Guest Editorial
Distributed Signal Processing for Security and Privacy in Networked Cyber-Physical Systems

NETWORKED cyber-physical systems (CPSs) are engineering systems with integrated computational and communication capabilities that interact with humans through cyber space. The CPSs have recently emerged in several practical applications of significant engineering importance including aerospace, industrial/manufacturing process control, multimedia networks, transportation systems, power grids, and medical systems. The CPSs typically consist of both wireless and wired sensor/agent networks with different capacity/reliability levels where the emphasis is on real-time operations, and performing distributed, secure, and optimal sensing/processing is the key concern. To satisfy these requirements of the CPSs, it is of paramount importance to design innovative "Signal Processing" tools to provide unprecedented performance and resource utilization efficiency. The spirit and wide scope of distributed signal processing in revolutionized CPSs calls for novel and innovative techniques beyond conventional approaches to provide precise guarantees on security and privacy of CPSs. In light of these considerations, it is not difficult to appreciate the timeliness of this special issue. The articles appearing in the issue help illustrate the fundamental role that distributed signal processing plays for making networked CPSs secure and protect our privacy.

I. Introduction

A significant challenge for implementation of signal processing solutions in CPSs is the difficulty of acquiring data from geographically distributed observation nodes and storing/processing the aggregated data at the fusion centre (FC). As such, there has been a recent surge of interest in development of distributed and collaborative signal processing technologies where adaptation, estimation, and/or control are performed locally and communication is limited to local neighbourhoods. Distributed signal processing over networked CPSs, however, raise significant privacy and security concerns as local observations are being shared by neighbouring nodes in a collaborative and iterative fashion. On the one hand, applications of CPSs are severely safety critical where potential cyber and physical attacks by adversaries on signal processing modules could lead to a variety of severe consequences including customer information leakage, destruction of infrastructures, and endangering human lives. On the other hand, the need for cooperation between neighbouring nodes makes it imperative to prevent the disclosure of sensitive local information during distributed information fusion step. At the same time, efficient usage of available resources (communication, computation, bandwidth, and energy) is a prerequisite for productive operation of the CPSs. To accommodate these critical aspects of CPSs, it is of great practical importance and theoretical significance to develop advanced "Secure and Privacy Preserving Distributed Signal Processing" solutions.

The objective of this special issue is to further advance recent developments of distributed signal processing to practical aspects of CPSs for real-time processing and monitoring of the underlying system in a secure and privacy preserving manner while avoiding degradation of the processing performance and preserving the valuable resources. To provide a systematic base for future advancements of CPSs, this special issue aims to provide a research venue to investigate distributed signal processing techniques with adaptation, cooperation, and learning capabilities which are secure against cyber attacks and protected against privacy leaks. The emphasis of this special issue is on distributed/network aspects of security and privacy in CPSs.

II. Summary of Articles

The Guest Editors would like to express their deepest gratitude to the many reviewers who have helped them to improve the quality of the final articles. They are confident that readers will find this collection of articles interesting and appealing.

1) *"Differentially Private Distributed Online Algorithms Over Time-Varying Directed Networks"* by Zhu *et al.* The authors consider a private distributed online optimization problem (PDOOP) where a set of agents aim to minimize the sum of locally convex cost functions while each desires that the local cost function of individual agent is kept differentially private.
2) *"Mitigation of Byzantine Attacks on Distributed Detection Systems Using Audit Bits"* by Hashlamoun *et al.* The authors propose a novel mechanism to mitigate Byzantine attacks by partitioning sensors into groups developed for distributed detection problems in the presence of Byzantines who seek to degrade detection performance by falsifying data.
3) *"Two-Tier Device-Based Authentication Protocol Against PUEA Attacks for IoT Applications"* by Lin *et al.* The authors consider a hierarchical cognitive internet of things (IoT) architecture and propose a novel methodology of spectrum management that can guard against common types of security threats despite the limitations of the local processing.
4) *"Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks"* by Guan and Ge. The authors construct resilient attack detection estimators to provide locally reliable state estimations and

Digital Object Identifier 10.1109/TSIPN.2018.2801659

detect the false data injection attack for the problem of joint distributed attack detection and distributed secure estimation for a networked cyber-physical system under physical and cyber attacks.

