside physical and cyber-attacks.**

***Index Terms* — *Cyber Physical Systems, Internet of Things, Vulnerability of Control Systems,***

## I. Introduction

Internet of Things (IoT) is a recent research trend in computer science, computer engineering, electrical engineering, and other engineering fields [1]-[2] with the goal of constructing "immersive and pervasive networks that enable easy accesses and interactions among "things"," [3]. The things are represented by any type of devices that can be connected to the network and interact with the network such as personal computers, smart phones, machines, vehicles, appliances, and in general their sensors and actuators, benefiting for example home automation, manufacturing, public transportation, and so on. Consequently, networks can be home networks, device-to-device networks, unmanned aerial networks, body area networks, satellite networks, and similar, providing person-to-person, person to machine, machine-to-machine communication. The things connected are used in different operations such as sensing [7], computing [11], communication [1], actuation and control [1], [4]-[5], [9], [13]. Closely related to IoT, and practically representing its integral parts are cyber-physical systems [6], [12], wireless sensor networks [8], mobile computing [1], and pervasive computing [1]. Computing involves also cloud computing, and recently fog computing [14]-[15] for end devices of IoT. For example, paper [15] uses fog computing [14] to solve the problem of selection of workers to complete some tasks in specified locations (spatial crowdsourcing). The problem is formulated as an optimization problem with two utility functions, one for the fog platform and another one for the workers. Security and privacy also play very important roles in IoT, [6] - [7], [9].

Wireless sensor networks have been instrumental in the development of IoT. Simultaneously used in numerous industrial applications these networks require efficient spectrum sharing. This problem has been recently studied in [16], where autonomous channel switching has been proposed to achieve fairness of spectrum usage among many users (things) connected to IoT. A survey of network methodologies that are efficient for big data IoT with billions of things, and related future research challenges have been considered in [17].

A nice overview of the present state of IoT and its future prospects can be found in [18]. The paper also discusses importance of security for IoT using the Smart Grid example. Detailed consideration of security and privacy in IoT smart city applications can be found in [19].

### A. IoT and Feedback Control Systems

The paper [1] presented the author view of future research directions for IoT, and among other issues emphasized the need for the development of the corresponding control algorithms that will be suitable for IoT applications. Paper [1] calls for much wider use of control systems in IoT and the development of new control techniques that will serve well the IoT: "…the scaling and interactions across systems also dynamically change the models and creates a need for decentralized control. While some work has been performed in topics such as stochastic control, robust control, distributed control, and adaptive control, these areas are not developed well enough to support the degree of openness and dynamics expected in some IoT systems. A new and richer set of techniques and theory is required. It is especially important to understand how large numbers of control loops might interact with each other." Control is needed first of all to provide a robust, reliable, secure, and adaptive performance in IoT. However, control algorithms

Submited for review: 08/09/2017".

Radisavljevic-Gajic Verica is with the Mechanical Engineering Department, University of Villanova, Villanova, PA 19085 USA, (e-mail: verica.gajic@villanova.edu).

Seri Park is with the Civil and Environmental Engineering Department, University of Villanova, Villanova, PA 19085 USA, (e-mail: seri.park@villanova.edu).

Danai Chasaki is with the Electrical and Computer Engineering Department, University of Villanova, Villanova, PA 19085 USA, (e-mail: danai.chasaki@villanova.edu).

and methods by themselves are vulnerable to outside attacks, especially attacks in an open system such as IoT. Among several research directions identified, [1] defines as a future research direction: "Challenge 1: The need for a comprehensive understanding of the complete spectrum of types of human-in-the-loop controls." In addition, [1] formulates "Challenge 3: Determining how to incorporate human behavior models into the formal methodology of feedback control. In the formal methodology of feedback control, there are several areas where a human model can be placed: 1) outside the loop; 2) inside the controller; 3) inside the system model; 4) inside a transducer; 5) at various levels in hierarchical control".

Importance of automatic control systems for IoT has been also indicated in several papers. Paper [4] states "… applications will not only enable the collection of information from devices and analysis of the gathered data, but also to actuate it through networks by using visualization, network management, control, …". As a matter of fact, [4] uses unity feedback control for crowd dynamics management to reduce congestion via IoT at stadiums, shopping malls, stations. For the problem considered, it develops a linear model with reaction of users being modeled by a first-order transfer function with a time delay. The delay element is approximated by another first-order transfer function that has an unstable zero and a stable pole. The performance criterion used is the absolute error between the desired and actual numbers of people. The corresponding feedback control block diagram with all transfer functions identified, including the closed-loop feedback control transfer function, is also presented in [4]. The application of [4] is one of many applications of IoT in the smart city concept [3].

Another call for the use of controllers in IoT came from [3], where a study was performed for IoT for smart cities with specific application to the city of Padova, Italy: "Internet of Things (IoT) is a recent communication paradigm that envisions a near future, in which the objects of everyday life will be equipped with microcontrollers, transceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, becoming an integral part of the Internet ...". Paper [10], developing an algorithm for on-line energy distribution in smart cities, asks for "The incorporation of communication, control and computation intelligence in the smart grid, and the deployment of smart meters (SMs) and smart facilities enable real-time sensing, monitoring, and automatic control of electricity generation, distribution, and consumption".

An optimal control technique, the dynamic programming, was used in [11] to improve the routing performance for large scale data centers used in IoT.

### *B. Cyber Physical Systems and Feedback Control Systems*

Cyber Physical Systems (CPS) are an integral part of IoT. In this paper, we present some initial results about vulnerability of control system that can be used in IoT/CPS applications. Up to our best knowledge, this is the first study about vulnerability of control systems, especially used in the IoT/CPS environment. Such control systems are largely exposed to potential cyber-threats. Paper [19] emphasizes potential vulnerabilities to outside attacks of control systems used in IoT: "The control and feedback systems in the physical world, especially public and industrial infrastructure, become highly attractive targets for attackers, criminals, and even terrorists." Current research shows that networked control systems are susceptible to direct as well as remote threats, including denial of service attacks, alteration of the system's operation or even sensor readings manipulation by false data injection. Malicious intruders are capable of performing very sophisticated attacks assuming they are familiar with the control system dynamics and/or have at least partial knowledge of some of the main control system features such as system stability, controllability, observability, optimality, sensitivity, robustness, structures of system feedback loops, system measurements (monitoring and sensing channels), types and placements of sensors and actuators, and controlled system input and output channels.

Control of real physical systems over wireless and wired communication channels, and in general with any type of communication channels and sensors with computers placed in feedback loops, has attracted a broad attention of control engineers for a number of years, see for example [20]-[24] and references there in. Security of such physical systems controlled via cyber space communication channels has become an important issue in recent years.

This paper *examine fundamentals of linear control systems and consider vulnerability of the main control system features (concepts) under malicious attacks*, *first of all, stability, controllability, and observability, and design of feedback loops*. The paper starts with the study of time invariant linear systems, and provides comments about systems with algebraic constraints. The study is limited to the deterministic time-invariant control systems. The paper outlines vulnerability of nonlinear systems, and nonlinear systems with algebraic constraints, and indicates the importance of such studies for distributed parameter control systems.

