A Comprehensive Overview of Cyber-Physical Systems: From Perspective of Feedback System

Xinping Guan, *Senior Member, IEEE*, Bo Yang, *Member, IEEE*, Cailian Chen, *Member, IEEE*, Wenbin Dai, *Member, IEEE*, and Yiyin Wang, *Member, IEEE*

***Abstract*—Cyber-physical systems (CPS) are characterized by integrating cybernetic and physical processes. The theories and applications of CPS face the enormous challenges. The aim of this paper is to provide a latest understanding of this emerging multi-disciplinary methodology. First, the features of CPS are described, and the research progresses are summarized from different components in CPS, such as system modeling, information acquisition, communication, control and security. Each part is also followed by the future directions. Then some typical applications are given to show the prospects of CPS.**

***Index Terms*—Cyber-physical systems (CPS), system modeling, information acquisition, communication, control, security.**

I. Introduction

In the last decade, the academia and industry have witnessed the flourishing research activities on cyber-physical systems (CPS). CPS are defined as the systems by integrating computation, networking, and physical processes, where the embedded computers and networks control and monitor and physical processes usually in a closed-loop while the latter affects the computations and even the networks. It should be noted that the integration does not mean the simple convergence of the physical world and the cyber space, but the physical and cyber components are deeply interacted. Therefore, the analysis and design of CPS is based on the understanding of the joint dynamics of physical processes, computer, software and networks.

Many systems can be categorized as CPS, such as demand response in smart grids[1−3], where the demand side users, such as various domestic appliances constitute the physical components, and the data of demand load are collected by the smart meters, which connect the physical world and the cyber space. The demand load data are transferred via the two-way communication channels that are used to measure and control the physical component. On the cyber side, the computations are carried out by the independent system operator (ISO) with the objective of utility maximization of user sides and cost minimization of user side, and a suitable real-time electricity price is announced, based on which the demand side (physical components) are further controlled. Another example is the body sensor network, which is a network of medical devices that can sense medical or physiological data, which can be used to augment bodily functions through drug delivery or support for the movement of prosthetic limbs[4]. A multi-agent system such as multiple autonomous underwater vehicles (AUVs) can be also seen as CPS whose sensors and networking system enable AUVs to monitor their location and operation while coordinating with each other to tracking a moving target. Thus, CPS range from miniscule such as body sensors to large scale such as power grid. The study on CPS can provide a comprehensive and inter-disciplinary framework for analyzing and designing these practical systems.

CPS shares some common features with the current popular information and communications technology (ICT) systems, namely embedded systems, networked control systems (NCSs), internet of things (IoT) and industrial internet. We list the comparisons in chronological order and state the relationship between CPS and other emerging technologies.

1) CPS are not the generic embedded systems or NCSs. It can be regarded as a networked embedded systems.

2) CPS are not IoTs, although they are sometimes used interchangeably. IoT is usually corresponding to a hierarchical communication infrastructure that has information sensing, processing and transmission functionalities in an application-driven way. While CPS emphasize the interaction between physical processes and cyber dynamics. IoT is more like a platform for implementing some applications. In another word, it can be regarded as an extension of internet. Contrasting with IoT, CPS is a way of understanding and designing real world.

3) The forthcoming industrial internet refers to the integration of the global industrial ecosystem, pervasive sensing, advanced computing and ubiquitous network connectivity that enables the increasing benefits of world economy[5]. Thus it can be seen that its technological basis is CPS.

Due to the tight coupling and coordination between cyber and physical worlds, CPS are dynamically reorganizing and reconfiguring control systems with high degree of automation at multiple spatial and temporal dimensions. To enable seamless integration, the implementation of CPS relies on the closed-loop consideration and design of the whole system. As shown in Fig. 1, the events sensed in the physical processes need to be

Manuscript received May 6, 2015; accepted August 18, 2015. This work was supported by National Natural Science Foundation of China (61221003, 61174127, 61573245, 61273181, 61503247, 61301223), and Shanghai Municipal Science and Technology Commission (15QA1402300, 14511107903). Recommended by Associate Editor Youxian Sun.

Citation: Xinping Guan, Bo Yang, Cailian Chen, Wenbin Dai, Yiyin Wang. A comprehensive overview of cyber-physical systems: from perspective of feedback system. *IEEE/CAA Journal of Automatica Sinica*, 2016, **3**(1): 1−14

Xinping Guan, Bo Yang, Cailian Chen, Wenbin Dai, and Yiyin Wang are with the Department of Automation, Shanghai Jiao Tong University, and Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China (e-mail: xpguan@sjtu.edu.cn; bo.yang@sjtu.edu.cn; cailianchen@sjtu.edu.cn; w.dai@sjtu.edu.cn; yiyinwang@sjtu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

reflected in the cyber world, and the control strategies taken by the cyber world needs to be transferred to the physical plants. It can be found from this process, the sensors and actuators serve as an interface between the physical and cyber worlds, and the networked communication infrastructure closes up the gap between physical world and cyber space, where security issues arise throughout the whole system. In the following, we list several features and requirements originating from the closed-loop system perspective, which make the design and analysis of CPS significantly different from other ICT systems.

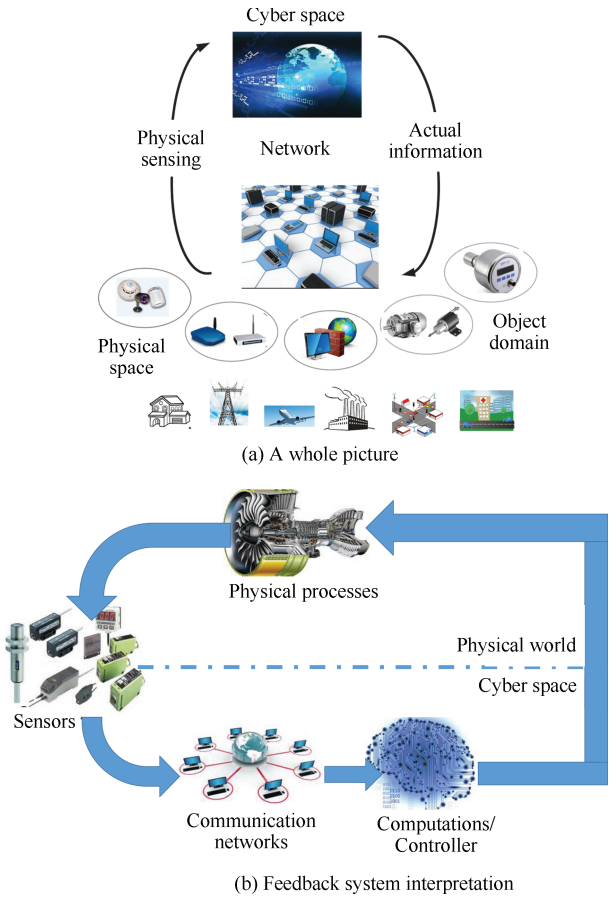

Fig. 1. CPS applications and closed-loop interpretations.

1) System modeling. Modeling is a key step to understand the interactive dynamics of CPS. Physical components run in continuous time and other cyber components consist of discrete time operations. With various hardware and software platforms are interconnected via networks, one CPS research challenge is to co-design and analyze the integration of physical models along with computational models and communication models.

2) Sensing. Sensing bridges cyber space and physical world. To achieve timely and reliable information, issues related to signal processing, compression, and data fusion need to be addressed carefully. Usually the research of sensing in CPS is application oriented, since the function of sensing is tightly coupled with other functions and there is no unifying treatment of sensing techniques.

3) Communications. The networked communication infrastructure for control in CPS has brought new challenges. The goal of communication infrastructure is to provide a channel for reliable and timely information transmission. It is expected that sensors, actuators and controllers in CPS can be flexibly removed, added or substituted. This flexibility calls for the scalability and adaptability of communication infrastructure for the changes of other components and environments in CPS.

4) Controller. One of the salient features of CPS is the existence of communication networks connecting among computing and physical components. Thus, many network induced issues, like delay, packet losses and communication constraints exist in CPS. However, the controller for NCS is not enough for CPS as stated later. Moreover, the real-time performance is more important in CPS control than any previous systems. Even if the control output is correct, it is useless without real-time guarantee especially for industry control.

5) Security. The security goal of CPS is to protect the normal operation from a malicious party attacking the cyber infrastructure since the threats due to intrusion from cyber space will spread and interfere the formal operation of physical entities. In additional to the protection of normal operation, there are non-operation goals. We must ensure that the measured private or sensitive information can only be accepted by authorized parties. Thus, we can see that security issues can be found in every component of CPS.

In this paper, we survey several recent works in the field of CPS. We classify the developmental efforts based on the basic components of CPS and identify the future challenges in the development of them. We discuss applications of CPS, along with the examples of existing CPS prototypes. Since it is not possible to cover all the aspects of CPS in a paper of this length, we review few works and emphasize the interaction between sensing, communication, control, and security in CPS.

