Open Invited Track Session Proposal IFAC 2017

Title: Security and Privacy for Networked Multi-agent Cyber-physical systems

Organizers:

Prof Subhrakanti Dey (Signals & Systems, Uppsala University, Sweden)
Prof Ling Shi (Hong Kong University of Science & Technology, Hong Kong, China)
Prof George Pappas (Dept of Electrical & Systems Engineering, University of Pennsylvania, USA)
Prof Bruno Sinopoli (Dept of ECE, Carnegie Mellon University, USA)

Abstract:

Cyber-physical systems will constitute many of the next generation engineered systems, integrating control, communication and computing together, and forming the core of many important future critical infrastructure facilities, advanced healthcare systems, and smart autonomous systems. Ensuring security and privacy of such systems from malicious attackers is critical. Recent surge of research activities in cyber-physical security of networked cyber-physical systems confirms the need and importance of such research. In the proposed invited session, we are soliciting contributions that investigate security and privacy of multi-agent networked cyber-physical systems from a variety of view-points, such as (i) cyber-physical security of networked control systems, (ii) game-theoretic security and privacy of networked systems, (iii) information-theoretic security and privacy of cyber-physical systems, as well as application-specific investigations in large-scale process control systems, smart grid and industrial automation for example.

IFAC Technical Committee (for evaluation):

TC 1.5 Networked Systems

Description:

Cyber- physical systems (CPS) refer broadly to the next generation of engineered systems that require efficient integration of computing, communication, and control technologies, achieving stability, robustness, reliability and optimized performance in many important application domains, such as future intelligent transportation systems, advanced healthcare, industrial automation, and "smart" power grids. The ubiquitous connectivity of such networks, and the use of off-the-shelf networking and computing devices in integrating control, computing and communications leave them vulnerable to malicious attacks, resulting in a complete shutdown or unsafe operation of critical infrastructure facilities. As CPS will form the core of many critical infrastructure facilities such as power grids, advanced healthcare systems etc., ensuring their safety and reliability is crucial. It has been illustrated that traditional *cryptographic cyber security*

Proposal submitted to 20th IFAC World Congress. Received July 19, 2016.

measures are not always sufficient for CPS, as these tools are ineffective against physical attacks or attacks launched by authenticated users. A recent example of a physical attack was the “Stuxnet Attack” which resulted in a complex malware infecting uranium enrichment facilities in Iran and causing damage to approximately 1000 centrifuges at these plants in 2010. Current supervisory control systems used in power networks such as SCADA are also prone to such cyber-physical attacks, as demonstrated via various recent unauthorized intrusions into the US electricity grid. These events have clearly demonstrated that traditional IT security, while being important for NCS consisting of feedback loops, provides a partial solution only to CPS security.
This has motivated researchers in diverse areas to look beyond cryptographic security and use alternative techniques to enhance security of communication networks and systems, and CPS and their underlying networked control systems. These techniques include but are not limited to (i) Control-theoretic cyber-physical security, (ii) Game-theoretic security and (iii) Information-theoretic security.

Cyber-physical attacks can affect the integrity, availability and confidentiality in CPS. Examples range from deception based attacks such as *false-data-injection, sensor and actuator attacks, replay attacks,* and also *denial-of-service attacks*. Documented defence mechanisms can range from attack identification and detection, intrusion detection as well as physical watermarking of valid control signals, or a stochastic game theory based approach that treats the true controller and the adversary/attacker as competitive decision makers. Although not widely explored in the context of CPS security, stochastic game-theoretic methods are commonly exploited for network security. Additionally, the notion of *information-theoretic security*, based on an extension of Claude Shannon’s notion of perfect secrecy has recently seen a surge of research activities in the wireless communication literature, especially in the context of *physical layer security,* which defines the so-called “secrecy rate” – the notion of reliable transmission rate to a desired user while keeping information private from an adversary/eavesdropper. Information theoretic security techniques are only beginning to make inroads into networked CPS with initial investigations being limited to optimizing specific control performance while minimizing information leakage to an adversary.

Finally, unlike CPS security, a related issue of “privacy preservation” of information during distributed operation in CPS has not received as much attention until recently. A critical example is medical CPS where lack of such privacy can result in confidential patient data being compromised leading to misuse or abuse of such data. Based on the concept of “differential privacy” borrowed from the database literature, differentially private Kalman filters, and consensus algorithms have been recently designed, which have strong relevance for CPS. This notion of privacy can protect sensitive individual information submitted to databases for statistical or aggregate information extraction.

Consequently, we have already noticed a proliferation of special issue proposals on related topics in various journals and magazines that are either already published or currently under submission and review process. Examples include the (i) IEEE Control Systems Magazine, February 2015 Special issue on Cyber-physical security, (ii) Special issue on secure control of CPS for IEEE Transactions on Control of Network Systems (publication date: March 2017), and (iii) a more recent call on IEEE Transactions on Signal and Information Processing over Networks Special Issue on Distributed Signal Processing for Security and Privacy in Networked Cyber-Physical Systems (call published July 2016).

Based on this exciting premise of a multi-disciplinary investigation into security and privacy of networked multi-agent CPS, this highly topical open invited track session proposal solicits papers in the following broad areas (but not limited to):

(i) Control-theoretic attack detection, identification and mitigation in multi-agent networked CPS,

(ii) Game-theoretic techniques in mitigating deception and denial-of-service attacks,

(iii) Enhancing security of networked control systems via novel physical-layer authentication algorithms

(iv) Privacy preserving distributed control/optimization algorithms in networked multi-agent CPS

(v) Information-theoretic security and privacy measures in networked multi-agent CPS

(vi) Exploration of trust and reputation based distributed optimization algorithms in multi-agent CPS,

(vii) Design of security and privacy enhancing algorithms under computation and communication constraints in networked CPS, and

(viii) Enhancing security and privacy in specific application areas such as smart grid, large-scale process control systems and industrial automation in general

Further References:

[1] http://sites.bu.edu/tcns/special-issue-on-secure-control-of-cyber-physical-systems/

[2] https://signalprocessingsociety.org/blog/tsipn-special-issue-distributed-signal-processing-security-and-privacy-networked-cyber-physical

[3] H. Sandberg, S. Amin and K.H. Johansson, "Cyber-physical Security in Networked Control Systems: An Introduction to the Issue," IEEE Control Systems Magazine, February 2015 http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=7011179