IoT/CPS control systems could have very complex structures that have to provide programming, integration, and Ethernet/IP communication for various personal computers (PCs), programmable logic controllers (PLCs) and single and multi-axis servos, variable frequency drives (to control alternating current (AC) motor speed and torque by varying motor input frequency and voltage), and direct current (DC) motor drives. Various software and hardware tools are used these days to facilitate such complexity while providing either partial or fully automated control systems, for example: ControlLogix (drives, motion, process, safety control together with communication input/output devices), CompactLogix, MicroLogix PLC's (all produced by Rockwell Automation); Kinetix 6000 and Ultra Servo Drives (multi-axis servo drives produced by Allen-Bradley), Sercos loop interface and Ethernet communications (a digital automation bus that interconnects motion controls, drives, I/Os, sensors and actuators over fiber optic rings or Ethernet), and associated tag and TCP/IP addressing.

The defense strategies against cyber-attacks at the present time are pretty limited since scientists and engineers have historically designed, analyzed, and controlled physical control systems under "normal" operating conditions, and excluded from their work all possibilities that a common sense cannot predict. However, in the present world, the "wars" are fought daily in the cyber space, either to provide some future advantages or for a simple reason to damage the "other side" or gain some material and/or financial (often illegal) benefits. Presently, scientists and engineers are faced with more difficult problems to study physical systems and cyber physical control systems under “abnormal” conditions, and extend their “normal” design and analysis to the situations that can be described as: (a) what to do if something that is almost unlikely to occur happens to a control system; (b) what to do if someone with bad intentions has an access to CPS.

Potential applications of the presented results are for IoT applications to power systems and smart power grids [25], water distribution networks, gas distribution networks, transportation systems, sensor networks, manufacturing systems, industrial automation systems, formation flights, string of smart vehicles equipped with vehicle to vehicle communication devices, transportations systems, intelligent highways with moving vehicles including strings of smart vehicles, and in general any physical system or any device connected, governed, and exposed to signals coming from the cyber space. For example, theoretical foundations for study of cyber physical systems for applications to transportation systems were made in a series of papers by Park [26]-[30].

## II. VULNERABILITY OF CONTROL SYSTEMS TO OUTSIDE ATTACKS

Many papers have been published about CPS, see for example [31]-[49] and references therein. Since physical systems can be either lumped (concentrated) parameter or distributed parameter dynamic systems, and since they can evolve either in continuous or discrete time and be either deterministic or stochastic, time-invariant or time-varying, there are almost endless possibilities for malicious attackers to damage cyber physical control systems either by inserting false signals via communication channels and in general IoT, or interfering directly with the system dynamics, or altering computational software (for example, MATLAB programs, programmable logic controllers software, supervisory control and data acquisition (SCADA) software) used to control and monitor physical control systems, or causing communication delays [4, 50] that affect the system stability, or very simple changing signs in the feedback loops and making negative feedback loops positive feedback loops that could have a tremendous impact on the system stability.

Various aspects of cyber-physical security, robustness, resilience [35, 38], data injection attacks [25], covert misappropriation [38, 44-45], detection of counterfeit sensors, attack detection and identification have been considered. Optimal control strategies, game-theoretic approaches [8, 13, 37, 46, 48-49], quantitative risk management strategies, secure estimation and control, distributed observer monitoring [41], data fusion engines [52]-[53] have been developed to cope with potential problems in CPS and in general IoT. To that end, linear and nonlinear physical systems, and systems described by differential-algebraic equations (generalized systems, singular systems) have been considered.

*The basic assumption in our paper is that attackers are very sophisticated and have full knowledge and understanding of theory and practice of real physical dynamic control systems*. It is also assumed that attackers have full knowledge of the given physical control system including the system mathematical model, access to system inputs and outputs, and even programs (for example, MATLAB, Simulink, Mathematica, PLC, SCADA, ControlLogix, Kinetix, Sercos interface software) used to control systems at their nominal operating points.

The main physical system features (concepts) are *stability*, *controllability*, *observability*. *Stability* protects physical system state variables to grow unbounded, which in general means physical system self-destruction, or at least that an unstable physical system leaves its normal (nominal) operating state, usually characterized by the physical system equilibrium point. *Controllability* means ability to fully control a physical system using system inputs as control variables, which allows to transfer the physical system state variables from any initial state to any final state. *Lousing controllability, simply means losing ability to control the physical system. Observability means ability to observe (monitor, estimate, measure) all system state variables at all times using information about system inputs and outputs.* If a system has some badly-behaved state variables, it is important that those state variables be at least observed at all times. If a physical system has some state variables that naturally should not be present in the system *(the system under attack) that state variables can be observed only if the system is observable*. Hence, *losing observability means losing ability to monitor presence of system attackers at all times*.

### A. Security Model

The control system cyber security framework consists of seven security dimensions and provides the foundation for defensive actions. Each of the seven dimensions of security represents an important aspect of the control system’s security posture at a given point in time. An *ideal cyber physical system* needs to meet the following security requirements:

1. Security Group (SG) knowledge - the Security Group (SG) should know the current control system perfectly.
2. Attack Group (AG) knowledge - Attack Group should know nothing about the control system.
3. Access - The control system should be inaccessible to AGs.
4. Vulnerabilities - The control system has no vulnerabilities.
5. Damage potential - The control system’s misbehavior cannot cause damage.
6. Detection SG detects any attack almost instantly.
7. Recovery SG can restore control system integrity almost instantly.

## III. VULNERABILITY OF SYSTEM STABILITY

In this section, time-invariant linear control systems are considered and vulnerability of the internal system stability (characterized by the eigenvalues) and bounded-input bounded-output (BIBO) stability are examined. Note that BIBO stability is determined in terms of the system impulse response and that it is characterized by the system transfer function poles. In addition, instability caused by malicious time delays, and instability of linear feedback system caused by altering signs of feedback loops (negative feedback loops altered into positive feedback loops) are also examined.

### A. Vulnerability of Internal System Stability

A linear time-invariant system is represented in *state space form* by the following vector differential equation

$$\frac{dx(t)}{dt} = \dot{x}(t) = Ax(t), \qquad x(t_0) = x_0 \tag{1}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2787962, IEEE Internet of Things Journal

where $x(t)$ is a $n$-dimensional vector of system variables and $A$ is a constant matrix of dimension $n \times n$. $x(t_0)$ is the system initial condition, which represents the energy stored in the system that drives the system dynamics. The system *internal stability* is determined in terms of *eigenvalue* locations [54]. For an asymptotically stable system, all eigenvalues must be strictly located in the left half of the complex plane, that is, $R\{\lambda_i(A)\} < 0, \forall i$. Since *eigenvalues are linear functions of the matrix elements* [55], one could conclude that the small changes in the system matrix elements will produce small changes in the system eigenvalues, in other words, the eigenvalues are little sensitive to changes in the system matrix elements. Of course, large changes in the system matrix elements will produce large changes in the system eigenvalues, and correspondingly effect the system stability, but large changes in the system elements can be easily detected, so that physical system instability can be prevented timely. It seems that as far as the *internal stability* of a linear time invariant system is concerned, the outside malicious attacks can be easily detected since they will have to do large (drastic) changes to the physical system to be able to considerably move the system eigenvalues and destabilize the system. The defensive strategy in this case will be simply to design linear time invariant systems with large robust stability margins (prescribed degree of stability), [56]-[58].