II. System Model

The interacting dynamics among integrated components result in difficulties in modeling and verifying CPS. Existing modeling and verification techniques that are devised within a particular discipline are no longer be adequate to meet complexities of CPS. Dynamics from cyber space and physical world shall be addressed in a unified system model before any subsequence contributions can actually be made to CPS.

A. Hybrid System Model

In modeling techniques, physical processes are commonly represented by continuous models. However control software and communications are usually programmed in discrete manner. How to bridge discrete execution semantic from control software with an intrinsically concurrent physical world is a challenge for designing and verifying CPS models. As shown in Fig. 2, the model of physical processes is reflected by a separated component that differs from cyber space. Cyber part, physical part together with communication part composes a closed-loop hybrid software model for CPS.

Model-driven engineering (MDE) with knowledge-base support plays an important role in software design. The MDE approach is considered as the enabler for modeling CPS[6−8]. For example, Ptolemy Project from UC Berkeley aims for solving

modeling issues in CPS design[9]. Ptolemy II provides actor-oriented modeling which supports multiple domains (model of computation) modeling in the same design workspace as illustrated in Fig. 3. Actors are triggered by input ports, execute internal logics and generate events on output ports. Actors could be set to various models of computation that represents either physical world or control systems. An actor could be encapsulated in another actor (modal model) in a nested structured. There exist similar modeling languages for CPS such as ExCHARON[10], CPSHCML[11], and even using mathematical models directly[12].

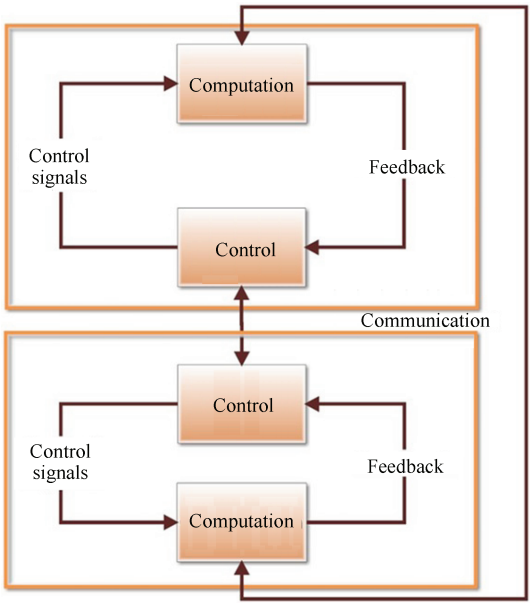

Fig. 2. Closed-loop modeling in CPS.

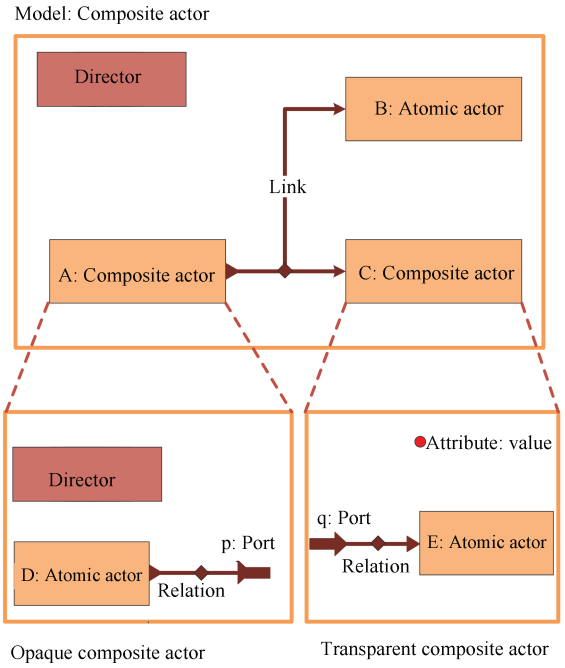

Fig. 3. Modeling CPS using Ptolemy II.

There are also some works on combining discrete and continuous dynamics in modeling CPS. In smart grid applications, stability issues are essential concerns in the performance of smart grids with the hybrid dynamics. Susuki et. al.[13] demonstrates the reachability analysis of hybrid systems enables quantitative estimation of stability in smart grids. Measurement for power grid stability as safety specifications are interpreted in a hybrid model of power grid dynamic performance. In energy CPS, transferring sensor measurements to controller is always a mission for communication. Nature of uncertain destination and switching routing modes for multicast routing is studied in [14] by hybrid system theories and linear matrix inequality techniques.

Hybrid systems model checking is an extremely important topic for ensuring correctness and safety of CPS from control perspective. For medical device plug-and-play (MDPnP) CPS, due to the difficulty to use offline differential equation to model human body and numerical measurable parameters in human body, an online hybrid system model checking method is proposed in [15] based on time-bounded future behavior. The design principal is based on the facts that majority of human body parameters can be predictable within short finite horizon. For many large-scale CPS, their components are scheduled currently that are not amenable to formal analysis. Alternatively, components may simply be too large and complicated to be verified. One approach to formally verify system behavior is to use Simplex Architecture for unverified control logic[16], where unverified control logic is combined with a verified controller. The unverified control logic typically has better performance, whereas the verified controller is designed only with safety-critical aspects. When the system is in abnormal state, the system will switch to verified controller automatically. The key challenge of designing a system based on the Simplex Architecture is to properly create the switching logic.

The integration of cyber and physical processes by using hybrid system modeling techniques are demonstrated by combining ordinary differential equations and automata using simple systems[17]. These models have a uniform notion of time, which is available to all parts of systems. For multi-agent system, especially for underwater acoustic sensor networks, how to synchronize local clocks with global time clock[18] is also an unsolved question.

B. Agent-based Model

One restriction of developing accurate models for CPS is the connection between cyber and physical components. A generic approach for handling interdependencies between cyber and physical infrastructures is desired. Agent-based modeling is a promising method to overcome these challenges, since software agents act as flexible autonomous and intelligent decision-making components. A semantic representation of the CPS interdependencies using semantic models implemented with multi-agent techniques is presented in [19]. Two compositional models are proposed, one for autonomous agents and the other for interactive agents. The interactive agent is in charge of interacting with the environment through interface points, and coordinates with other agents regulated by policies. To model CPS, interactions between physical

and cyber components are investigated by [20]. A multi-agent model that describes the interactions between cyber and physical components within a CPS, as well as inter-dependency among multiple CPS, are presented. In [21], multi-agent inter-model behavior and relations of entities are demonstrated for CPS. Since in CPS multiple entities could share one resource and system could be shut down due to conflicts of resources, conflict detection is highly important. Belief desire intention (BDI) agents are applied to detect the resource conflicts using local belief state information of agents without communication.

As a visual modeling language for formal specification with precise semantics, unified modeling language (UML) is an intuitive choice to model multi-agent systems with precise semantics. UML consists of several types of structured diagrams and graphical elements that are assembled to represent a model. How UML models can be applied to multi-agent systems is demonstrated by [22] and discussion on pros and cons are provided. Lin et al.[23] aim to model a CPS using multi-agent system concepts, where information from sensor networks is dynamically integrated with semantic services to support real-time decision making support for CPS. UML is also utilized in this MAS approach for creating models for agents.

Existing agent-based modeling techniques consider CPS as either an agent for integrating with larger systems or a collection of independent agents, which interact with each other. The existing agent models focus mainly on data processing and information collection to reflect interactions between physical and cyber subsystems, however, physical behavior of CPS is not well defined.

C. Modeling with Big Data

With advance in sensing, communication and cloud computing techniques, size of CPS is continuously increasing. For example, smart cities and transportation networks could also be considered as CPS. Also information generated from CPS is increasing dramatically, how to improve accuracy of models by analyzing massive data from CPS becomes a new challenge. Several unique challenges are raised by big data generated from CPS[24]: Firstly, how to transform collected data to useful information for modeling; Secondly, how to utilize massive information collected by sensors for high level control and decision making in CPS. These challenges also bring new opportunities for developing new modeling and analytical methodologies. Zhang[25] proposes a model based approach to model big data driven CPS based on integration of AADL, OpenModelica and clock theory, applying object-oriented paradigm and component-based design model for big data driven CPS. Lee et al.[26] propose a five-layer architecture for the implementation of CPS with industrial big data. Furthermore, trends of manufacturing service transformation in big data environment as well as big data management to achieve transparency and productivity are also discussed[27]. A generic data analysis approach is required to cover multiple disciplines of CPS.

D. Future Direction

Existing modeling methodologies cannot fulfill all requirements of CPS. For example, a description language is sufficient for designing entire systems in old school. However, with current level of complexities and varieties, existing description language lacks physical information of networked systems such as positions. Thus, a unique modeling language is highly desired for designing CPS. Ptolemy II provides certain level of abstraction and encapsulation for CPS. But not all application domains can be covered yet. In addition, this new modeling language shall also bridge real-time control with event-based computations and communications. Furthermore, although real applications could be extremely complicated, system model should cover as much details as possible and balance between abstraction view and characteristics. To conclude, a novel modeling method is required for covering design, develop, verify and validate CPS with all physical and cyber related information to ensure high degree of dependability and reconfigurability.