5) *"Resilient Consensus With Mobile Detectors Against Malicious Attacks"* by Zhao *et al.* The authors investigate the problem of resilient consensus under malicious attacks for multi-agent systems by considering a general attack model, where malicious agents can neighbor and collude with each other and the number of tolerable attacks is not limited by the network connectivity. In this regard, the resilient consensus algorithm with mobile detectors (MRCA) is designed.
6) *"A Distributed Control Paradigm for Smart Grid to Address Attacks on Data Integrity and Availability"* by Farraj *et al.* The authors propose an adaptive cyber-enabled parametric feedback linearization (PFL) control scheme for transient stability of smart grids, which utilizes a distributed energy storage system to modify the dynamics of the power system during transients.
7) *"Privacy Aware Stochastic Games of Distributed End-User Energy Storage Sharing"* by Yao *et al.* The authors propose a game theoretical framework to capture the competitive behaviors of users sending messages through a communication network to an independent battery controller with an infinite horizon limiting average signaling game formulation.
8) *"Distributed Joint Attack Detection and Secure State Estimation"* by Forti *et al.* The authors address the joint task of detecting attacks and securely monitoring the state of a cyber-physical system over a cluster-based network wherein multiple fusion nodes collect data from sensors and cooperate in a neighborwise fashion in order to accomplish the task.
9) *"Secure Information Sharing in Adversarial Adaptive Diffusion Networks"* by Ntemos *et al.* The authors consider information sharing over adversarial adaptive networks, and for defense against adversarial attacks propose an attack detection mechanism that guides the diffusion strategy in the parameter estimation task and the transmission decisions of agents.
10) *"A Novel Data Fusion Algorithm to Combat False Data Injection Attacks in Networked Radar Systems"* by Yang *et al.* The authors take the first attempt to investigate the false data injection (FDI) attack's effects on a networked radar system, and propose a novel data fusion algorithm to combat this attack.
11) *"Distributed Graph-based Statistical Approach for Intrusion Detection in Cyber-Physical Systems"* by Sadreazami *et al.* The authors propose a novel distributed blind intrusion detection framework by modeling sensor measurements as the target graph-signal and utilizing the statistical properties of the graph-signal for intrusion detection.
12) *"Distributed Privacy-Preserving Collaborative Intrusion Detection Systems For VANETs"* by Zhang and Zhu. The authors propose a privacy-preserving machine learning based collaborative intrusion detection system (PML-CIDS) for vehicular ad hoc network (VANET).

A. MOHAMMADI, *Lead Guest Editor*
Concordia Institute for Information System Engineering
Concordia University
Montreal, QC H3G-2W1, Canada

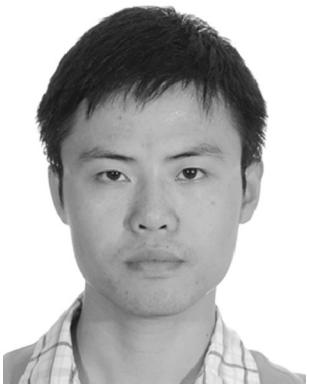
P. CHENG, *Guest Editor*
Department of Control Science and Engineering
Zhejiang University
Hangzhou 310027, China

V. PIURI, *Guest Editor*
Department of Information Technology
Università degli Studi di Milano
Crema, CR 26013, Italy

K. N. PLATANIOTIS, *Guest Editor*
Department of Electrical and Computer Engineering
University of Toronto
Toronto, ON M5S-3G4, Canada

P. CAMPISI, *Guest Editor*
Department of Applied Electronics
Università degli Studi Roma Tre
Rome 00146, Italy

Arash Mohammadi (S'08–M'14–SM'17) received the B.Sc. degree from the University of Tehran, Tehran, Iran, in 2005, the M.Sc. degree from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, in 2007, and the Ph.D. degree from York University, Toronto, ON, Canada, in 2013. He is currently an Assistant Professor with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC, Canada. Prior to joining Concordia University, he was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada. He is the Director-Membership Services of the IEEE Signal Processing Society, and the Vice-Chair of the IEEE Signal Processing Montreal Chapter. He was the Organizing Committee chair of "IEEE Signal Processing Society Winter School on Distributed Signal Processing for Secure Cyber-Physical Systems", the Co-Chair of the "Symposium on Advanced Bio-signal Processing for Rehabilitation & Assistive Systems," as part of IEEE GlobalSIP'17, and a Co-Organizer of the Special Session on "Bio-Signal Processing for Movement Assessment, Neuro-Rehabilitation and Assistive Technologies," in IEEE SMC'17. He is a co-organizer of the Special Session on "Advanced Machine Learning and Bio-Signal Processing for Rehabilitation and Assistive System" in IEEE SMC'18. His research interests include cyber-physical systems, information fusion, distributed signal processing for agent networks, secure networked control systems, biomedical signal processing, consensus algorithms, large-scale dynamical systems, and smart grids. He was the recipient of several distinguishing awards, including the Eshrat Arjomandi Award for outstanding Ph.D. dissertation from York University, in 2013.