However, there are real physical systems such as *large space structures and antennas whose eigenvalues (even multiple eigenvalues) are located on the imaginary axis (marginally stable systems)*. Hence, their normal operations are on the verge of stability. Such real physical systems are prone to outside attacks. Stability of these systems is determined using the corresponding *Jordan forms* and finding and examining their *minimal polynomials* [59]. The numerical procedure for finding the Jordan form is extremely sensitive to small changes in the matrix elements; it is known to be an ill-defined numerical problem. A sophisticated malicious attacker can easily damage stability of such systems and even go undetected for a long time.

### B. *Vulnerability of Transfer Function and BIBO Stability*

In engineering and other scientific areas linear and linearized physical systems, in addition to state space representation given in (1), are represented also by *transfer functions*, for which the system BIBO stability is determined in terms of transfer *function poles*. For BIBO stability all transfer poles must be located in the left half complex plane. A sophisticated attacker can insert in a stable physical system transfer function an unstable transfer function zero and an unstable transfer function pole that are very close to each other (acting as a dipole) so they in fact cancel out each other and do not appear in the system transfer function. However, in the long run, the unstable zero and the unstable pole will not cancel each other perfectly, due to physical system tiny perturbations or aging of the system components, which will activate inserted unstable pole and make the overall system unstable. Let the stable nominal transfer function be $H_{nom}(s)$, and let the inserted pole and zero be denoted by $p$, then the overall physical system transfer function is given by

$$H(s) = H_{nom}(s)\frac{s-z}{s-p} = H_{nom}(s), \quad z = p, \quad p > 0 \tag{2}$$

A simple example can be used to show how the inserted unstable pole marked by the unstable zero in the same location might damage system stability and make the system step response to blow up in the long run.

*Motivating Example 1:* Consider the nominal system transfer function and its altered variant

$$H_{nom}(s) = \frac{s+2}{(s+1)(s+3)},$$

$$H_{altered}(s) = \frac{(s+2)(s-1.2000000001)}{(s+1)(s+3)(s-1.200000002)}$$

The open-loop step responses of these two transfer functions obtained via MATLAB are presented in Figure 1. It should be noted that the impact of such an attack is almost impossible to detect by monitoring the system dynamics since at the beginning the system response has normal behavior, but as in Fig. 1, the step response of the system will start exploding after a relatively long-time interval. It looks like that the system dynamics is "normal" as expected for 18 seconds, but suddenly within 3-4 seconds it explodes due to instability of the hidden system pole that was intentionally introduced by a hostile intruder. Different scenarios of "exploding" step response in the long run are possible. It might take much longer, minutes, hours, even days before the step response becomes unstable.

It can be concluded that the bounded-input bounded-output (BIBO) stability is even more prone to the outside malicious attacks than the internal system stability. Namely, a linear time-invariant system is BIBO stable if its impulse response is absolutely integrable, [54]. Since the impulse response is obtained by applying the inverse Laplace transform to the system transfer function, we are faced here exactly with the same problem as presented in Example 1: proper locations of the poles of a physical system transfer function.

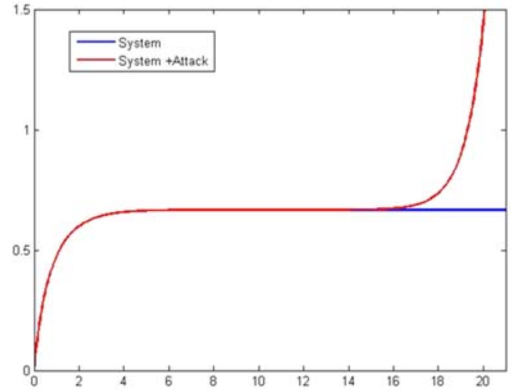

Fig. 1. Step Responses of the Nominal and Maliciously Altered System Transfer Functions. The Time Axis Units are in Seconds

### C. *Linear System Vulnerability to Time Delays*

A hidden stability issue is loss of stability in linear time invariant physical systems due to *time delays*. In general time delays make the system dynamics much more complicated since time delays correspond to infinite dimensional systems. It is well known from that even in the simplest cases of linear time invariant systems with an explicit time delay element $e^{-sT}$ appearing in the system transfer function that is

$$H(s) = H_{nom}(s)e^{-sT} \tag{3}$$

the system stability becomes a function of the time delay $T$ and it may be lost when the time delay exceeds a certain bound. Such a transfer function with a time delay element was derived in [4] in modeling of the crowd dynamics and used to design a feedback controller for management of the crowd dynamics via IoT in a smart city. In the case of (3), the physical system stability analysis can be performed using the Nyquist diagram [56]. Assuming that $H_{nom}(s)$ is stable, it is possible to find an upper bound on the time delay that will preserve stability, or a malicious attacker can find the lower limit of the time delay that will destabilize the system. Monitoring such delays using observers to observe all system state variables at all-time [54], [60] will be a promising method to detect whether the delays are present and which state variables are under such attacks.

### D. *Vulnerability of Feedback Systems*

It very well known that negative feedback loops are used to stabilize linear time invariant systems and that positive feedback loops lead to oscillations and instability [56]. Just a sign change can make a negative feedback loop to become a positive feedback loop and cause instability of a control system. *This is probably the most vulnerably point in a physical feedback (control) system*. A block diagram of common physical linear time-invariant feedback control system is presented in Fig. 2, where $H(s)$ is the system transfer function, $U(s)$ and $Y(s)$ are respectively the Laplace transforms of the system input and output signals, and $G(s)$ is the transfer function of the feedback loop.

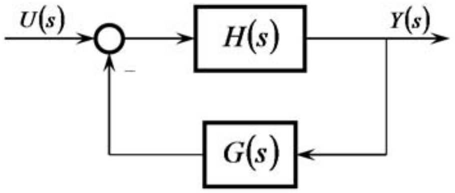

Fig. 2. Block Diagram of a Physical Feedback Control System

One possible solution to cope with this problem is to design feedback loops in multiple stages, see for example [61]-[63], where designs of two stage feedback static controllers where considered. Extended the robustness results of [57-58, 64] to multi stage designs will make the corresponding control system feedback loops more robust, and less prone to altering of feedback loop signs by malicious outside agents.

## IV. VULNERABILITY OF CONTROLLABILITY AND OBSERVABILITY

A sophisticated attacker who knows physical system dynamics and understands physical system concepts known as controllability and observability, may in a very sophisticated manner change either system or its measurements such that the ability to control the physical system is lost and/or gathering information about all system state space variables of the system at all times becomes either impossible or erroneous. These events are very dangerous for real systems since they imply that the *system either cannot be completely controlled and/or some of its state variables cannot be accurately observed at all times*.