III. Information acquisition

A CPS is the integration of abstract computations and physical processes, where sensors, actuators, and embedded devices are networked to sense, monitor, and control the physical world. Information acquisition is the first step in designing a CPS after system modeling. In CPS, sensors collect information about the physical operation of the system, and communicate this information in real-time to the computers and embedded systems used for intelligent control. In this process, the information acquisition section usually suffers from the effects of sensing with hardware constraints, imperfect communication constraints and time-varying transmission environments. In the following, we will review the recent works on information acquisition in typical CPS applications and state the future research directions.

A. Sensing

Wireless sensor network (WSN) is one of the main way of information acquisition in CPS. On salient feature of WSN in CPS is that rapid change of network topology. The time-varying topology can be passive or active. For the former, some wearable sensors might be worn by people. For the latter, sensors can act as mobile agents which can move around for better sensing performance. Assuming each mobile agent has a map of the natural fluidic environment, [28] raised a distributed control policies enabling a homogeneous team of mobile sensing agents to maintain a desired spatial distribution. Reference [29] discusses coordinating a mobile sensor team, which can dynamically change their positions to optimize their coverage of the target. In [30], two new patrol algorithms are introduced to plan the paths of controllable floating cars to participate in traffic monitoring. Reference [29] is a study of a more general case, while the control strategy in [28] is derived from the Lagrangian coherent structures of the flow, and the patrol algorithm in [30] is closely related to the characteristics of the data reconstruction scheme. It goes without saying that there is a lot of work to do about control

strategy in new environments. Besides, seldom paper analyzes energy efficiency of the control strategy in the evaluation part.

B. Data Compression for Communication

Nowadays, wide application of mobile devices such as smart-phones, sensor-equipped vehicles makes mobile crowd sensing highly feasible. Typical application is urban area monitoring, such as traffic monitoring[31] and estimation of urban pedestrian flows[32]. Due to the limitation of communication bandwidth and a lot of redundancies in raw data, there is the need for data compression. In [33], the author applied compressed sampling theory in distributed sensor data gathering, and it has been proved that the scheme can effectively reduce the communication cost. In [34], the authors raised an event-driven transmission scheme which can reduce data transmission rate of sensor nodes. However, there are limitations on the algorithms of both paper. The strategy in [33] is not suitable for small scale sensor networks. In [34] they have to choose the consensus gain carefully for the stability of the filter. In the application of mobile sensor reporting its trajectory to data sink, [35] proposed an adaptive trajectory compression algorithm based on compressive sensing. The authors in [35] developed a method to compute a deterministic projection matrix from a learnt dictionary and a technique for the mobile nodes to adaptively predict the number of projections needed based on the speed of the mobile nodes.

C. Data Processing

After data is acquired by the sink, more actions have to be done on data processing in order to reconstruct the whole information based on data sparsity properties and estimate the necessary states with partial observed information.

1) Data reconstruction. Distributed deployment of sensors and the unreliable communication circumstance make data loss a common but serious problem. Traditional interpolation methods are simpler and more effective for less serious data loss problems. In [36], the authors propose a data recovery scheme, called the efficient temporal and spatial data recovery (ETSDR) scheme for incomplete feedback of CPS using the temporal and spatial correlation of the data. For data with large scale, simple interpolation cannot handle serious data loss problems. Compressed sensing, a new tool developed in the field of statistical signal processing, shed new light on this area. For sparse signals, it is possible to surpass traditional limits of sampling theory, and enable recovery of the signal from very few measurements [37]. In [38], due to the insufficiency and uneven distribution of GPS data from taxis, the author raised a method based on compressed sensing for urban traffic sensing. Matrix completion, a data reconstruction method closely related to compressed sensing is adopted in [39] for effective urban traffic monitoring. However, there are some limitations for the adaptation of compressed sensing. We have to find a domain in which the signal is sparse. In other words, unlike the Shannon theorem, compressed sensing is not universal for each signal.

2) State estimation. The second problem is state estimation in CPS. Some physical variables cannot be directly perceived by sensors: sensors may not be able to sense data from the area of interest, or they can only sense physical variable relevant to variables of interest[40]. CPS are usually large systems, which makes the problem more challenging due to coupling effects. In addition, CPS are usually tasked with advanced duty such as prediction and self-diagnostics. In an intelligent transportation system, CPS will predict the vehicle flow rate. In a water system, they will assess the spread of toxic chemicals. For example, in battery management system, it is very important to accurately estimate the state of charge (SoC) of battery. In [41], the author reviewed some estimation methods for SoC, such as Kalman filter, artificial intelligence and formal methods. Hybrid method derived from existing methods may perform better.

Another problem is estimation under communication constraint, such as packet loss, time delay and intermittent topology in a multi-agent system. In [42], the authors analyze the stability of Kalman filter based state estimation in spatially distributed lossy CPS due to time delay and packet loss. In [36], the authors discuss the estimation problem in CPS due to feedback loss. To tackle the communication constraint problem and enable efficient communication, many proposals are raised. In [43], the authors elaborate the significance of power control and coding for Kalman filtering over wireless channels, and raise two estimation architectures and reexamine several coding strategies. In [44], the authors reconfigure network topology in wireless sensor networks for remote state estimation. In [45], the authors study the use of relays to improve the performance of Kalman filtering to tackle the packet loss problem. In [46], the authors propose a design strategy for transmission energy allocation at a sensor equipped with energy harvesting technology for remote state estimation. In [47], the authors raised a novel method for attack-resilient state estimation. Future work might be to reduce the algorithm complexity and consider the dynamic online strategy.

In addition, it is also worth noticing that recently there has been some research about estimation in heterogenous sensor networks. For example, in [48], the CPS can fuse uncertain information from different types of distributed sensors, such as power system meters and cyber-side intrusion detectors. In [49], the authors consider the heterogeneous sensor networks with two types of sensors different on processing abilities (denoted as type-I and type-II sensors, respectively) and address the problem of filter design for target tracking over sensor networks.

3) Data with anomalies. Another problem is about processing of data with anomalies. It is worth noticing that the anomalies might come from attackers. Two common strategies are anomaly detection and designing a robust algorithm. In [48], the authors present a security-oriented cyber-physical state estimation system and it can detect the malicious activities within the system and fuse uncertain information. In [50], the authors propose a novel methodology to address the detection of such attacks, and further incorporate appropriate remedial actions in the estimator. In [51], the authors propose a novel model of atypical cluster to effectively represent atypical events and efficiently retrieve them from massive data. In CPS, anomalies or attacks might come from the cyber side

or the physical side and thus, anomaly detection based on information from both sides needs more work to do.

D. Future Direction

From 2003 to 2009, academia have witnessed the golden years of human-free information acquisition with sensor networks. With the development of smart portable devices, human-centric information acquisition has attracted industry players from the very outset and caused the research community to move its focus toward the human-centric paradigm in recent years. A convergence of human-free and human-centric information acquisition will be one of the mainstream directions. The interface between the cyber space and the physical world will be necessarily characterized by an ever growing variety of sensing devices producing an ever-increasing data volume that will create excellent opportunities for value creation through big data analytics. Moreover, as the development of micro-electro-mechanical systems (MEMS) techniques, the embedded information acquisition application will pervade people's lives everywhere and result in heterogeneous information flow, multi dimensional sensor cooperation and high level of intelligence and algorithm behind the actuation and decision framework.

IV. Communications in CPS

CPS emerges from conventional researching areas WSN and machine-to-machine (M2M) systems, with an attempt to bridge the physical world and the cyber world. To this end, communication, computation and control methods should be aggregated to monitor, analyze and take action in physical world. Communication in CPS, whether wired or wireless, takes the responsibility of connecting individual devices and information exchanging among the whole network. Thus efficient communication is needed for cross-domain cooperation, and the communication strategy should be specially designed.

A. Requirements of Communication in CPS

For the quality of service (QoS) requirement of communication in CPS, several terms should be considered, namely real-time, reliability, scalability, mobility and security which are as follows:

1) Real-time. Real-time is a must in CPS. Data that have missed its deadline is not only deemed useless, but also is harmful for the communication subsystem. Thus, managing acceptable dynamic traffic load with the ability to deliver data in real-time is an essential task of the communication subsystem in CPS.

2) Reliability. Sensors transmit monitoring data to intended controllers; controllers generate decision and forward command data to actuators. Reliability of the communication subsystem is highly important in this monitor-control type applications, which are the most common in CPS, such as distributed state monitoring in power networks[52]. Also, outage in data transmission in CPS could quickly force the system out of normal operation and result in cascade failure.

3) Time-varying QoS. CPS is basically interacting with the physical world and dynamics in the physical world result in time-varying traffic in CPS. Overall traffic within a certain period of time could be much higher than that of other times. This is similar to the periodic traffic trend in business cellular networks. However, the changes can be nonperiodic. For a data stream generated from a specific sensor, traffic rate and QoS could also change distinctly, which is brought either by large change in the sensors neighborhood, or due to urgent reports from other places.

