

Proposal for an ICSPAC 2021 Invited Session on “Control and Security in Networked Control Systems”

Proposers: Jinliang Shao, Heng Zhang

Abstract—Networked control systems (NCSs) has drawn a great deal of attention from our control community due to its potential benefits to the engineering, economy and society. It is widely recognised that networks and control is a very challenging and promising research field. Nevertheless, the area of theoretical research on NCSs is still in its start stage, and it is important and fundamental both in practice and in theory to focus on the enhancement of control robustness against network constraints, and the improvement of network reliability and security. In order to support the development of study on the control and security of NCSs, we propose an invited sessions in ICSPAC 2021 that will present recent advances in the area of NCSs. In particular, this session contains novel works on the distributed collaborative control of networked multi-agent system, state estimation and control, and cyber security.

I. MOTIVATION AND RELEVANCE

In recent years, a major trend in modern industrial and commercial systems is to integrate the modern communication, computation, and control technologies into different levels of machine/factory operations and information processes, for dramatically improving the efficiency, stability, reliability, safety, and other performances in real operating systems [1], [2]. As a new generation of engineering systems, networked control systems is an umbrella term encompassing a broad variety of infrastructures, and networked control has ever-increasing applications in a wide range of areas, such as smart grids, manufacturing systems, process control, automobiles, automated highway systems, and unmanned aerial vehicles [3]. The basis capabilities of any NCSs are information acquisition (sensors/users), command (controllers/users), communication, and network and control (actuators) [4]. In broader terms, two of the key research directions for NCSs are “control of networks” and “control over networks” [5]. From the point of control systems, “Control over networks” aims to design suitable control strategies to reduce the effects of network imperfections on desired control performance, which includes sampled-data control [6], [7], quantization control [8], [9], event-triggered control [10], [11], networked control [12], [13] and security control [14], [15], and so on.

In particular, as summarized in [16], network induced vulnerabilities arise in NCS due to four factors. First, due to wider deployment of off-the-shelf IT devices, NCS inherit the vulnerabilities of these devices, and thus are subject to correlated software and hardware failures. Second, the proprietary network protocols, which are traditional for control systems, are being upgraded to open design protocols, making it easier

for attackers to learn about NCS operations. Third, sensor-control data is being made accessible to authorized remote users via corporate networks and Internet. This makes NCS subject to insider attacks. Fourth, the existence of organized cybercrime groups enhances attacker capabilities to conduct intrusions into NCS.

Due to the increasing number of cyber attacks and their serious consequences, *secure estimation and control* has become another hot topic in NCSs. A multi-channel transmission schedule for remote state estimation has been proposed when the communication networks are under DoS attacks and the sensors have limited energy budgets [17]. A satisfiability modulo theory approach has been introduced to securely estimate the state of a dynamical system when there only exist limited secure sensors in NCSs [18]. For the given system constraints, a set-theoretic approach for secure and resilient control of Cyber-Physical Systems has been presented to defend the false data injection attacks [19]. This secure approach also has been validated in an Unmanned Ground Vehicle system. Although the advantages are well motivated and practical applications show its potential [20], [21], [22], [23], [17], [18], [19], many questions remain unanswered to date even though progress was made in recent years and the people is receiving an increasing amount of attention in our community. See, e.g., [24], [25] for a recent overview.

To sum up, networked control systems has become increasingly prevalent for the last two decades due to wide applications in many industrial areas, where the control and security problems in NCSs are important and fundamental both in practice and in theory, and have aroused great concern up to now. Therefore, we would like to organize an invited session in ICSPAC 2021 to shed light on the recent advances in the area of “Control and Security in Networked Control Systems”.

II. SUMMARY OF THE SESSION AND ITS COHESIVE STRUCTURE

The common denominator of all the contributions in this invited session are novel works on Control and Security in NCSs. In particular, this sessions contains topics on the crossroads of distributed collaborative control of networked multi-agent system, state estimation, cyber security for NCSs. This provides a cohesive structure between the high-quality contributions in this session.

Given the current interest in this challenging research domain we anticipate that many researchers at the Conference will attend this invited session. Based on our own experiences with similar invited sessions on NCSs and Cyber-Physical Systems that were organized at

Jinliang Shao is with the School of Automation Engineering, University of Electronic Science and Technology of China, Sichuan, 611731, China (e-mail: jinliangshao@uestc.edu.cn).

