UNIVERSITY OF TORONTO
Identity, Privacy & Security Institute

The IPSI Lecture Series Presents:

Secure State Estimation in Cyber-Physical Systems/Smart Grids: Challenges and Opportunities

Professor Arash Mohammadi
Concordia University

We live in an era of data deluge. The volume, variety, and velocity of data is exploding and the ability to process such large amounts of information promises to limit the spread of epidemics, learn the dynamics of emergent social-computational systems, and protect critical infrastructures. Of particular interest to this talk is security and privacy issues associated with the big data collected from Cyber-Physical Systems (CPS), which exhibit a wide range of diversities. The CPSs are engineering systems with embedded control, communication and sensing capabilities that can interact with humans through cyber space. The rapid growth of CPSs and the fact that privacy and security are key concerns in this context makes identification and prevention of cyber-attacks and development of privacy preserving mechanisms of significant practical importance. The first part of this talk is devoted to large-scale CPSs with nonlinear dynamics and sparse observations. I present a multi-rate consensus/fusion based distributed estimation framework for scenarios where network connectivity is intermittent. A novel distributed sensor selection algorithm is then presented with the objective of dynamically activating a time-variant subset of sensor nodes for adaptive resource management in CPSs. The second part of this talk is motivated by recent evolution of cutting-edge smart-sensor technologies (smart-meters) in CPSs. Managing privacy and security of such new technologies is of paramount importance in future smart grid and smart metering networks. This talk will explore different aspects of security and privacy issues related to smart metering systems. Data injection attack models will then be reviewed and a specific attack model for compromising Phasor Measurement Units (PMUs) will be discussed in more details. Talk will be concluded by summarizing challenges and opportunities in developing privacy preserving and secure methodologies for future CPSs.

Thursday, February 02, 2017

12:00 PM – 1:15 PM

Rosebrugh Building, RM 211

164 College Street Toronto, ON, M5S 3G9

Arash Mohammadi (S'08-M'13) received B.Sc. degree from University of Tehran in 2005, the M.Sc. degree in from Amirkabir University of Technology (Tehran Polytechnic) in 2007, and Ph.D. from York University in 2013. He is currently an Assistant Professor with Concordia Institute for Information Systems Engineering (CIISE), Concordia University, Montreal, Canada. Prior to joining Concordia University, he was a Postdoctoral Fellow at Department of Electrical and Computer Engineering, University of Toronto, Canada. He is the Vice-Chair of IEEE Signal Processing Montreal Chapter. He serves as the leading Guest Editor in IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORKS on "Distributed Signal Processing for Security and Privacy in Networked Cyber-Physical Systems". He was the Organizing Committee chair of "IEEE Signal Processing Society Winter School on Distributed Signal Processing for Secure Cyber-Physical Systems". His research interests include: cyber-physical systems; information fusion; distributed signal processing for agent networks; secure networked control systems; consensus algorithms, large-scale dynamical systems, and; smart grids. He has authored about 50 technical contributions, including invited ones, published in international journals and conference proceedings of high caliber. Dr. Mohammadi has received several distinguishing awards, including the Eshrat Arjomandi Award for outstanding Ph.D. dissertation from Electrical Engineering and Computer Science Department of York University in 2013, and one of the best student paper awards from IEEE International Conference on Information Fusion.

IPSI

Bahen Centre, RM 7208
40 St. George Street, Toronto ON M5S 2E4
E ipsi@utoronto.ca W www.ipsi.utoronto.ca