4) Scalability and mobility. The objective of communication subsystem in CPS is to provide reliable and timely information transmission. It is desirable that sensors, actuators, and controllers in CPS can be flexibly added, removed, or replaced. This flexibility calls for scalability and adaptability of a communication subsystem that can endure frequent change of other entities in CPS.

B. Communication Network Design in CPS

CPS rely on an underlying communication network to transmit data packets between sensors, computational units, and actuators. For these packets to be delivered within a deadline, transmission nodes may require a certain minimum throughput of such packets. Thus, CPS need a real-time communication network that can provide guarantees on both the throughputs and delays of flows. Since both wireless and wireline networks have stochastic natures, the real-time and minimum throughput performance can be measured in a stochastic way. There are several methods can be used to design resource allocation for communication networks in order to guarantee the real-time performance. In [53], the authors compare three methods, namely large deviation theory, Lyapunov optimization technique, and approximate Markov decision process approach (MDP). For the large derivation theoretic method, it converts average delay constraints into equivalent average rate constraints using the large deviation theory and solves the optimization problem using a purely information theoretical formulation based on the rate constraints[54]. While Lyapunov optimization technique can be used to design online algorithm without needing to know the distribution of underlying stochastic process[55]. The MDP approach is useful in design algorithm for small delay regime.

Reliability relates to transmission failure due to packet drop, interference and outage. As for random packet drops, the communication subsystem can be regarded as a Markovian jumping process, and the equivalence can be found in [56]. In [57], the authors demonstrate that network coding improves network reliability by reducing the number of packet retransmissions in lossy networks. They further study the extent of the reliability benefit of network coding analytically. In wireless networks transmission failure may be due to the multipath fading. Laneman et al.[58] develop and analyze space-time coded cooperative diversity protocols for combating multipath fading across multiple protocol layers in a wireless network. Factory monitoring and control applications pose strict reliability and delay requirements for wireless communications in industrial environments. To reduce outage in such fading-rich areas, cooperative relays can be used to overhear source-destination transmissions failure. Reference [59] presents the results of an experimental study of selective cooperative relaying protocols

that are implemented in IEEE 802.15.4-compatible devices which is implemented in an industrial production plant.

Since a large volume of data needs to be properly transferred from time-varying heterogenous networks to the controller and vice versa, it is required that the communication network design for CPS should have favorable scalable property and adaptability to ensure the time-varying QoS[60]. It should be noted that scalability is highly related with other performance index. Deng et al.[61] proposed two algorithms in order to ensure the delay performance in a large-scale wireless sensor networks for CPS, namely a cycle-based synchronous scheduling and a clustering structure are designed to guarantee the low delay and high throughput. Data acquisition via densely deployed sensor networks is a typical application in CPS, e.g. densely embedded sensors/actuators across an aircraft wing to perform active flow control. Ehyaei et al.[62] design an interpolation scheme of sensor readings by incorporating physical world model, which can result in a favorable tradeoff for designers: some physical models are very simple and cause very low run-time overhead whereas other physical models are more accurate but cause a larger run-time overhead. Zhou et al.[63] proposed three communication architectures for advanced metering infrastructure (AMI) in smart grid. They introduced a new performance metric, accumulated bandwidth distance product (ABDP), to denote the total communication resource usages and designed corresponding solutions for minimizing the total system cost with respect to ABDP and the deployment cost of the meter data management.

C. Future Direction

One of the major features of CPS is that there can be an extremely large number of machines involved in the system operation, where multiple communication technologies coexist. For example, WiFi, Bluetooth, and Zigbee work on the same unlicensed ISM band to support short-range communications. To provide ubiquitous coverage, especial the access to cloud without additional cyber infrastructure deployment costs, connecting all these machines by leveraging cellular communication systems turns out to be an effective and efficient solution, whereas cellular systems work on licensed band[64]. Then, one research direction is how to design a scalable architecture and enable technology to support the massive machine-type connections. Currently, cognitive radio can be a candidate technology for spectrum sharing between unlicensed and licensed bands[65]. However, it is still far from requirement of reliability and real-time performance. In addition, the fourth-generation (4G) wireless communication system and the forthcoming fifth generation (5G) one claim to support machine-type communication. It would be better that the next-generation communication system can manage the M2M communications and human-to-human (H2H) communications separately but with a system point of view, since M2M and H2M have different traffic characteristics and QoS requirements but share the same spectrum resources.

V. Control in CPS

CPS already exists, at some level in industrial process control, oil refineries, and power networks[66], where time-critical and safety-critical operations are the heart of these systems. To meet the real-time and reliability requirements, fidelity and timely sensing and communication are not enough for the networked CPS. Each component in CPS should be autonomous and behave consistently to achieve a or several system targets. Control plays the central role in realizing the self-autonomous operation in the coherent closed-loop interaction in CPS. For control in a closed-loop system there are many issues to be considered depending on diverse applications and domains. In the following, we only summarize several salient issues that CPS designers have to tackle from the perspective of control theory. Then we give the state of the art on this topic together with future directions.

A. Requirements of Control in CPS

1) Robustness. Robustness is the property ensuring that slight perturbations in the cyber, physical, or in the interaction between the cyber and the physical components, e.g., noise in sensor measurements, have little effects on the system operation. Robustness in CPS also means fault tolerance. The stability of CPS should be guaranteed in the presence of cyber and physical failures.

2) Resource constrained. CPS are in many cases implemented over resource-constrained embedded platforms, where components with limited computational capacity are integrated with imperfect communication and networking. The closed-loop stability of CPS should be maintained in the face of non-idealities of computations and communications.

3) Co-design. It should be emphasized that traditional control theory for physical process relies on continuous mathematical model, whereas scheduling, computation and communication in cyber space behaves discrete manner. Then the tight interaction between the physical and cyber parts may necessitate cross layer design, and specifications on timing issues in order to achieve the system goals.

4) Real-time and reliability. These two metrics have been mentioned in communication network design for CPS, however, they are also paramount in controller design for CPS since control strategies decide the output from cyber space to physical plant. Moreover, these two metrics are highly challenging not only because sometimes they are conflicting objectives but also due to that the same system has to co-design with constrained resource to ensure robustness.

B. State of the Art

With the aim of developing a robustness theory for CPS, Tabuada et al.[67] introduce the robustness notion for cyber systems to express two intuitive goals: bounded disturbances lead to bounded deviations from nominal behavior, and the effect of a sporadic disturbance disappears in finitely many steps. Reference [68] studies the real-time implementation of distributed controllers on CPS by combining event-triggered and self-triggered control. Aminifar et al.[69] argue that either robustness or expected control quality alone is not enough to guide controller design and propose an integrated approach for designing high-quality robust cyber-physical systems. For resource constrained CPS system, the event-triggered scheduling outperforms time-triggered schemes for control applications.

Molin et al.[70] adopt techniques from distributed optimization and adaptive Markov decision process (MDP) to develop distributed self-regulating event-trigger based controllers for CPS. Since the communication channel is limited, the authors in [71] addressed the event-triggered estimation and control for teleoperation systems. In [72], the authors consider a wireless control system comprising of multiple control loops, which are implemented over a shared wireless medium. A scheduler is designed to allocate non-overlapping frequencies to different control loops in order to meet stability requirement of control systems. To minimize the dependence of communication in CPS applications, Antunes et al.[73] proposed an event-triggered control methods that guarantee closed-loop improvements over traditional periodic transmission strategies.

Since control performance highly depends on signal exchange in CPS, there are a lots of works turning to co-design principle to guarantee the system performance. Goswami et al.[74] proposed a co-design principle for coordinating communication and control in a CPS architecture. Demirel et al.[75] consider the joint design of signal transmission and controller design for wireless control systems by utilizing MDP methods. Cao et al.[76] proposed a joint optimization framework incorporating the control objective and communication constraints considering the packet losses and physically constrained actuators' action.

The aforementioned articles mainly focus on controller design to fulfil the preliminary performance requirement of a CPS, such as closed-loop stability. Real-time is another important metric for CPS. Nowzari et al.[68] address the real-time implementation of distributed controller in networked CPS by combining the strength of event-triggered and self-triggered control. Giordano et al.[77] proposed a real-time control applied to drainage networks by merging gossip-based algorithm for a global correct behavior and PID control for local actuations. As the complexity of CPS increases, reliability is more challenging to maintain, especially in the presence of system failures. Moreover, traditional control theory lacks the necessary tools to analyze interconnected systems of heterogeneous components in large scale. Wu et al.[78] present a framework for benchmarking reliability of cyber-physical systems. Wang et al.[79] presents the L1Simplex architecture to handle a class of software and physical failures.

C. Future Direction

Stability is only one of the essential goals for controller design in CPS. Preserving compositionality in other properties, such as robustness, real-time, and other performance requirements are also an important and essential design goal. Co-design in CPS is an efficient way for system synthesis. Further development of powerful tools for analyzing and predicting the tight interaction between different modules in order to facilitate co-design is needed. Fundamental theoretical frameworks that can address the dynamics containing communication, computation, control and applications of CPS in a comprehensive manner is missing.

