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

GUEST EDITORS

Arash Mohammadi, Concordia University, Montreal, Canada, arashmoh@encs.concordia.ca
Peng Cheng, Zhejiang University, Hangzhou, China, pcheng@iipc.zju.edu.cn
Vincenzo Piuri, Universita degli Studi di Milano, Milan, Italy, vincenzo.piuri@unimi.it
Konstantinos N. Plataniotis, University of Toronto, Toronto, Canada, kostas@ece.utoronto.ca
Patrizio Campisi, Universitá degli Studi Roma Tre, Italy, patrizio.campisi@uniroma3.it

SCOPE

The focus of this special issue is on distributed information acquisition, estimation, and adaptive learning for security and privacy in the context of networked cyber-physical systems (CPSs) which 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 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.

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 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 pre-requisite 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 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. 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. Papers with primary emphasis on forensics and security will be redirected to IEEE Transactions on Information Forensics and Security (TIFS). Topics of interest include, but are not limited to:

- Security and Privacy of distributed signal processing in networked CPSs.
- Distributed and secure detection, estimation, and information fusion.
- Security and privacy of consensus and diffusive strategies in networked systems.
- Secure and privacy preserving distributed adaptation and learning.
- Security and privacy of distributed sensor resource management in networked systems.
- Distributed event-based estimation/control in networked CPSs.
- Detection and identification of potential attacks on distributed signal processing mechanisms.
- Application domains including but not limited to, smart grids, camera networks, multimedia network, and vehicular networks.

SUBMISSION GUIDELINES

Authors are invited to submit original research contributions by following the detailed instructions given in the "Information for Authors" at `http://www.signalprocessingsociety.org/publications/periodicals/tsipn/`. Manuscripts should be submitted via Manuscript Central at `http://mc.manuscriptcentral.com/tsipn-ieee` . Questions about the special issue should be directed to the Guest Editors.

TENTATIVE SCHEDULE

Paper submission deadline:	December 15, 2016	Final notification:	September 1, 2017
Notification of the first review:	March 1, 2017	Final manuscript:	October 15, 2017
Revised paper submission:	April 15, 2017	Publication:	Advance posting in IEEE explore as soon as authors approve galley proofs
Notification of the re-review:	June 15, 2017		
Minor revision deadline:	August 1, 2017	Expected inclusion in an issue:	March 2018