System controllability and observability can be determined in terms of matrix rank of the corresponding controllability and observability matrices [56]. It is known from linear algebra that the rank operation is numerically ill-defined operation since tiny perturbations in the matrix elements can change the result about the rank of the given matrix [59]. However, the system controllability and observability can be determined via controllability and observability Gramians and the requirement that they are positive definite matrices [54]. The rank and Gramian tests are reviewed in the next paragraph. For a linear time-invariant control system represented by

$$\begin{aligned} \frac{dx(t)}{dt} &= Ax(t) + Bu(t), \quad x(0) = x_0 \\ y(t) &= Cx(t) \end{aligned} \tag{4}$$

where $x(t) \in R^n$ are system state space variables, $u(t) \in R^m$ are system inputs, and $y(t) \in R^p$ are system measurements. The system controllability/observability matrices are given by

$$M_C = \begin{bmatrix} B & AB & A^2B & \cdots & A^{n-1}B \end{bmatrix}, \quad M_O = \begin{bmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{n-1} \end{bmatrix} \tag{5}$$

with the controllability and observability rank tests given by

$$\text{rank}\{M_C\} = n, \qquad \text{rank}\{M_O\} = n \tag{6}$$

The controllability and observability Gramians are given by

$$W_C(t_1) = \int_0^{t_1} e^{At}BB^T e^{A^T t}dt, \quad W_O(t_1) = \int_0^{t_1} e^{A^T t}C^T Ce^{At}dt \tag{7}$$

For system controllability and observability, the Gramian matrices have to be positive definite (nonsingular) for every $t_1 > 0$, [54], that is

$$W_C(t_1) > 0, \quad W_O(t_1) > 0 \tag{8}$$

When matrix $A$ is asymptotically stable and $t_1 = \infty$, the controllability and observability Gramians can be obtained from the algebraic Lyapunov equations [54, 57-58]

$$W_C A^T + AW_C + BB^T = 0, \quad W_O A + A^T W_O + C^T C = 0 \tag{9}$$

The controllability and observability tests $W_C > 0$ and $W_O > 0$ now can be expressed in terms of eigenvalues of the controllability and observability Gramians. Since for symmetric positive definite matrices the eigenvalues are positive and real [59], the eigenvalues of $W_C$ and $W_O$ serve also as *controllability/observability measures* [57]-[58]. The farther the eigenvalue is from the origin the better controllable/observable the corresponding state variable is. The eigenvalues of $W_C$ ($W_O$) that are close to the origin indicate that the corresponding state variable is difficult to control/observe. Such state variables are called *weakly controllable/observable*, in contrast to the system state variables that are *strongly controllable/observable* whose Gramian eigenvalues are far from the origin.

*Remark 1:* If controllability and observability are studied

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2787962, IEEE Internet of Things Journal

over finite time interval $(0, t_1]$, (7) leads to the differential Lyapunov equations whose structures are similar to the algebraic Lyapunov equations (9), given by

$$\begin{aligned} -\frac{dW_C}{dt} &= W_C A^T + AW_C + BB^T,\ W_C(0) = 0, \\ -\frac{dW_O}{dt} &= W_O A + A^T W_O + C^T C,\ W_O(0) = 0 \end{aligned} \tag{10}$$

in which case, the following must be satisfied $W_C(t) > 0,\ W_O(t) > 0,\ \forall t \in (0, t_1]$.

*Motivating Example 2:* An interesting example can be found in [57]-[58]. The system state space form, transfer function, controllability and observability Gramians are

$$\begin{aligned} \frac{dx(t)}{dt} &= \begin{bmatrix} -1 & -\dfrac{4}{\alpha} \\ 4\alpha & -2 \end{bmatrix} x(t) + \begin{bmatrix} 1 \\ 2\alpha \end{bmatrix} u(t), \quad x(0) = x_0 \\ y(t) &= \begin{bmatrix} -1 & \dfrac{2}{\alpha} \end{bmatrix} x(t) \end{aligned} \tag{11}$$

$$H(s) = \frac{3s + 18}{s^2 + 3s + 18},\ W_C = \begin{bmatrix} 0.5 & 0 \\ 0 & \alpha^2 \end{bmatrix}, W_O = \begin{bmatrix} 0.5 & 0 \\ 0 & \dfrac{1}{\alpha^2} \end{bmatrix}$$

The system transfer function is invariant with respect to $\alpha$, and that one state variable for very small values of $\alpha$ is weakly controllable and strongly observable, and for very large values of $\alpha$ the same state variable is strongly controllable and weakly observable. If a malicious attacker can change $\alpha$, one of the state space variables can be made either weakly controllable (difficult to control) or weakly observable (difficult to observe). The presence of the attacker will be undetected in the system transfer function since the transfer function will remain unchanged regardless the chosen value of $\alpha$.

It is known from the Kalman canonical decomposition theorem [54, 57-58, 65] that the state space variables that are either uncontrollable or unobservable or both do not appear in the system transfer function. These state variables cannot be controlled or observed or both. They are particularly dangerous for the system, even in the cases when they are asymptotically stable. Namely, if a malicious attacker can access them and control them in his/her own way, *the attacker will be undetected, and through these state space variables the attacker can do many undesired things to the system.* Checking the physical system transfer function to look for potential changes in the system and/or potential sources of malicious attacks is not advisable. The state space form must be used to monitor for the intruders (if the system is observable). In general, observers can be used as monitoring devices in all areas of sciences and engineering, see for example [66]-[67], and references there in.

To study dynamical importance of every state variables on the system output, it is necessary to map the system into the balanced coordinates [57]-[58] in which the controllability and observability Gramians are identical and diagonal. It follows from the balancing transformation study that the state variables that are both strongly controllable and strongly observable determine the system dominant dynamics and that they are the ones that we should be primarily concerned about. That is true under the "normal" conditions. However, under attacks ("abnormal" conditions), the concept of system balancing should be further explored since the attackers may hide in the non-dominant state variables. Moreover, the non-dominant state variables have much faster dynamics than the dominant state space variables, so that that such systems display the singularly perturbed structure [68]-[70]. It is important to emphasize that the defense strategies should be developed in a very fast time scale, much faster than the original system time scale, such that they will be able to efficiently combat very fast dynamics that could be controlled by malicious attackers. The next example indicates that the balancing transformation can drastically change the original system controllability and observability measures of some state space variables.

*Motivating Example 3:* Consider an aircraft example taken from [68], whose state space matrices are

$$A = \begin{bmatrix} -0.01357 & -32.2 & -46.3 & 0 \\ 0.00012 & 0 & 1.214 & 0 \\ -0.0001212 & 0 & -1.214 & 1 \\ 0.00057 & 0 & -9.1 & -0.6696 \end{bmatrix}, B = \begin{bmatrix} -0.433 \\ 0.1394 \\ -0.1394 \\ -0.1577 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

The controllability and observability measures (eigenvalues of the solutions of the corresponding algebraic Lyapunov equations defined in (9)) in the original coordinates, obtained using MATLAB, are respectively given by

$$\lambda(W_c) = \{0.006789,\quad 0.037171,\quad 0.393259,\quad 69889.185600\}$$

$$\lambda(W_o) = \{0.023079,\quad 0.306281,\quad 0.500586,\quad 91624.199738\}$$

In the original coordinates, the system has three extremely weakly controllable state variables and one very strongly controllable state variable, and three extremely weakly observably state variables and one very strongly observable state variable. After balancing, the eigenvalues are

$$\begin{aligned} &\lambda(W_c^{bal}) = \lambda(W_o^{bal}) = \\ &\{1685.819144,\quad 1385.348986,\quad 0.598934,\quad 0.466737\} \end{aligned}$$

It can be seen from this example that *balancing transformation can change very drastically the eigenvalues of the controllability and observability Gramians*.