VI. Security

Security issues are vital in CPS due to the tight interaction between the physical world and the cyber world. Wide deployment of sensing, processing and communication devices in CPS introduce new security threats. Thus, the security problems and corresponding solutions are especially different and profound. Modeling and addressing security problems in CPS require a joint consideration of the cyber and physical components at the design stage. In fact, the cyber component and physical component are connected by information system. A lot of efforts have been made to secure the information system including sensing, communication and computation stages.

A. Security in Sensing

The cyber component observes the physical states by sensing and measurement. Effects and solutions of specific attacks have been studied. For instance, false data injection attack and corresponding countermeasures are proposed in [80−81]. Corrupted measurement data can be detected and isolated in the computation stage. Similarly, the deception and stealthy deception attacks against CPS are introduced in [82−83]. Even the attackers have limited capability, they can also inject false measurement data to the sensing stage not being detected by sensors. Reference [84] studies the effect of replay attacks on CPS. It shows that by introducing an additive noisy signal unknown to the attackers, the replay attacks can be detected by traditional detection mechanism. A malicious attacker can corrupt and alter the behavior of the physical plant as well as not being detected. This type of attack is called convert attacks and the effect of convert attacks is discussed in [85]. All the mentioned attacks aim to corrupt the sensing data. Denial of service attacks are in another way to prevent sensors from obtaining measurement data. The effect of denial of service and a semi-definite programming method to solve the attack problems are presented in [82].

B. Security in Communications

The goal of communication stage in CPS is to exchange information within cyber and physical systems as well as between them. Confidentiality, integrity and availability are the main security problems of communication[86]. However, traditional ICT security methods can not be applied directly to ensuring secure communication in CPS due to the interaction between physical process and cyber dynamics. A lot of works have been made to analyze the secure communication problem of specific CPS. Information flow is a fundamental concept underlying the secure communication of a CPS. A semantic model for information flow analysis in a CPS is presented in [87]. Reference [84] also describes an approach to perform the analysis, including both trace-based analysis and automated analysis through process algebra specification. Reference [88] investigates the vulnerability of the communication infrastructures in power systems and analyze how to mitigate data integrity attacks. A new metric to measure the security of information transmission is introduced to adapt the dynamic of

CPS in [89], and fundamental limit to guarantee the security is also analyzed. For large scale CPS communications, to meet the scalability, extensibility, and thinness requirements, [90] designed a resilient end-to-end message protection framework by exploiting the notion of the long-term key that is given on per node basis. The scheme in [91] can improve secure communications without compromising scalability and end-to-end security. For secure communication applications,[90] presented a secure and scalable data communications protocol for smart grid data collection under a hierarchical architecture, where relay nodes collect and convey the data securely from measurement devices to the power operator.

C. Security in Control

Security in control parts of a CPS is vital important, since a malicious party attacking the cyber infrastructure can interfere the normal operation of physical process. Information security has developed advanced technologies and tools that can prevent and react to attacks against control systems. However, research in computer security has focused traditionally on the protection of information without considering how attacks affect the physical world. Thus, in recent years there are numerous research on secure control consideration that is resilient to malicious attack. Before presenting the related works on security issues for CPS, the difference between fault-tolerant and secure control framework should be classified, since both mechanisms aim at mitigating or avoiding the abnormal system operation. Faults are limited by the physical dynamics and do not have an active intention to interfere, unlike cyber attacks that do have a malicious purpose and are not directly constrained by the dynamics of the physical process. In [92], the authors present a model to describe the adversary's intent that is to drive the physical plant to an unsafe state while remaining undetected by detectors. Reference [92] also proposes the analysis of attack and defense policies as well as the tools for risk assessment. The attack scenarios including denial-of-service, replay, zero-dynamics, and bias injection attacks on linear time-invariant systems are introduced in [93], where the attack's impact is characterized using the concept of safe sets. The authors in [94] design a stochastic model for CPS to investigate the repair policies for the corresponding failures from either cyber attacks or physical tampering. In real CPS, the platform can only reserve limited resources for security purposes, since controller performance highly depends on the available computation and communication resources in systems. Thus, the co-design for control scheme and security algorithm is needed. In [95], the authors quantify a tradeoff among control performance and system security in resource constrained CPS. Reference [96] fulfills the codesign principle from cross-layer point of view: the design of robust controller at physical layer takes into account risk of failures due to cyber system, while the design of security policies is based on its impacts on physical layer.

D. Future Direction

Possible future directions include the risk modeling methodology and subsequent risk index that should capture both the vulnerability of cyber networks and the potential impacts an adversary could inflict. The detection monitors are needed to be capable of revealing and locating attacks independently of the attack strategy and implementation. In addition, investigating the effect of partial knowledge of the parameters of the system on the strategies of both the attacker and the defender is an interesting future work.

VII. Applications in Vehicular Systems

CPS use computations and communication deeply embedded in and interacting with physical processes to add new capabilities to physical systems. This unique feature has been used in vehicular systems and networks. The development of communication and computing technique increases the capability of real-time data acquisition and local or remote computation which provide more accurate and timely information. Although utilizing CPS in vehicular systems and networks has huge potentiality to improve the efficiency and safety of vehicular systems and transportation, there are also challenges. The complexity of transportation system, positioning and data collection of high mobility vehicular system, the high requirements of accuracy and timeliness of data make a lot of difficulties in utilizing CPS in vehicular systems. Many aspects of works are discussed in recent researches, including data fusion and analysis, CPS design in vehicular systems and energy management in vehicular systems and so on. These aspects of CPS functions have been used in vehicular systems in recent researches.

Wu et al.[97] proposed a collision avoidance system, which can predict collision risks by comprehensively assessing vehicles location/motion, driver behavior and road geometry information from the vehicular CPS. The proposed vehicular CPS consist of five simulated components: vehicular sensors, roadside equipments, data fusion, risk assessment and warning devices. As sensors in this model are distributed, the process of information data fusion in order to predict vehicle location/motion and estimate the gap among vehicles nearby is necessary. The proposed method that can explicitly consider driver behavior and road geometry is used to predict vehicles position and calculate the travel distance real-time.

Sau et al.[98] proposed a particle-filter based real-time estimation and prediction model of intelligent traffic systems. Since the traffic models have the high nonlinearity characteristics, particle filter method is applied in combined with the celebrated first order macroscopic traffic model. The approach is an iterative stochastic approach that captures the dynamic behavior of traffic flow for the purpose of the travel time prediction. Then using Monte Carlo procedure the travel time estimation and prediction problem can be solved.

Jaeger et al.[99] described the scenario that the data in vehicular ad-hoc networks (VANETs) may not be trustworthy and potential attackers may exist and be able to get valid secret keys. The attackers may send authenticated messages with faked information mobility which can cause fault or error in VANETs. This article proposed novel framework for verifying mobility data, the goal of which is to detect messages representing non-plausible movement behavior with a Kalman

filter detecting malicious behavior based on past movements of vehicle.

Fallah et al.[100] examined characteristics of a cooperative vehicle safety system, and identified how the design and operation of such CPS should consider the tight coupling of computing and communications aspects of the system with its physical dynamics. This article proposed a novel method which models the behavior of each component as a function of the controllable parameters and measurable parameters of other components, in comparison with the traditional method each component is modeled separately.

Shen et al.[101] provided an efficient public key management system for vehicular ad-hoc networks (VANETs), which aims at offering a safety-related message access for drivers to make a life-critical decision for road safety enhancement. Although the guaranteeing communication message secure is vital for motorists, introducing secure services into VANETs which causes considerable transmission delays may defeat the purpose of improving road safety. This paper not only demonstrates that the proposed public key system can preserve security but also asserts that it can enhance overall performance at a lower cost.

Murphey et al.[102] propose an optimal online power management strategy applied to vehicular power system which serves multiple power sources and meets the largely fluctuated load requests. Hybrid vehicles of multiple power source have more complex configuration and more varieties of operation modes, thus power control strategy is more significant for fuel efficiency than conventional vehicle, which makes power management strategy vital for vehicular systems. The optimal online power strategy is presented with knowledge of machine learning and fuzzy logic.

VIII. Conclusions and Future Directions

This paper has comprehensively reviewed the research works in the design and application of CPS. The principle behind CPS places the focus on the integrated system design instead of on the cyber or the physical system independently. The all-in-one modeling methodology of CPS could improve design efficiency dramatically. The requirements of different parts in a CPS are summarized, which are followed by state of the arts. The future direction of each part is also pointed out. Vehicular systems and networks are used to illustrate the application of CPS in design. The progress made in the development of CPS will also greatly enhance their performance in many other important applications.

