Resilient Control in Large-Scale Networked Cyber-Physical Systems: Guest Editorial

Giuseppe Franzè, Giancarlo Fortino, Xianghui Cao, Giuseppe Maria Luigi Sarnè, Zhen Song

RECENT advances in sensing, communication and computing have open the door to the deployment of large-scale networks of sensors and actuators that allow fine-grain monitoring and control of a multitude of physical processes and infrastructures. The appellation used by field experts for these paradigms is Cyber-Physical Systems (CPS) because the dynamics among computers, networking media/resources and physical systems interact in a way that multi-disciplinary technologies (embedded systems, computers, communications and controls) are required to accomplish prescribed missions. Moreover, they are expected to play a significant role in the design and development of future engineering applications such as smart grids, transportation systems, nuclear plants and smart factories.

This special issue deals with the opportunities offered by these emerging technologies to mitigate undesired phenomena arising when intentional jamming and false data injections, categorized as cyber-attacks, infer communication channels. As it is well-known, the main consequence is that measurement and actuator data integrity and availability might be compromised with a significant degradation of the control performance [1]−[4].

The goal of this special issue is to provide new ideas and solutions when cyber-attack countermeasures or resilient control strategies are concerned. Along these lines, secure/robust and resilient control frameworks for networked control system (NCS) configurations capable to jointly take care of state/input constraints under cyber-attack occurrences on the communication medium are of noticeable interest. Accordingly, trust management, cyber-attacks in smart grids, internet of things systems of systems and applications in emerging domains (e.g. Internet of Vehicles, Smart Cities) assume a relevant importance in the new Industry 4.0 era [5]−[7].

The special issue has been conceived as follow-up of the IEEE International Conference on Control Decision and Information Technologies 2019, Paris (Fra), April 2019, and to address some of the aforementioned issues. The seven articles in this special issue combine extended and revised papers accurately selected as best papers among those presented at CodiT 2019 with new contributions. The selected papers address many research challenges in the field of the resilient control for networked cyber-physical systems. Specifically, the main topics include: set-theoretic approaches for constrained regulation problems in networked multi-agent systems subject to denial-of-service (DoS) attacks, secure synchronization control problems for a class of CPSs subject to intermittent DoSs, collaborative estimation processes in sensor networks, formation-containment control based on a dynamic event-triggering mechanisms for multi-agent systems collaborative wireless autonomous systems network frameworks for disaster area management, trust oriented architectures for agents operating in IoT environments, fault diagnosis tool in smart industrial systems [8]−[9].

The paper "*A Resilient Control Strategy for Cyber-Physical systems Subject to Denial of Service Attacks: A Leader-Follower Set-Theoretic Approach*" [10] by Giuseppe Franzè, Domenico Famularo, Walter Lucia and Francesco Tedesco, presents a distributed model predictive control algorithm to formally address constrained regulation problems arising in networked multi-agent systems when external actors maliciously affect the normal operation mode. By exploiting ideas borrowed from the set-theoretic approach, sequences of one-step controllable sets have been adequately determined in order to take care of time-varying leader-follower configurations.

The paper "*Secure Synchronization Control for a Class of Cyber-Physical Systems with Unknown Dynamics*" [11] by Ning Wang and Xiaojian Li, authors investigate the secure synchronization control problem for CPSs subject to intermittent DoS attacks. The considered CPSs are modeled as a class of complex dynamical networks with unknown dynamics.

The paper "*Stochastic DoS Attack Allocation Against Collaborative Estimation in Sensor Networks*" [12] by Ya Zhang, Lishuang Du and Frank L. Lewis, proposes a stochastic scheduling and attack power allocation scheme from the perspective of the energy-constrained DoS attacker, so as to influence the estimation of the collaboratively working sensor network with minimum attack energy cost. Necessary condition and sufficient conditions on the packet loss probabilities of the channels in the attack set are also provided.

The paper "*Formation-Containment Control Using Dynamic Event-Triggering Mechanism for Multi-Agent Systems*" [13] by Amir Amini, Amir Asif and Arash Mohammadi, presents a novel approach for formation-containment control based on a dynamic event-triggering mechanism for multi-agent systems.

Citation: G. Franzè, G. Fortino, X. H. Cao, G. M. L. Sarnè, Z. Song, "Resilient control in large-scale networked cyber-physical systems: Guest editorial," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 5, pp. 1201−1203, Sept. 2020.

G. Franzè and G. Fortino are with University of Calabria, Italy (e-mail: giuseppe.franze@unical.it; g.fortino@unical.it)

X. H. Cao is with Southeast University, China (e-mail: xhcao@seu.edu.cn)

G. M. L. Sarnè is with University Mediterranea of Reggio Calabria, Italy (e-mail: sarne@unirc.it)

Z. Song is with First State IoT, China (e-mail: ZhenSong23931@gmail.com)

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2020.1003327

The leader-leader and follower-follower communications are reduced by utilizing the distributed dynamic event-triggered framework.