It is important to emphasize that the balancing transformation does not change the system eigenvalues and it does not change the system controllability and observability [54, 57-58]. However, it does change the controllability and observability measures of every single state space variables in a pretty drastic manner as demonstrated in Motivating Example 3. For example, applying a similarity transformation to the system defined in (4) as $\overline{x}(t) = \mathbf{T}x(t)$ the new system state space matrices will become $\overline{A} = \mathbf{T}^{-1}A\mathbf{T},\quad \overline{B} = \mathbf{T}^{-1}B,\quad \overline{C} = C\mathbf{T}$ and preserve the system eigenvalues, that is $\lambda(\overline{A}) = \lambda(A)$, but the new controllability and observability Gramians become

$$\begin{aligned} &\mathbf{T}^{-1}W_C A^T \mathbf{T}^{-T} + \mathbf{T}^{-1} A W_C \mathbf{T}^{-T} + \mathbf{T}^{-1} B B^T \mathbf{T}^{-T} = 0 \\ &0 = \overline{W}_C \overline{A}^T + \overline{A}\,\overline{W}_C + \overline{B}\,\overline{B}^T \\ &\mathbf{T}^T W_O A \mathbf{T} + \mathbf{T}^T A^T W_O \mathbf{T} + \mathbf{T}^{\mathbf{-1}} C^T C \mathbf{T} = 0 \\ &0 = \overline{W}_O \overline{A} + \overline{A}^T \overline{W}_O + \overline{C}^T \overline{C} \end{aligned} \tag{12}$$

Hence, in the new coordinates the controllability and observability Gramians are given by

$$\overline{W}_C = \mathbf{T}^{-1} W_C \mathbf{T}^{-T}, \qquad \overline{W}_O = \mathbf{T}^{\mathbf{T}} W_O \mathbf{T} \tag{13}$$

It is an important problem to examine what are the numerical causes for potential drastic changes in the eigenvalues of $\overline{W}_C$ and $\overline{W}_O$ under the transformation (13), which can be exploited by a potential malicious attacker.

Systems described by linear differential equations coupled with algebraic equations, where algebraic equations represent the system constraints, are often seen in engineering practice [71]. It will be an important future research topic to study vulnerability of controllability and observability of linear time-invariant physical systems modeled by differential-algebraic equations, where the algebraic equations represent constraints of physical system state space variables and control inputs.

### *A. Loss of Controllability (Observability) due to Sampling*

Models of physical control systems continuous in nature, connected to computers and communication networks, which is particularly important for IoT, have to be represented in the discrete-time domain using sampling. Sampling a continuous-time mathematical model represented by a differential equation using a given sampling period produces a discrete-time system described by a difference equation. It is interesting and *important* to observe that the system controllability (observability) may be lost under sampling. Namely, *if the original continuous-time system is controllable (observable) the corresponding discrete-time counterpart might be uncontrollable (unobservable).* An example was presented in [54] to demonstrate this phenomenon. As a matter of fact, it was known from [65] that in order to preserve controllability (observability), the sampling period of a linear continuous-time system represented by system matrix $A$ must satisfy the following condition

$$T \neq \frac{2\pi k}{\operatorname{Im}\{\lambda_i(A) - \lambda_j(A)\}}, \quad i, j = 1,2,...,n, \quad k = 1,2,... \tag{14}$$

where $\lambda_i(A)$ are the system eigenvalues.

It will be interesting and important to explore how a malicious attacker can exploit the controllability (observability) loss due to sampling as presented in formula (14), and damage the corresponding physical control system. Namely, by doing so, a computer that is supposed to provide the control input signal for a physical system will have false information that the system is not controllable (observable) and in cases when such conditions are required (for example to provide optimal feedback gains for the linear-quadratic regulator and/or the Kalman filter), the computer will not be able to do so. Even worse, if digital controllers and/or filters are used to drive continuous-time systems such lack of correct information can have catastrophic effects. One way to cope with this problem is to use the gain-scheduling control technique [72] (to have pre-computed feedback gains (calculated off-line) and stored in the computer memory) instead of calculating them on-line, or to explore some ideas from predictive control techniques [73] and keep an active feedback loop on.

## V. SENSOR FUSION WITH NON-OPTIMAL LOCAL "KALMAN" FILTERS

Combining data from several sources and using them to obtain desired estimates of variables of interest has recently become an attractive and important research area mostly known under sensor fusion. The sensor fusion can be efficiently done by implementing the "centralized" Kalman filter in a decentralized manner and using local filters as sensors. It is interesting, what our simple analysis shows, that the local filters should be implemented as non-optimal "Kalman" filters such that the proposed sensor fusion technique produces the "centralized" Kalman filter *optimal* estimate. Note that the original Kalman filter has been used in smart power grids, [74], for detection of faults and attacks, including false data injection.

Consider a linear dynamic system corrupted by noise and noisy measurements

$$\begin{aligned} &\frac{dx(t)}{dt} = Ax(t) + Gw(t), \quad \mathrm{E}\{x(t_0\} = \bar{x}_0, \mathrm{Var}\{x(t_0\} = P_0 \\ &y(t) = Cx(t) + v(t) \end{aligned} \tag{15}$$

where $x(t) \in R^n$ are the system state space variables, $y(t) \in R^p$ are the system "centralized" measurements. White noise processes $w(t) \in R^r$ and $v(t) \in R^q$ are assumed to be zero-mean, mutually uncorrelated and Gaussian with spectral densities $W \geq 0$ and $V > 0$, which are assumed to be constant.

Assume that the measurements are obtained by augmenting data from several sensors, say $N$, that is

$$y(t) = \begin{bmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_N(t) \end{bmatrix} = \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_N \end{bmatrix} x(t) + \begin{bmatrix} v_1(t) \\ v_2(t) \\ \vdots \\ v_N(t) \end{bmatrix} = Cx(t) + v(t) \tag{16}$$

where $y_i(t) \in R^{p_i}$, $p_1 + p_2 + \cdots p_N = p$ and $v_i(t) \in R^{q_i}$ with $q_1 + q_2 + \cdots q_N = q$ being mutually uncorrelated, zero-mean, Gaussian white noise stochastic processes with intensities $V_i > 0$. Measurements $y_i(t)$ can be generated from different sources such as cameras, radars, satellites (GPS). The "centralized" optimal Kalman filter

$$\frac{d\hat{x}(t)}{dt} = (A - KC)\hat{x}(t) + Ky(t), \quad \mathrm{E}\{\hat{x}(t_0\} = \bar{x}_0 \tag{17}$$

minimizes the variance of the estimation error $e(t) = x(t) - \hat{x}(t)$ and makes $\mathrm{E}\{e(t)\} = 0$. The optimal Kalman filter gain is [60]