Peng Cheng (M'10) received the B.E. degree in automation and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2004 and 2009, respectively. He is currently a Professor with the College of Control Science and Engineering, Zhejiang University. He is currently an Associate Editor of the IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS, *Wireless Networks*, and *International Journal of Communication Systems*. He was the Guest Editor of the IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS. He was the TPC co-chair of the IEEE IOV 2016, the local arrangement co-chair for ACM MobiHoc 2015, and the publicity co-chair for IEEE MASS 2013. His research interests include networked sensing and control, control system security, and cyber-physical systems.

Vincenzo Piuri (F'01) received the Ph.D. degree in computer engineering from Politecnico di Milano, Milan, Italy, in 1989. He has been an Associate Professor with Politecnico di Milano and a Visiting Professor with the University of Texas at Austin, Austin, TX, USA, and George Mason University, Fairfax, VA, USA, respectively. Since 2000, he has been a Full Professor in computer engineering at the Università Degli Studi di Milano, Milan. His current research interests include signal and image processing, biometrics, pattern analysis and recognition, and machine learning. He has authored or co-authored more than 400 papers in international journals, proceedings of international conferences, books, and book chapters. He is a Distinguished Scientist of the Association for Computing Machinery. He is the Editor-in-Chief of the IEEE SYSTEMS JOURNAL. He has been the 2015 IEEE Vice President for Technical Activities and the IEEE Director.

Konstantinos N. Plataniotis (S'93–M'95–SM'03–F'12) is currently a Professor and the Bell Canada Chair in Multimedia with the ECE Department, University of Toronto, Toronto, ON, Canada. He is the Founder and inaugural Director-Research for the Identity, Privacy, and Security Institute, the University of Toronto and was the Director for the Knowledge Media Design Institute, University of Toronto from January 2010 to July 2012. His research interests include knowledge and digital media design, multimedia systems, biometrics, image & signal processing, communications systems, and pattern recognition. Among his publications in these fields are the books *WLAN Positioning Systems* (Cambridge Univ. Press, 2012) and *Multilinear Subspace Learning: Reduction of Multidimensional Data* (CRC Press, 2013). He is a Registered Professional Engineer in Ontario, and the Fellow of the Engineering Institute of Canada. He has served as the Editor-in-Chief of the IEEE SIGNAL PROCESSING LETTERS, as the Technical Co-Chair of the IEEE 2013 International Conference in Acoustics, Speech and Signal Processing, the General Co-Chair of the IEEE 2017 Global Signal Processing Conference, and as the IEEE Signal Processing Society Vice President for Membership (2014–2016). He is the General Chair for the 2018 International Conference on Image Processing, and the General Chair of the 2021 IEEE International Conference on Acoustics, Speech and Signal Processing.

Patrizio Campisi (SM'08) received the Ph.D. degree in electronic engineering from Roma Tre University, Rome, Italy. He is currently a Full Professor with the Section of Applied Electronics, Department of Engineering, Roma Tre University. His current research interests include secure multimedia communications and biometrics. Specifically, he has been working on secure biometric recognition, image deconvolution, image analysis, stereo image and video processing, blind equalization of data signals, and secure communications. He is an Editor of the books *High Dynamic Range Video, Concepts, Technologies and Applications*, (Academic Press, 2016), *Security and Privacy in Biometrics*, (Springer, 2013), and *Blind Image Deconvolution: Theory and Applications* (CRC Press, 2007). He is the General Chair of the 26th European Signal Processing Conference, Rome, in 2018. He was the General Chair of the 12th ACM Workshop on Multimedia and Security, Rome, in 2010, and the seventh IEEE Workshop on Information Forensics and Security (WIFS), Rome, in 2015. He was the Technical Co-Chair of the Fourth IEEE WIFS, Spain, in 2012, and the First ACM Workshop on Information Hiding and Multimedia Security, France, in 2013. He has been a member of the IEEE Certified Biometric Program Learning System Committee. He was a co-recipient of the IEEE ICIP06 and the IEEE BTAS 2008 Best Student Paper Award, and the IEEE Biometric Symposium 2007 Best Paper Award. He has served as the IEEE Director for Student Services of the Signal Processing Society from 2015 to 2017. He is the Chair of the IEEE Technical Committee on Information Forensics and Security of the Signal Processing Society from 2017 to 2018 and the IEEE Italy Section Biometric Council from 2018 to 2020. He has been an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and both an Associate Editor and a Senior Associate Editor of the IEEE SIGNAL PROCESSING LETTERS. He is the Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (2018–2020).