In the paper "*IoT-Enabled Autonomous System Collaboration for Disaster-Area Management*" [14] by Abenezer Girma, Niloofar Bahadori, Mrinmoy Sarkar, Tadewos G. Tadewos, Mohammad R. Behnia, M. Nabil Mahmoud, Ali Karimoddini, and Abdollah Homaifar, the authors develops a collaborative wireless autonomous systems network architecture for disaster area management. The framework enables synergy between heterogeneous autonomous system for assisting human agents to safely investigate post-disaster areas in a timely manner.

The paper entitled "*ResIoT: An IoT Social Framework Resilient to Malicious Activities*" [15] by Giancarlo Fortino, Fabrizio Messina, Domenico Rosaci and Giuseppe M. L. Sarnè, presents a new reputation based framework for IoT agents, called Resilient IoT (ResIoT), having the social capability to form agent local communities. ResIoT has been specifically designed to be resilient to a certain kind of malicious attacks. ResIoT has been conceived for all those IoT scenarios formed by federated environments in which heterogeneous devices, provided of limited computational, storage and power resources, are free to move between domains and where cooperation exploits the formation of social structures based on the widespread reputation in the network.

The paper entitled "*Resilient Fault Diagnosis Under Imperfect Observations – A Need for Industry 4.0 Era*" [16] by Alejandro White, Ali Karimoddini and Mohammad Karimadini, provides a diagnosis technique which is capable of diagnosing faults under imperfect observations. A new concept of asynchronous detectability is introduced, which, if holds, allows to detect a miss observation from its post observations.

We hope that the seven papers included in this special issue will provide valuable knowledge for those researchers and practitioners working in the area of robust and resilient control and related applications.

Finally, we would like to thank to Prof. Mengchu Zhou, Editor-in-Chief of the *IEEE/CAA Journal of Automatica Sinica* and Dr. Yan Ou, for their continuous support and encouragement for the development of this special section. We would like also to thank the anonymous reviewers who reviewed the seven papers by providing constructive feedback useful to improve the quality of the final papers.

REFERENCES

[1] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11 pp. 2715−2729, 2013.

[2] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51 pp. 135−148, 2015.

[3] W. Lucia, B. Sinopoli, and G. Franzè, "A set-theoretic approach for secure and resilient control of cyber-physical systems subject to false data injection attacks," in *Proc. Science of Security for Cyber-Physical Systems Workshop (SOSCYPS)*, pp. 1−5, Apr. 2016.

[4] G. Franzè, F. Tedesco, and W. Lucia, "Resilient control for cyber-physical systems subject to replay attacks," *IEEE Control Systems Letters*, vol. 3, no. 4 pp. 984−989, 2019.

[5] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10−28, 2017.

[6] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *Proc. IEEE World Congress on Services*, pp. 21−28, Jun. 2015.

[7] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," *IEEE Internet Things J*, vol. 5, no. 4, pp. 2483−2495, 2018.

[8] C. Savaglio, M. Ganzha, M. Paprzycki, C. Badica, M. Ivanovic, G. Fortino, "Agent-based internet of things: state-of-the-art and research challenges," *Future Gener. ComputSyst*, DOI: 10.1016/j.future.2019.09.016.

[9] S. F. Ochoa, G. Fortino, and G. Di Fatta, "Cyber-physical systems, internet of things and big data," *Future Gener. Comput. Syst.*, vol.75, pp.82−84 2017.

[10] G. Franzè, D. Famularo, W. Lucia, and F. Tedesco, "A resilient control strategy for cyber-physical systems subject to denial of service attacks: A leader-follower set-theoretic approach," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 5, pp. 1204−1214, Sept. 2020.

[11] X. J. Li, "Secure synchronization control for a class of cyber-physical systems with unknown dynamics," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 5, pp. 1215−1224, Sept. 2020.

[12] Y. Zhang, L. Du, and F. L. Lewis, "Stochastic DoS attack allocation against collaborative estimation in sensor networks," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 5, pp. 1225−1234, Sept. 2020.

[13] A. Amini, A. Asif, and A. Mohammadi, "Formation-containment control using dynamic event-triggering mechanism for multi-agent systems," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 5, pp. 1235−1248, Sept. 2020.

[14] A. Girma, N.Bahadori, M. Sarkar, T. G. Tadewos, M. R. Behnia, M. N. Mahmoud, A.Karimoddini, and A. Homaifar, "IoT-enabled autonomous system collaboration for disaster-area management," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 5, pp. 1249−1262, Sept. 2020.

[15] G. Fortino, F. Messina, D. Rosaci, and G. M.L.Sarnè, "ResIoT: An IoT social framework resilient to malicious activities," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 5, pp. 1263−1278, Sept. 2020.

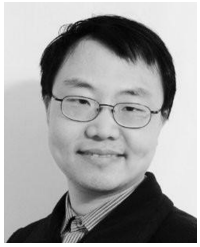
[16] A. White, A. Karimoddini, and M. Karimadini, "Resilient fault diagnosis under imperfect observations – a need for industry 4.0 era," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 5, pp. 1279−1288, Sept. 2020.