$$K = C^T P V^{-1} \tag{18}$$

where $P$ is the positive semidefinite stabilizing solution of the algebraic Riccati equation

$$AP + PA^T + GWG^T - PBV^{-1}B^T P = 0 \tag{19}$$

$$\mathrm{Var}\{e(t)\} = \mathrm{Var}\{x(t) - \hat{x}(t)\} = P \tag{20}$$

It is not difficult to show that the *optimal estimate of the centralized optimal Kalman filter* can be *obtained from the non-optimal decentralized Kalman filters* as follows

$$\hat{x}(t) = \hat{z}_1(t) + \hat{z}_2(t) + \cdots + \hat{z}_N(t) \tag{21}$$

$$\frac{d\hat{z}_i(t)}{dt} = \left(A - K_1C_1 - K_2C_2 \ldots - K_NC_N\right)\hat{z}_i(t) + K_i y_i(t)$$

$$\mathrm{E}\{\bar{z}(t_0\} = \frac{1}{N}\bar{x}_0, \quad i = 1,2,\ldots,N \tag{22}$$

The local filter non-optimal Kalman filter gains obtained by partitioning the optimal Kalman filter gain as

$$\begin{bmatrix} K_1^{p_1\times n} \\ K_1^{p_2\times n} \\ \vdots \\ K_N^{p_2\times n} \end{bmatrix} = K^{p\times n}, \begin{bmatrix} K_1 & K_2 & \cdots & K_N \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_N \end{bmatrix} = KC \tag{23}$$

Such local filters (22)-(23) and the global estimates (21) make the Kalman filter more robust to outside attacks since the failure of one or two locally non-optimal “Kalman” filters will not completely degrade the optimality of the global Kalman filter.

This idea can be extended to decentralized implementation of linear observers [54, 60, 66], deterministic versions of the Kalman filter with the observer gain determined obtained via the eigenvalue assignment technique [54] such that the closed-loop observer matrix has desired eigenvalues, that is $\lambda(A-KC) = \lambda^{\text{desired}}$. Moreover, it can be combined with the multi-stage feedback design [61-63, 75] to find the gains $K_i, i = 1,2,\ldots,N$ in a decentralized manner.

## VI. Vulnerability of Nonlinear and Distributed Parameter Systems

In this section, we provide only a brief introduction to vulnerability issues in nonlinear and distributed parameter systems. Due to numerous phenomena present in nonlinear systems, they are even more vulnerable to malicious attacks than linear systems. In the case of nonlinear systems [72] researchers should consider the impact of malicious attacks on nonlinear system dynamics related to basic nonlinear phenomena such as multiple equilibrium points, harmonics and sub-harmonics, finite escape time, limit cycles, and chaos.

Different system equilibrium points can display very different dynamics, and those equilibrium points are parametrized by control input signals. For a nonlinear control system given by

$$\frac{dx(t)}{dt} = f(x(t), u(t)) \tag{24}$$

the equilibrium points are obtained from

$$0 = f(x_e(t), u(t)) \tag{25}$$

If a malicious attacker has an access to control input channels, the attacker can change the system equilibrium points that are often used as system operating (nominal, set, trim) points. In that case, the attacker will be also able to affect the choice of the system equilibrium point. That will have tremendous impact on the system since some equilibrium points might be unstable, have unstable limit cycles, or display chaotic behavior. It is known, for example, that aircraft wings can go into chaotic motion (irregular bounded, but stable motion). Human heart and brain can produce signals that are chaotic in nature.

Chaos is sometimes intentionally introduced in the system (anti control) since chaotic behavior is very sensitive to the system initial conditions. For example, the gravitational field is chaotic. To be able to send space ships far away with the help of the gravitational filed it is extremely important to choose properly the initial time. Limit cycles (either stable or unstable) are very sensitive to small perturbations, which gives to malicious attackers possibilities to make (with only small efforts) big changes in the nonlinear control system dynamics.

Distributed parameter systems described by partial differentia equations are particularly vulnerable to outside attacked since there are infinitely many points of entry in such systems.

It will be important that researchers consider basic nonlinear phenomena subject to malicious attacks, particularly the impact of these attacks on the selection of equilibrium points, existence of state variables finite escape times, changes in harmonics and sub-harmonics, stability and instability limit cycles, and nonlinear system chaotic behavior (either intentionally introduced or suppressed by control inputs. Extending those studies to nonlinear with algebraic constraints described by nonlinear differential-algebraic equations (constrained coordinates) [66], and distributed parameter control systems will be mandatory tasks for control scientists and practitioners.

## VII. Conclusions

Vulnerability of several main attributes (features) of linear control feedback systems that are integral parts of the IoT to malicious attacks was considered, and some motivating examples were presented. The study was limited to time-invariant systems. Future research is needed to address these issues and propose the best defense strategies in cases of such attacks. It is expected that this paper will motivate corresponding vulnerability studies of time-invariant linear and nonlinear systems with algebraic constraints, and eventually the corresponding study will be extended to time varying and/or stochastic physical systems with and without constraints, as well as to distributed parameter physical systems whose dynamics is described by partial differential equations.

## References

[1] J. A. Stankovic, “Research directions for the Internet of Things,” *IEEE Internet of Things Journal,* vol. 1, no. 1, pp. 3-9, Feb. 2014.

[2] T. Kumrai, K. Ota, M. Dong, J. Kishigami, and D. K. Sung, “Multiobjective optimization in cloud brokering systems for connected Internet of Things,” *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 404-413, Apr. 2017.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, “Internet of Things for smart cities,” *IEEE Internet of Things Journal,* vol. 1, no. 1, pp. 22-32, Feb. 2014.

[4] Y. Kawamoto, N. Yamada, H. Nishiyama, N. Kato, Y. Shimizu, Y. Zheng, “A feedback control based crowd dynamics management in IoT system,” *IEEE Internet of Things Journal*, vol. 4, pp. 1466-1476, 2017.

[5] K. Sato, Y. Kawamoto, H. Nishiyama, N. Kato and Y. Shimizu, “A modeling technique utilizing feedback control theory for performance evaluation of IoT system in real time,” International Conference *Wireless Communications & Signal Processing*, Nanjing, China, pp. 1-5, 2015.

[6] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-physical systems security – A Survey,” *IEEE Internet of Things Journal*, early view, 2017.

[7] W. Li, H. Song, and F. Zeng, “Policy-based secure and trustworthy sensing for Internet of Things in smart cities,” *IEEE Internet of Things Journal*, early view, 2017.

[8] J. Duan, D. Gao, D. Yang, C-H. Foh, and H-H. Chen, Fellow, “An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications,” *IEEE Internet of Things Journal,* vol. 1, no. 1, pp. 58-69, Feb. 2014.

[9] D. Li, Z. Aung, J. Williams, and A. Sanchez, “P3: Privacy preservation protocol for automatic appliance control application in smart grid,” *IEEE Internet of Things Journal,* vol. 1, no. 5, pp. 414-429, Feb. 2014.

