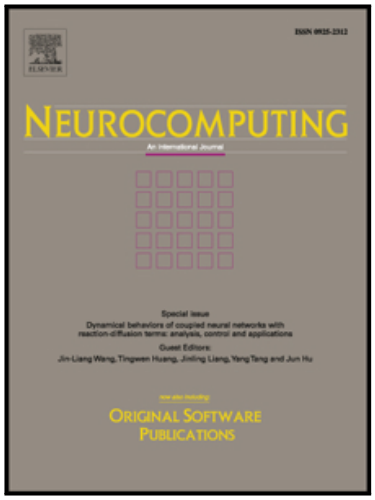
Communicated by Prof. Zidong Wang

Accepted Manuscript



A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems

Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, Xian-Ming Zhang

PII: S0925-2312(17)31635-1
DOI: 10.1016/j.neucom.2017.10.009
Reference: NEUCOM 18989

To appear in: *Neurocomputing*

Received date: 22 August 2017
Revised date: 6 October 2017
Accepted date: 6 October 2017

Please cite this article as: Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, Xian-Ming Zhang, A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems, *Neurocomputing* (2017), doi: 10.1016/j.neucom.2017.10.009

A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems

Derui Ding, Qing-Long Han*, Yang Xiang, Xiaohua Ge, and Xian-Ming Zhang

***Abstract*—Cyber-physical systems (CPSs), which are an integration of computation, networking, and physical processes, play an increasingly important role in critical infrastructure, government and everyday life. Due to physical constraints, embedded computers and networks may give rise to some additional security vulnerabilities, which results in losses of enormous economy benefits or disorder of social life. As a result, it is of significant to properly investigate the security issue of CPSs to ensure that such systems are operating in a safe manner. This paper, from a control theory perspective, presents an overview of recent advances on security control and attack detection of industrial CPSs. First, the typical system modeling on CPSs is summarized to cater for the requirement of the performance analysis. Then three typical types of cyber-attacks, i.e. denial-of-service attacks, replay attacks, and deception attacks, are disclosed from an engineering perspective. Moreover, robustness, security and resilience as well as stability are discussed to govern the capability of weakening various attacks. The development on attack detection for industrial CPSs is reviewed according to the categories on detection approaches. Furthermore, the security control and state estimation are discussed in detail. Finally, some challenge issues are raised for the future research.**

***Index Terms*—Industrial cyber-physical systems; cyber-attacks; attack detection; security control.**

I. Cyber-Physical Systems

Recent years have witnessed rapid developments of cyber-physical systems (CPSs) due to advances in computing, communication, and related hardware technologies. As a new research frontier, a CPS is an integration of physical processes, ubiquitous computation, efficient communication and effective control [12]. Its holistic framework is shown in Fig. 1. Various social and physical applications have been performed in light of CPSs. The application fields include, but are not limited to, transportation networks, smart grids, health care, and water/gas distribution networks [69]. Moreover, networked control systems, wireless sensor and actuator networks, and wireless industrial sensor networks can be referred to as a subgroup of CPSs in the published literature [32], [39], [46], [51], [52], [58], [83], [84], [86], [108], [119], [129]. For the recent developments, see survey papers [39], [58], [59] and the references therein. CPSs have been regarded as a core ingredient in the so-called 4th industrial revolution, and lots of efforts have been made for establishing its important position, such as, Industry 4.0 in Germany [62], and Industrial Internet in the U.S. [8]. It is worth mentioning that, performance analysis and synthesis have been intensively investigated for networked systems with various network-induced phenomena or communication protocols that include, but are not limited to, missing measurements [41], [42], [123], fading channels [24], communication delays [40], [44], [65], [85], [87], [95], sampled data [47], [104], [143], Round-Robin protocols [77], stochastic communication protocols [142], event-triggering protocols [25], [33], [54], [96], [97], [130], [135].

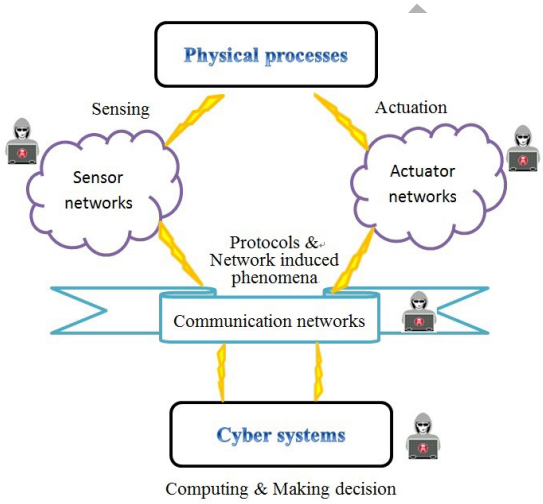


Fig. 1. A holistic framework of a CPS [36].

CPSs are large-scale, geographically dispersed, federated, heterogeneous, and life-critical systems in which embedded devices such as sensors and actuators are networked to sense, monitor and control the physical world. In a CPS operation, there is no doubt that the resource scheduling via various shared or own networks plays an important role. One of the essential tasks is to decide which actuators/sensors should be activated to perform a particular action or how to manage control/sampling actions properly. Due to physical constraints or technological limitations, data among sensors, actuators and other networked components may be transmitted over networks without proper security protections. On the one hand, the interconnection of large-scale networked components makes it complicated to protect against inherent physical

This work was supported in part by the Australian Research Council Discovery Project under Grant DP160103567, the National Natural Science Foundation of China under Grant 61573246, the Shanghai Rising-Star Program of China under Grant 16QA1403000, and the Program for Capability Construction of Shanghai Provincial Universities under Grant 15550502500.
(* *Corresponding author: Qing-Long Han.*)

D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang are with the School of Software and Electrical Engineering, Swinburne University of Technology, Melbourne, VIC 3122, Australia.