Giuseppe Franzè (SM' 19), received the Laurea degree in computer engineering in 1994 and the Ph.D. degree in systems engineering in 1999 from the University of Calabria, Italy. Since 2015 he is an Associate Professor at the University of Calabria with the DIMES Department. He authored or co-authored more than 160 research papers in archival journals, book chapters and international conference proceedings. His current research interests include constrained predictive control, nonlinear systems, networked control systems, control under constraints and control reconfiguration for fault tolerant systems, resilient control for cyber-physical systems. In November-December 2019, he was a visiting professor at Concordia University (CA) with the ECCE Department. He is a co-recipient of the Best Paper Award at the IEEE-CoDIT 2019 Conference, Paris, France. He currently serves as a Associate Editor of the *IEEE/CAA Journal of Automatica Sinica*. He is the Guest Editor of the Special Issue "Resilient Control in Large-Scale Networked Cyber-Physical Systems" *IEEE/CAA Journal of Automatica Sinica*. Since January 2018, he is Graduate Program Director of the Master Degree in Automation Engineering at the DIMES Department, University of Calabria.

Giancarlo Fortino (SM'12) is Full Professor of Computer Engineering at the Dept of Informatics, Modeling, Electronics, and Systems of the University of Calabria (Unical), Italy. He received a Ph.D. in Computer Engineering from Unical in 2000. He is also distinguished professor at Wuhan University of Technology and Huazhong Agricultural University (China), high-end expert at HUST (China), senior research fellow at the ICAR-CNR Institute, and CAS PIFI visiting scientist at SIAT -Shenzhen. He is the director of the SPEME lab at Unical as well as co-chair of Joint labs on IoT established between Unical and WUT and SMU and HZAU Chinese universities, respectively. His research interests include agent-based computing, wireless (body) sensor networks, and IoT. He is author of 450+ papers in int'l journals, conferences and books. He is (founding) series editor of IEEE Press Book Series on Human-Machine Systems and EiC of Springer Internet of Things series and AE of many int'l journals such as *IEEE TAC, IEEE THMS, IEEE IoTJ, IEEE SJ, IEEE SMCM, IEEE OJEMB, IEEE OJCS, Information Fusion, JNCA, EAAI*, etc. He organized as chair many int'l workshops and conferences (100+), was involved in a huge number of int'l conferences/workshops (500+) as IPC member, is/was guest-editor of many special issues (60+). He is cofounder and CEO of SenSysCalS.r.l., a Unical spinoff focused on innovative IoT systems. Fortino is currently member of the IEEE SMCS BoG and of the IEEE Press BoG, and chair of the IEEE SMCS Italian Chapter.

Xianghui Cao (S'08–M'11–SM'16) received the B.S. and Ph.D. degrees in control science and engineering from Zhejiang University, Hangzhou, China, in 2006 and 2011, respectively. From 2012 to 2015, he was a Senior Research Associate with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL, USA. He is currently a Professor with the School of Automation, Southeast University, Nanjing, China. His current research interests include cyber-physical systems, industrial Internet of Things, wireless networked control, and network security. He served as the Technical Program Co-Chair for The Youth Academic Annual Conference of Chinese Association of Automation in 2019, the Symposium Co-Chair for ICNC 2017 and IEEE/CIC ICCC 2015, and an International Program Committee member for IFAC CPHS 2020. He also serves as an Associate Editor for *Acta Automatica Sinica, IEEE/CAA Journal of Automatica Sinica*. He was a recipient of the First Prize of Natural Science Award of Ministry of Education of China in 2017 and the Best Paper Runner-Up Award from ACM MobiHoc in 2014.

Giuseppe M. L. Sarnè is Assistant Professor of Computer Science at the Department of Civil, Energy, Environment and Materials Engineering at the University Mediterranea of Reggio Calabria (UNIRC), Italy. He is director of the Network and Complex Systems (NeCS) Laboratory at UNIRC and member of IEEE. His main research interests include distributed artificial intelligence, agent-based computing, recommender systems, trust and reputation systems and IoT systems. He is Associate Editor of *E-Commerce Research and Applications* (Elsevier) and *Big Data and Cognitive Computing* (MDPI) journals and guest editor of special issues.



Zhen Song (S'02–M'07–SM'17) received the B.S. degree in automation from Beijing Inst. Tech., Beijing, China, in 1997. He received the M.S. and Ph.D. degrees from Utah State University, UT, USA, in 2003 and 2007 respectively. Currently, he is the CTO of First State IoT, China. He was a senior data scientist at Siemens Smart Infrastructure from 2018 to 2019. From 2006 to 2018, he worked for Siemens Corporate Technology, Princeton, NJ, USA, where he has been the principal investigator of government research projects sponsored by DOD, DOE, NRL, ONR, ARL and New York State. His research interests include IIoT, prognostic, machine learning, optimal control, sensor networks. He has more than 30 patents and 50 publications, including a monograph published by Springer. He was a session co-chair of IEEE ACC and IEEE CASE conferences in 2007 and 2017, and a plenary speaker in IEEE PES conference 2018. He serves as an associated editor of *IEEE JAS*. He won the 2nd place 2005 Smart Dust competition in UC Berkeley and the 3rd place best paper award of IEEE Sarnoff Symposium in Princeton University 2007.