[10] Y. Wang, S. Mao, and R. M. Nelms, “Distributed online algorithm for optimal real-time energy distribution in the smart grid.” *IEEE Internet of Things Journal,* vol. 1, no. 1, pp.70-80, Feb. 2014.

[11] J. Xie, L. Lyu, Y. Deng, and L. T. Yang, “Improving routing performance via dynamic programming in large-scale data centers,” *IEEE Internet of Things Journal,* vol. 2, no. 4, pp. 321-328, 2015.

[12] M. Moness and A. Moustafa, "A Survey of cyber-physical advances and challenges of wind energy conversion systems: Prospects for Internet of Energy," *IEEE Internet of Things Journal*, vol. 3, 134-145, 2016.

[13] X. Zhao, Y. Zhang, C. Jiang, J. Yuan, and J. Cao, "Mobile-aware topology control potential game: Equilibrium and connectivity," *IEEE Internet of Things Journal*, vol. 3, 1267-1273, 2016.

[14] Q. Huang, Y. Yang, and L. Wang, "Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things," *IEEE Access*, vol. 5, pp. 12941-12950, 2017.

[15] P. Yang, N. Zhang, S. Zhang, K. Yang, L. Yu, X. Shen, "Identifying the most valuable workers in fog-assisted spatial crowdsourcing," *IEEE Internet of Things Journal*, vol. 4, pp. 1193-1203, 2017.

[16] F. Lin, C. Chen, N. Zhang, X. Guan, and X. Shen, "Autonomous channel switching: Towards efficient spectrum sharing for industrial wireless sensor networks," *IEEE Internet of Things Journal*, vol. 3, pp. 231-243, 2016.

[17] S. Verma, Y. Kawamoto, Z. Fadlullah, H. Nishiyama, and N. Kato, "A survey on network methodologies for real-time analytics of massive IoT data and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 19, pp. 1457-1477, 2017.

[18] Y. Kawamoto, H. Nishiyama, N. Kako, N. Yoshimura, and S. Yamamoto, "Internet of Things (IoT): Present state and future prospects," *IEICE Transactions on Information and Systems*, vol. E97-D, pp. 2568-2575, 2014.

[19] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Communications Magazine*, pp. 122-129, January 2017.

[20] S. Yang, X. Chen, and J. Alty, "Design issues and internet-based process control systems," *Control Engineering Practice*, vol. 11, pp. 709-720, 2003.

[21] S. Yang, C. Dai, and R. Knott, "Remote maintenance of control system performance over the Internet," *Control Engineering Practice*, vol. 15, pp. 533-544, 2007.

[22] H. Thompson, "Wireless and Internet communication technologies for monitoring and control," *Control Engineering Practice*, vol. 12, pp. 781-791, 2004.

[23] I. Calvo, M. Marcos, D. Orive, and I. Sarachaga, "A methodology based on distributed object-oriented technologies for providing remote access to industrial plants," *Control Engineering Practice*, vol. 14, pp. 975-990, 2006.

[24] P. Neumann, "Communication in industrial automation—what is going on?," *Control Engineering Practice*, vol. 15, pp. 1332-1347, 2007.

[25] H. He and J. Yan, "Cyber-physical attacks and defenses in the smart grid: A survey," *IET Cyber-Physical Systems*, vol. 1, 13-27, 2016.

[26] C. Oh, S. Park, and S. Ritchie, "A method for identifying rear-end collision risks using inductive loop detectors," *Journal of Accident Analysis and Prevention*, pp. 38.2, 2006.

[27] S. Ritchie, S. Jeng, Y. Tok, and S. Park, "Corridor deployment and investigation of anonymous vehicle tracking for real-time traffic performance measurement," *PATH Final Report* TO 5304, UCB-ITS-PRR-2008-23, 2008.

[28] S. Park and S. Ritchie, "Automated real-rime vehicle classifier development based on vehicle signature," *International Journal of Granular Computing, Rough Sets and Intelligent Systems*, pp. 1.2, 2009.

[29] S. Park and S. Ritchie, "Innovative single loop speed estimation model with advanced loop data," *Institution of Engineering and Technology Intelligent Transport System*, pp. 4.4, 2010.

[30] T. Song, S. Park, and C. Oh, "Investigating the effects of in-vehicle warning information on driver's responsive behavior based on field experiment," *Institution of Engineering and Technology (IET) The Journal of Engineering*, 2016.

[31] P. Ralston, J. Graham, and J. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Transactions*, vol. 46, pp. 583-594, 2007.

[32] C-W. Ten, C-C. Liu, and G. Manimaran, "Vulnerability of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems*, vol. 23, pp. 1836-1846, 2008.

[33] M. McQueen and W. Boyer, "Deception used for cyber defense of control systems," *2nd Conference on Human System Interactions. HSI '09*, pp. 624-631, 2009.

[34] M. Ilic, L. Xie, U. Khan, and J. Moura, "Modeling of future cyber-physical energy systems for distributed sensing and control," *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, vol. 40, pp. 825-838, 2010.

[35] T. Kim and V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, pp. 326–333, 2011.

[36] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, 645–658, 2011.

[37] S. Sundaram, S. Revzen, and G. Pappas, "A control-theoretic approach to disseminating values and overcoming malicious links in wireless networks," *Automatica*, vol. 48, pp. 2894–2901, 2011.

[38] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, pp. 2715–2729, 2013.

[39] B. Horowitz, and K. Pierce, "The integration of diversity redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems," *Systems Engineering*, vol. 16, pp. 401-412, 2013.

[40] A. Giani, E. Bitar, M. Garcia, M. Mc Queen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Trans. Smart Grid*, vol. 4, pp. 1244–1253, 2013.

[41] F. Dörfler, F. Pasqualetti, and F. Bullo, "Continuous-time distributed observers with discrete communication," *IEEE Journal on Selected Topics Signal Processing*, vol. 7, pp. 296–304, 2013.

[42] A. Teixeira, K. Sou, H. Sandberg, and K. Johansson, "Quantifying cyber-security for networked control systems," *Control of Cyber-Physical Systems*, Lecture Notes in Control and Information Sciences, D. C. Tarraf, (ed.), Springer, pp. 123–142, 2013.

[43] A. Teixeira, I. Shames, H. Sandberg, and K. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135-148, 2014.

[44] S. Amin, X. Litrico, S. Sastry, and A. Bayen, "Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks," *IEEE Transactions on Control Systems Technology*, vol. 21, pp. 1963–1970, 2013.

[45] S. Amin, X. Litrico, S. Sastry, and A. Bayen, "Cyber security of water SCADA systems—Part II: Attack detection using enhanced hydrodynamic models," *IEEE Transactions on Control Systems Technology*, vol. 21, pp. 1679–1693, 2013.

[46] S. Amin, G. Schwartz, A. Cardenas, and S. Sastry, "Game-theoretic models of electricity theft detection in smart utility networks," *IEEE Control Systems Magazine*, vol. 35, pp. 66-81, 2007.

[47] W-C. Lin, K. Villez, and H. Garcia, "Experimental validation of a resilent monitoring and control system," *Journal of Process Control*, vol. 24, pp. 621-639, 2014.

[48] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyber-physical control systems," *IEEE Control Systems Magazine*, vol. 35, pp. 46-65, 2015.