Next generation CPS are expected to be deployed with adequate scalability as well as reliable performance under dynamic conditions. In addition to the interaction between cyber and physical space, one should realize that CPS are becoming platforms. This trend is accompanied by the increasing system complexity. Many techniques, namely IoT, big data analysis, cloud computing are converged into the same platform. One typical example is Industry 4.0-based manufacturing system, which serves as a platform for different stakeholders on industry value chain to collaborate by sharing information in the cyber space and interact with each other in the physical world[26]. This modeling language shall cover control, communication and physical part described as a single model. We also need a novel software architecture to be applied across many application domains, and to provide solutions to resource management and security problems, as well as services that are application independent. However, current communication networks including heterogeneous networks are less considered to support interactions of multiple applications that use information on the same platform. Software-defined networking provides an architecture for resilient, adaptive and scalable systems of the future. To cope with control and design problems in such platform-like systems requires models, abstractions and methods that enable precise evaluation of design alternatives.

References

[1] Chen J, Yang B, Guan X P. Optimal demand response scheduling with stackelberg game approach under load uncertainty for smart grid. In: Proceedings of the 3rd IEEE International Conference on Smart Grid Communications (SmartGridComm). Tainan, China: IEEE, 2012. 546−551

[2] Li N, Chen L J, Low S H. Optimal demand response based on utility maximization in power networks. In: Proceedings of the 2011 IEEE Power and Energy Society General Meeting. San Diego, CA: IEEE, 2011. 1−8

[3] Deng R L, Chen J M, Cao X H, et al. Sensing-performance tradeoff in cognitive radio enabled smart grid. *IEEE Transactions on Smart Grid*, 2013, **4**(1): 302−310

[4] Calhoun B H, Lach J, Stankovic J, Wentzloff D D, Whitehouse K, Barth A T, Brown J K, Li Q, Oh S, Roberts N E, Zhang Y Q. Body sensor networks: a holistic approach from silicon to users. *Proceedings of the IEEE*, 2012, **100**(1): 91−106

[5] Fell M. Roadmap for the internet of things — its impact, architecture and future governance. *Carre & Strauss*, 2014.

[6] Wehrmeister M A, Pereira C E, Rammig F J. Aspect-oriented model-driven engineering for embedded systems applied to automation systems. *IEEE Transactions on Industrial Informatics*, 2013, **9**(4): 2373−2386

[7] Estevez E, Marcos M. Model-based validation of industrial control systems. *IEEE Transactions on Industrial Informatics*, 2012, **8**(2): 302−310

[8] Zotil A, Prahofer H. Guidelines and patterns for building hierarchical automation solutions in the IEC 61499 modeling language. *IEEE Transactions on Industrial Informatics*, 2013, **9**(4): 2387−2396

[9] Lee E A, Seshia S A. *Introduction to Embedded Systems, A Cyber-Physical Systems Approach*. Lulu.com, 2011.

[10] Han Y H, Kang S, Kim J. ExCHARON: improved modeling language for cyber-physical systems based on CHARON. In: Proceedings of the 16th IEEE International Conference on Computational Science and Engineering (CSE). Sydney, NSW: IEEE, 2013. 734−741

[11] Liu M X, Ma W B, Su D S, Huang H B. A new model language for cyber physical systems. In: Proceedings of the 2013 IEEE Conference on Information Science and Cloud Computing Companion (ISCC-C). Guangzhou, China: IEEE, 2013. 435−440

[12] Taha W, Brauner P, Zeng Y F, Cartwright R, Gaspes V, Ames A, Chapoutot A. A core language for executable models of cyber-physical systems (Preliminary report). In: Proceedings of the 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW). Macau, China: IEEE, 2013. 303−308

[13] Susuki Y, Koo T J, Ebina H, Yamazaki T, Ochi T, Uemura T, Hikihara T. A hybrid system approach to the analysis and design of power grid dynamic performance. *Proceedings of the IEEE*, 2012, **100**(1): 225−239

[14] Li H S, Lai L F, Poor H V. Multicast routing for decentralized control of cyber physical systems with an application in smart grid. *IEEE Journal on Selected Areas in Communications*, 2012, **30**(6): 1097−1107

[15] Li T, Tan F, Wang Q X, Bu L, Cao J N, Liu X. From offline toward real time: a hybrid systems model checking and cps codesign approach for medical device plug-and-play collaborations. *IEEE Transactions on Parallel and Distributed Systems*, 2014, **25**(3): 642−652

[16] Bak S, Johnson T T, Caccamo M, Sha L. Real-time reachability for verified simplex design. In: Proceedings of the 2014 IEEE Real-Time Systems Symposium (RTSS). Rome: IEEE, 2014. 138−148

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

[18] Akyildiz I F, Pompili D, Melodia T. Underwater acoustic sensor networks: research challenges. *Ad Hoc Networks*, 2005, **3**(3): 257−279

[19] Talcott C. Cyber-physical systems and events. *Software-Intensive Systems and New Computing Paradigms*. Berlin Heidelberg: Springer, 2008. 105−115

[20] Zhu Q Y, Bushnell L, Başar T. Resilient distributed control of multi-agent cyber-physical systems. *Control of Cyber-Physical Systems*. Switzerland: Springer, 2013.

[21] Le N T, Martin L, Mumme C, Pinkwart N. Communication-free detection of resource conflicts in multi-agent-based cyber-physical systems. In: Proceedings of the 6th IEEE International Conference on Digital Ecosystems Technologies (DEST). Campione, d'Italia: IEEE, 2012. 1−6

[22] Guedes G T A, Vicari R M. Applying AUML and UML 2 in the multi-agent systems project. *Advances in Conceptual Modeling-Challenging Perspectives*. Berlin Heidelberg: Springer, 2009. 106−115

[23] Lin J, Sedigh S, Miller A. A semantic agent framework for cyber-physical systems. *Semantic Agent Systems*. Berlin Heidelberg: Springer, 2011. 189−213

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

[25] Zhang L C. A framework to model big data driven complex cyber physical control systems. In: Proceedings of the 20th International Conference on Automation and Computing (ICAC). Cranfield: IEEE, 2014. 283−288

[26] Lee J, Bagheri B, Kao H A. A cyber-physical systems architecture for industry 4. 0-based manufacturing systems. *Manufacturing Letters*, 2015, **3**: 18−23

[27] Lee J, Kao H A, Yang S H. Service innovation and smart analytics for industry 4. 0 and big data environment. *Procedia CIRP*, 2014, **16**: 3−8

[28] Hsieh M A, Mallory K, Forgoston E, Schwartz I B. Distributed allocation of mobile sensing agents in geophysical flows. In: Proceedings of the 2014 IEEE American Control Conference (ACC). Portland, OR: IEEE, 2014. 165−171

[29] Zivan R, Yedidsion H, Okamoto S, Glinton R, Sycara K. Distributed constraint optimization for teams of mobile sensing agents. *Autonomous Agents and Multi-Agent Systems*, 2015, **29**(3): 495−536

[30] Du R, Chen C, Yang B, Lu N, Guan X P, Shen X M. Effective urban traffic monitoring by vehicular sensor networks. *IEEE Transactions on Vehicular Technology*, 2015, **64**(1): 273−286

[31] Work D B, Bayen A M. Impacts of the mobile internet on transportation cyberphysical systems: traffic monitoring using smartphones. In: Proceedings of the 2008 National Workshop for Research on High-Confidence Transportation Cyber-Physical Systems: Automotive Aviation, & Rail. Washington D. C., USA, 2008. 1−3

[32] Higashino T, Uchiyama A. A study for human centric cyber physical system based sensing: toward safe and secure urban life. *Information Search, Integration and Personalization, Communications in Computer and Information Science*. Berlin Heidelberg: Springer, 2013. 61−70

[33] Luo C, Wu F, Sun J, Chen C W. Compressive data gathering for large-scale wireless sensor networks. In: Proceedings of the 15th Annual International Conference on Mobile Computing and Networking (MobiCom). Beijing, China: ACM, 2009. 145−156

[34] Li W S, Zhu S Y, Chen C L, Guan X P. Distributed consensus filtering based on event-driven transmission for wireless sensor networks. In: Proceedings of the 31st Chinese Control Conference (CCC). Hefei, China: IEEE, 2012. 6588−6593

[35] Rana R, Yang M R, Wark T, Chou C T, Hu W. SimpleTrack: adaptive trajectory compression with deterministic projection matrix for mobile sensor networks. *IEEE Sensors Journal*, 2015, **15**(1): 365−373

[36] Nower N, Tan Y S, Lim A O. Efficient temporal and spatial data recovery scheme for stochastic and incomplete feedback data of cyber-physical systems. In: Proceedings of the 8th IEEE International Symposium on Service Oriented System Engineering (SOSE). Oxford: IEEE, 2014. 192−197

[37] Eldar Y C, Kutyniok G. *Compressed Sensing: Theory and Applications*. Cambridge: Cambridge University Press, 2012.

[38] Li Y, Tian C, Zhang F, Xu C Z. Traffic condition matrix estimation via weighted spatio-temporal compressive sensing for unevenly-distributed and unreliable GPS data. In: Proceedings of the 17th IEEE International Conference on Intelligent Transportation Systems (ITSC). Qingdao, China: IEEE, 2014. 1304−1311

[39] Du R, Chen C L, Yang B, Guan X P. VANET based traffic estimation: a matrix completion approach. In: Proceedings of the 2013 IEEE Global Communications Conference (GLOBECOM). Atlanta, USA: IEEE, 2013. 30−35

[40] Han D, Cheng P, Chen J M, Shi L. An online sensor power schedule for remote state estimation with communication energy constraint. *IEEE Transactions on Automatic Control*, 2014, **59**(7): 1942−1947

[41] Man K L, Wan K Y, Ting T O, Chen C, Krilavičius T, Chang J,

Poon S H. Towards a hybrid approach to SoC estimation for a smart battery management system (BMS) and battery supported cyber-physical systems (CPS). In: Proceedings of the 2nd IEEE Baltic Congress on Future Internet Communications. Vilnius: IEEE, 2012. 113−116

[42] Deshmukh S, Natarajan B, Pahwa A. State estimation in spatially distributed cyber-physical systems: Bounds on critical measurement drop rates. In: Proceedings of the 2013 IEEE Conference on Distributed Computing in Sensor Systems. Cambridge, MA: IEEE, 2013. 157−164

[43] Quevedo D E, Ostergaard J, Ahlen A. Power control and coding formulation for state estimation with wireless sensors. *IEEE Transactions on Control Systems Technology*, 2014, **22**(2): 413−427

[44] Leong A S, Quevedo D E, Ahln A, Johansson K H. Network topology reconfiguration for state estimation over sensor networks with correlated packet drops. In: Proceedings of the 19th IFAC World Congress on International Federation of Automatic Control. Cape Town, South Africa: IFAC, 2014. 5532−5537

[45] Leong A, Quevedo D. Kalman filtering with relays over wireless fading channels. *IEEE Transactions on Automatic Control* 2015 (accepted). DOI: 10.1109/TAC.2015.2478129

[46] Nourian M, Leong A S, Dey S. Optimal energy allocation for kalman filtering over packet dropping links with imperfect acknowledgments and energy harvesting constraints. *IEEE Transactions on Automatic Control*, 2014, **59**(8): 2128−2143

[47] Pajic M, Weimer J, Bezzo N, Tabuada P, Sokolsky O, Lee I, Pappas G J. Robustness of attack-resilient state estimators. In: Proceedings of the 2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS). Berlin, German: IEEE, 2014. 163−174

[48] Zonouz S, Rogers K M, Berthier R, Bobba R B, Sanders W H, Overbye T J. SCPSE: security-oriented cyber-physical state estimation for power grid critical infrastructures. *IEEE Transactions on Smart Grid*, 2012, **3**(4): 1790−1799

[49] Zhu S Y, Chen C L, Guan X P. Distributed optimal consensus filter for target tracking in heterogeneous sensor networks. In: Proceedings of the 8th Asian Control Conference (ASCC). Kaohsiung, China: IEEE, 2011. 806−811

[50] Khan U A, Stankovic A M. Secure distributed estimation in cyber-physical systems. In: Proceedings of the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Vancouver, BC: IEEE, 2013. 5209−5213

[51] Tang A L, Yu X, Kim S, Han J W, Peng W C, Sun Y Z, Leung A, La Porta T. Multidimensional sensor data analysis in cyber-physical system: an atypical cube approach. *International Journal of Distributed Sensor Networks*, 2012, **2012**: Article ID 724846

[52] Fang X, Misra S, Xue G L, Yang D J. Smart grid: the new and improved power grid: a survey. *IEEE Communications Surveys & Tutorials*, 2012, **14**(4): 944−980

[53] Cui Y, Lau V K N, Wang R, Huang H, Zhang S Q. A survey on delay-aware resource control for wireless systems–large deviation theory, stochastic Lyapunov drift, and distributed stochastic learning. *IEEE Transactions on Information Theory*, 2012, **58**(3): 1677−1701

[54] Lien S Y, Cheng S M, Shih S Y, Chen K C. radio resource management for QoS guarantees in cyber-physical systems. *IEEE Transactions on Parallel and Distributed Systems*, 2012, **23**(9): 1752−1761

[55] Zhu X, Yang B, Chen C, Xue L, Guan X P, Wu F. Cross-layer scheduling for ofdma-based cognitive radio systems with delay and security constraints. *IEEE Transactions on Vehicular Technology*, 2015, **64**(12): 5919−5934

[56] Seiler P, Sengupta R. Analysis of communication losses in vehicle control problems. In: Proceedings of the 2001 American Control Conference. Arlington, USA: IEEE, 2001. 1491−1496

[57] Ghaderi M, Towsley D, Kurose J. Reliability gain of network coding in lossy wireless networks. In: Proceedings of the 27th IEEE Conference on Computer Communications. Phoenix, USA: IEEE, 2008.1−6

[58] Laneman J N, Wornell G W. Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks. *IEEE Transactions on Information Theory*, 2003, **49**(10): 2415−2425

[59] Marchenko N, Andre T, Brandner G, Masood W, Bettstetter C. An experimental study of selective cooperative relaying in industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics*, 2014, **10**(3): 1806−1816

[60] Yang B, Shen Y Y, Johansson M, Chen C L, Guan X P. Opportunistic multichannel access with decentralized channel state information. *Wireless Communications and Mobile Computing*, 2015, **15**(2): 322−339

[61] Deng X, Yang Y Y. Communication synchronization in cluster-based sensor networks for cyber-physical systems. *IEEE Transactions on Emerging Topics in Computing*, 2013, **1**(1): 98−110

[62] Ehyaei A, Tovar E, Pereira N, Andersson B. Scalable data acquisition for densely instrumented cyber-physical systems. In: Proceedings of the 2011 IEEE/ACM International Conference on Cyber-Physical Systems (ICCPS). Chicago, USA: IEEE, 2011. 174−183

[63] Zhou J Z, Hu R Q, Qian Y. Scalable distributed communication architectures to support advanced metering infrastructure in smart grid. *IEEE Transactions on Parallel and Distributed Systems*, 2012, **23**(9): 1632−1642

[64] Han Q N, Yang B, Wang X C, Ma K, Chen C L, Guan X P. Hierarchical-game-based uplink power control in Femtocell networks. *IEEE Transactions on Vehicular Technology*, 2014, **63**(6): 2819−2835

[65] Yang B, Feng G, Shen Y Y, Long C N, Guan X P. Channel-aware access for cognitive radio networks. *IEEE Transactions on Vehicular Technology*, 2009, **58**(7): 3726−3737

[66] Wang Y B, Vuran M C, Goddard S. Cyber-physical systems in industrial process control. *ACM SIGBED Review*, 2008, **5**(1): Article No. 12

[67] Tabuada P, Caliskan S Y, Rungger M, Majumdar R. Towards robustness for cyber-physical systems. *IEEE Transactions on Automatic Control*, 2014, **59**(12): 3151−3163

[68] Nowzari C, Cortes J. Team-triggered coordination for real-time control of networked cyber-physical systems. *IEEE Transactions on Automatic Control*, 2015, **61**(1): 34−47

[69] Aminifar A, Eles P, Peng Z B, Cervin A. Control-quality driven design of cyber-physical systems with robustness guarantees. In: Proceedings of the 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE). Grenoble, France: IEEE, 2013. 1093−1098

[70] Molin A, Hirche S. Price-based adaptive scheduling in multi-loop control

systems with resource constraints. *IEEE Transactions on Automatic Control*, 2014, **59**(12): 3282−3295

[71] Trimpe S, Buchli J. Event-based estimation and control for remote robot operation with reduced communication. In: Proceedings of the IEEE International Conference on Robotics and Automation. Seattle, USA: IEEE, 2015. 5018−5025

[72] Gatsis K, Pajic M, Ribeiro A, Pappas G J. Opportunistic control over shared wireless channels. *IEEE Transactions on Automatic Control*, 2015, **60**(12): 3140−3155

[73] Antunes D, Heemels W P M H. Rollout event-triggered control: beyond periodic control performance. *IEEE Transactions on Automatic Control*, 2014, **59**(12): 3296−3311

[74] Goswami D, Schneider R, Chakraborty S. Co-design of cyber-physical systems via controllers with flexible delay constraints. In: Proceedings of the 16th Asia and South Pacific Design Automation Conference. Yokohama, Japan: IEEE, 2011. 225−230

[75] Demirel B, Zou Z H, Soldati P, Johansson M. Modular design of jointly optimal controllers and forwarding policies for wireless control. *IEEE Transactions on Automatic Control*, 2014, **59**(12): 3252−3265

[76] Cao X H, Cheng P, Chen J M, Sun Y X. An online optimization approach for control and communication codesign in networked cyber-physical systems. *IEEE Transactions on Industrial Informatics*, 2013, **9**(1): 439−450

[77] Giordano A, Spezzano G, Vinci A, Garofalo G, Piro P. A cyber-physical system for distributed real-time control of urban drainage networks in smart cities. *Internet and Distributed Computing Systems*. Switzerland: Springer International Publishing, 2014. 87−98