[49] Y. Yuan, F. Sun, and H. Liu, "Resilient control of cyber-physical systems against intelligent attacker: a hierarchal Stackelberg game approach," *International Journal of Systems Science*, vol. 47, pp. 2067-2077, 2016.

[50] E. Penera and D. Chasaki, "Packet scheduling attacks on shipboard networked control systems," *International Symposium on Resilient Control Systems (ISRCS)*, 2015.

[51] C. Rieger, K. Moore, and T. Baldwin, "Resilient control systems: A multi-agent dynamic systems perspective," *IEEE International Conference on Electro/Information Technology (EIT)*, vol. 9, pp. 1-16, 2013.

[52] O. Linda, M. Manic, J. Alves-Foss, and T. Vollmer, "Towards resilient critical infrastructures: Application of type-2 fuzzy logic in embedded network security cyber sensor," *4th International Symposium on Resilient Control Systems (ISRCS)*, pp. 26-32, 2011.

[53] O. Linda, M. Manic, and T. Mc Junkin, "Anomaly detection for resilient control systems using fuzzy-neural data fusion engine," *4th International Symposium on Resilient Control Systems (ISRCS)*, pp. 35-41, 2011.

[54] T-C. Chen, *Linear System Theory and Design*, 4th edition, Oxford University Press, Oxford, 2013.

[55] T. Kato, *Perturbation Theory of Linear Operators*, New York: Springer Verlag, 1980.

[56] G. Franklin, J. Powel, and A. Emami-Naeini, *Feedback Control of Dynamic Systems*, Upper Saddle River, NJ: Prentice-Hall, 2002.

[57] K. Zhou, J. Doyle, and K. Glover, *Robust and Optimal Control*, Upper Saddle River, NJ: Prentice Hall, 1995.

[58] K. Zhou and J. Doyle, *Essentials of Robust Control*, Upper Saddle River, NJ: Prentice Hall, 1998..

[59] G. Golub and C. Van Loan, *Matrix Computations*, Academic Press, 2002.

[60] A. Sinha, *Linear Systems: Optimal and Robust Control*, Boca Raton: Francis & Taylor/CRC Press, 2007.

[61] V. Radisavljevic-Gajic and P. Rose, "A new two stage design of feedback controllers for a hydrogen gas reformer," *International Journal of Hydrogen Energy*, vol. 39, pp. 11738-11748, 2014.

[62] V. Radisavljevic-Gajic, "A simplified two-stage design of linear discrete-time feedback controllers," *ASME Journal of Dynamic Systems Measurements and Control*, vol. 138, pp. 014506-1 – 014506-7, 2015.

[63] V. Radisavljevic-Gajic, "Two-stage feedback design for a class of linear discrete-time systems with slow and fast variables," *ASME Journal of Dynamic Systems Measurements and Control*, vol. 138, pp. 086502-085507, 2015.

[64] V. Radisavljevic-Gajic, "Simple practical classical- $H_2$ robust controller," *AIAA Journal of Guidance, Control, and Dynamics*, vol. 29, pp. 417-420, 2006.

[65] R. Kalman, "Mathematical description of linear dynamical systems," *SAIM Journal of Control*, vol. 1, pp. 152-192, 1963.

[66] V. Radisavljevic-Gajic, "Full-order and reduced-order observer implementations in MATLAB/SIMULINK," *IEEE Control Systems Magazine*, pp. 91-101, 2015.

[67] J. Ali, N. Hoang, M. Hussain and D. Dochain, "Review and classification of recent observers applied in chemical process systems," *Computers and Chemical Engineering*, vol. 76, pp. 27-41, 2015.

[68] P. Kokotovic, H. Khalil, and J. O'Reilly, *Singular Perturbation Methods in Control: Analysis and Design*, Philadelphia: SIAM Publishers, 2000.

[69] D. Naidu and A. Calise, "Singular perturbation and time scales in guidance and control of aerospace systems: A survey," *AIAA Journal of Guidance, Control and Dynamics*, vol. 24, pp. 1057-1078, 2001.

[70] C. Kuehn, Multiple *Time Scale Dynamics*, Springer, 2015.

[71] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control theoretic methods for cyberphysical security," *IEEE Control Systems Magazine*, vol. 35, pp. 110-127, 2015.

[72] H. Khalil, *Nonlinear Systems*, 3rd edition, Upper Saddle River, New Jersey: Prentice Hall, 2001.

[73] E. Camacho and C. Alba, *Model Predictive Control*, Springer, 2007.

[74] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection in smart grid using Kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, pp. 370-379, 2014.

[75] V. Radisavljevic and M. Milanovic, and G. Clayton, "Three-stage feedback controller design with applications to three time-scale control systems," *ASME Journal of Dynamic Systems Measurements and Control*, vol. 139, pp. 104502-1-104502-10, 2017.

**Verica Radisavljevic-Gajic** (M'12) received her Dipl. Ing. Mechanical Engineering degree from the University of Belgrade, and her M.S. and Ph.D. degrees both in Mechanical and Aerospace Engineering from Rutgers University, Piscataway, NJ, USA. She held research and teaching positions at Lafayette College, Rutgers University, California State University Los Angeles, and the American University of Sharjah, UAE. Since 2012 she has been a Clare Boothe Luce Assistant Professor at Villanova University, Department of Mechanical Engineering, Pensilvania, USA. Her research interests are in the area of dynamics and control of complex systems, with applications to distributed parameter systems with sliding mode boundary control, PEM fuel cells modeling and control, modeling and control of biological systems, internet of things.

**Seri Park** (PhD, PTP) received the B.S. degree in urban planning from Hongik University, Seoul, South Korea in 1992, M. S. degree in transportation engineering from Seoul National University, Seoul, South Korea in 1998, and PhD in civil and environmental engineering from University of California, Irvine, CA in 2004. Currently, she is a Clare Boothe Luce Assistant Professor in the Civil and Environmental Engineering department at Villanova University. She conducts research on highway safety, traffic control & operation, Intelligent Transportation System (ITS) and sustainable infrastructure. She has published several journal papers focusing on traffic safety and operation. She is also Panel Member of various research projects sponsored by *National Academy of Sciences, Engineering and Medicine*. Prior to joining VU, she worked with Tetra Tech Inc. and the University of California, Irvine. She is certified as a Professional Transportation Planner. (seri.park@villanova.edu, 610-519-3307)

**Danai Chasaki** received her Diploma in Electrical and Computer Engineering from the National Technical University of Athens, Greece, in 2006. She also received her MS and PhD degrees in Electrical and Computer Engineering from the University of Massachusetts Amherst, in 2009 and 2012 respectively. In 2012, she joined the Department of Electrical and Computer Engineering at Villanova University as an Assistant Professor. Before that, she was an Adjunct Instructor at Worcester Polytechnic Institute and a Research Assistant at the Network Systems Lab of the University of Massachusetts Amherst. Her current research interests include embedded system design, network security and cyber-physical systems. She is a member of the IEEE, the ACM and the ASEE. She is an active as program committee member of some professional conferences including IEEE ICNP and ACM/IEEE ANCS.