[78] Wu L, Kaiser G. FARE: a framework for benchmarking reliability of cyber-physical systems. In: Proceedings of the 2013 IEEE Long Island Systems, Applications and Technology Conference (LISAT). Farmingdale, NY: IEEE, 2013. 1−6

[79] Wang X F, Hovakimyan N, Sha L. L1Simplex: fault-tolerant control of cyber-physical systems. In: Proceedings of the 2013 ACM/IEEE International Conference on Cyber-Physical Systems. Philadelphia, PA: IEEE, 2013. 41−50

[80] Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security*, 2011, **14**(1): Article No. 13

[81] Pasqualetti F, Carli R, Bullo F A. A distributed method for state estimation and false data detection in power networks. In: Proceedings of the 2011 IEEE International Conference on Smart Grid Communications. Brussels, French: IEEE, 2011. 469−474

[82] Amin S, Cárdenas A, Sastry S S. Safe and secure networked control systems under denial-of-service attacks. *Hybrid Systems: Computation and Control*. Berlin Heidelberg: Springer, 2006. 31−45

[83] Teixeira A, Amin S, Sandberg H, Johansson K H, Sastry S S. Cyber security analysis of state estimators in electric power systems. In: Proceedings of the 49th IEEE Conference on Decision and Control. Atlanta, GA: IEEE, 2010. 5991−5998

[84] Mo Y L, Sinopoli B. Secure control against replay attacks. In: Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing. Monticello, IL, 2009. 911−918

[85] Smith R S. A decoupled feedback structure for covertly appropriating networked control systems. In: Proceedings of the 18th IFAC World Congress. Milano, Italy: IFAC, 2011. 90−95

[86] Gkoulalas-Divanis A, Loukides G, Xiong L, Sun J M. Informatics methods in medical privacy. *Journal of Biomedical Informatics*, 2014, **50**(1): 1−3

[87] Akella R, Tang H, McMillin B M. Analysis of information flow security in cyber-physical systems. *International Journal of Critical Infrastructure Protection*, 2010, **3**(3−4): 157−173

[88] Vukovic O, Sou K C, Dan G, Sandberg H. Network-aware mitigation of data integrity attacks on power system state estimation. *IEEE Journal on Selected Areas in Communications*, 2012, **30**(6): 1108−1118

[89] Li H S, Lai L F, Zhang W Y. Communication requirement for reliable and secure state estimation and control in smart grid. *IEEE Transactions on Smart Grid*, 2011, **2**(3): 476−486

[90] Uludag S, Lui K S, Ren W, Nahrstedt K. Secure and scalable data collection with time minimization in the smart grid. *IEEE Transactions on Smart Grid*, 2016, **7**(1): 43−54

[91] Kim Y J, Kolesnikov V, Thottan M. Resilient end-to-end message protection for large-scale cyber-physical system communications. In: Proceedings of the 3rd IEEE International Conference on Smart Grid Communications (SmartGridComm). Tainan, China: IEEE, 2012. 193−198

[92] Teixeira A, Sou K C, Sandberg H, Johansson K H. Secure control systems: a quantitative risk management approach. *IEEE Control Systems*, 2015, **35**(1): 24−45

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

[94] Sleptchenko A, Johnson M E. Maintaining secure and reliable distributed control systems. *Informs Journal on Computing*, 2015, **27**(1): 103−117

[95] Pasqualetti F, Zhu Q. Design and operation of secure cyber-physical systems. *IEEE Embedded Systems Letters*, 2015, **7**(1): 3−6

[96] Zhu Q Y, Basar T. Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. *IEEE Control Systems*, 2015, **35**(1): 46−65

[97] Wu C Z, Peng L Q, Huang Z, Zhong M, Chu D F. A method of vehicle motion prediction and collision risk assessment with a simulated vehicular cyber physical system. *Transportation Research, Part C: Emerging Technologies*, 2014, **47**: 179−191

[98] Sau J, El Faouzi N E, Billot R, Canaud M. Particle filter-based strategy for online calibration and parameter estimation of motorway traffic model. In: Proceedings of the 2013 Transportation Research Board (TRB) 92nd Annual Meeting. Washington, D. C, USA, 2013. 1−8

[99] Jaeger A, Bimeyer N, Stübing H, Huss S A. A novel framework for efficient mobility data verification in vehicular ad-hoc networks. *International Journal of Intelligent Transportation Systems Research*, 2012, **10**(1): 11−21

[100] Fallah Y P, Huang C L, Sengupta R, Krishnan H. Design of cooperative vehicle safety systems based on tight coupling of communication,

computing and physical vehicle dynamics. In: Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS). New York, USA: ACM, 2010. 159−167

[101] Shen P Y, Liu V, Tang M L, Caelli W. An efficient public key management system: an application in vehicular ad hoc networks. In: Proceedigns of the 2011 Pacific Asia Conference on Information Systems (PACIS). Brisbane: AIS Electronic Library, 2011. 175

[102] Murphey Y L, Chen Z H, Kiliaris L, Masrur M A. Intelligent power management in a vehicular system with multiple power sources. *Journal of Power Sources*, 2011, **196**(2): 835−846

Xinping Guan received the Ph. D. degree in control and systems from Harbin Institute of Technology, China. He joined the Department of Automation, Shanghai Jiao Tong University, China in 2007 where he is currently a chair professor, director of Key Laboratory of Systems Control and Information Processing, Ministry of Education of China. He has authored and/or coauthored 3 research monographs, more than 120 journal papers in IEEE Transactions and other well-known international journals and numerous conference papers. His research interests include wireless sensor networks, ground-air communication of aircrafts, and cognitive radio networks and their applications in industry.

Prof. Guan is currently a committee member of Chinese Automation Association Council and Chinese Artificial Intelligence Association Council. He served/serves as Associate Editor for *IEEE Transaction on System, Man, and Cybernetics-C*, and several Chinese journals and as international technical committee member for a lot of conferences.

Bo Yang obtained the Ph. D. degree in electrical engineering from City University of Hong Kong in 2009. Prior to joining Shanghai Jiao Tong University as an assistant professor in 2010, he was a postdoctoral researcher at the Royal Institute of Technology (KTH), Sweden from 2009-2010 and a visiting scholar at the Polytechnic Institute of New York University in 2007. He is now a full professor in Shanghai Jiao Tong University. He is also a cyber scholar with the Cyber Joint Innovation Center founded by Zhejiang University, Tsinghua University, and Shanghai Jiao Tong University.

His research interests include game theoretical analysis and nonlinear optimization of communication networks and smart grid. He is on the editorial board of *Digital Signal Processing*-Elsevier and in the TPC of several international conferences.

Dr. Yang has been the principle/co-investigator in several research projects funded by NSF of China, Swedish Governmental Agency for Innovation Systems and US air force. He is a member of IEEE and ACM. Corresponding author of this paper.

Cailian Chen received the Ph. D. degree in control and systems from City University of Hong Kong in 2006. She currently is a professor with Shanghai Jiao Tong University, Shanghai, China. Her research interests include vehicular ad hoc network, wireless sensor and actuator network, multi-agent systems and non-linear systems. She has authored and/or coauthored 2 research monographs and over 80 referred international journal and conference papers in the areas of intelligent control, nonlinear systems and wireless sensor networks.

Dr. Chen is a member of IEEE. She serves as an associate editor of *IEEE Transactions on Vehicular Technology and Peer-to-Peer Networking and Applications* (Springer), and TPC member of lots of conferences including IEEE Infocom, IEEE Globecom, IEEE ICC, and IEEE WCCI.

Wenbin (William) Dai is an assistant professor at Shanghai Jiao Tong University, China. He received a bachelor of engineering (with honours) degree in computer systems engineering from the University of Auckland, New Zealand in 2006. He completed Ph. D. in electrical and electronic engineering in the Department of Electrical and Computer Engineering, The University of Auckland, New Zealand in 2012. He was a postdoctor fellow at Lulea University of Technology, Sweden from 2013 to 2014. He was also a software engineer from Glidepath Limited, a New Zealand based airport baggage handling system provider from 2007 to 2013. His research interests include IEC 61131-3 PLC, IEC 61499 function blocks, industrial cyber-physical systems, cloud-based simulation and software architecture in industrial automation.

Yiyin Wang received the B. S. degree in electrical engineering from Fudan University, Shanghai, China, in 2002, the M. S. degree (*cum laude*) in microelectronics from Delft University of Technology (TU Delft), The Netherlands, and Fudan University, China, in 2005, respectively, and the Ph. D. degree in electrical engineering from TU Delft, The Netherlands, in 2011. She is currently an associate professor in the Department of Automation, Shanghai Jiao Tong University, China. Prior to that, she was a research assistant at the Circuits and Systems group (CAS), TU Delft from 2006 to 2007. From February 2010 till July 2010, she visited Georgia Institute of Technology (Gatech), Atlanta, USA. She was a postdocor fellow at TU Delft and then Gatech from 2011 to 2013. Her research interests include the general area of signal processing for communications and networking. Her research interests include tracking, localization, and synchronization for wireless sensor networks and underwater sensor networks.