H. Zhang is with School of Science, Jiangsu Ocean University, Lianyungang, Jiangsu, 222005, P. R. China (email: Dr.Zhang.Heng@ieec.org).

- IEEE Conference on Decision and Control (CDC) 2016 in Las Vegas, NV, USA
- Chinese Control Conference (CCC) 2016 in Chengdu, China
- IFAC World Congress 2017 in Toulouse, France
- IEEE Conference on Decision and Control (CDC) 2018 in Miami Beach, FL, USA.
- American Control Conference 2019 in Philadelphia, PA, USA
- IFAC World Congress 2020 in Berlin, Germany
- International Symposium on Circuits and Systems 2020 Virtual, 8 October 2020.

we estimate that the session will attract around forty to sixty researchers, and hope the application for the invited session can be approved.

REFERENCES

- [1] T. C. Yang, "Networked control system: a brief survey," *Control Theory and Applications, IEE Proceedings* -, vol. 153, no. 4, pp. 403–412, 2006.
- [2] K.-D. Kim and P. R. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proceedings of the IEEE*, vol. 100 Special Centennial Issue, pp. 1287–1308, 2012.
- [3] X. M. Zhang, Q. L. Han, X. Ge, D. Ding, and C. Peng, "Networked control systems: a survey of trends and techniques," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 1, pp. 1–17, 2020.
- [4] R. A. Gupta and M. Y. Chow, "Networked control system: Overview and research trends," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 7, pp. 2527–2535, 2010.
- [5] M. Murray, Richard, "Control in an information rich world :report of the panel on future directions in control, dynamics, and systems," in *Philadelphia, PA: SIAM*, 2003.
- [6] L. S. Hu, T. Bai, P. Shi, and Z. Wu, "Sampled-data control of networked linear control systems," *Automatica*, vol. 43, no. 5, pp. 903–911, 2007.
- [7] Y. Wang, H. Shen, and D. Duan, "On stabilization of quantized sampled-data neural-network-based control systems," *IEEE Transactions on Cybernetics*, vol. 47, no. 10, pp. 3124–3135, 2017.
- [8] G. Gu and L. Qiu, "Networked control systems for multi-input plants based on polar logarithmic quantization," *Systems & Control Letters*, vol. 69, no. 1, pp. 16–22, 2014.
- [9] X. Liu, J. Zhang, and Y. Xia, "Co-design of quantization and event-driven control for networked control systems," *IEEE Transactions on Systems Man & Cybernetics Systems*, 2019, doi: 10.1109/TSM-C.2019.2918006.
- [10] V. Lchapp, E. Moulay, F. Plestan, and Q.-L. Han, "Discrete predictor-based event-triggered control of networked control systems," *Automatica*, vol. 70, pp. 101–108, 2016.
- [11] A. D. McKernan and G. W. Irwin, "Event-based sampling for wireless network control systems with qos," in *Proceedings of American Control Conference*, 2010, pp. 1841–1846.
- [12] J. Chen, S. Meng, and J. Sun, "Stability analysis of networked control systems with aperiodic sampling and time-varying delay," *IEEE Transactions on Cybernetics*, pp. 1–9, 2016.
- [13] B. Xue, S. Li, and Q. Zhu, "Moving horizon state estimation for networked control systems with multiple packet dropouts," *IEEE Transactions on Automatic Control*, vol. 57, no. 9, pp. 2360–2366, 2012.
- [14] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in *IEEE Conference on Decision and Control*, 2015.
- [15] H. Yang, M. Shi, Y. Xia, and P. Zhang, "Security research on wireless networked control systems subject to jamming attacks," *IEEE Transactions on Cybernetics*, vol. 49, no. 6, pp. 2022–2031, 2019.
- [16] S. Amin, G. A. Schwartz, and S. S. Sastry, "On the interdependence of reliability and security in networked control systems," in *2011 50th IEEE Conference on Decision and Control and European Control Conference*, 2012.
- [17] K. Ding, Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "A multi-channel transmission schedule for remote state estimation under DoS attacks," *Automatica*, vol. 78, pp. 194–201, 2017.
- [18] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, "Secure state estimation for cyber physical systems under sensor attacks: a satisfiability modulo theory approach," *IEEE Transactions on Automatic Control*, 2017.
- [19] W. Lucia, B. Sinopoli, and G. Franze, "A set-theoretic approach for secure and resilient control of cyber-physical systems subject to false data injection attacks," in *Proceedings of Science of Security for Cyber-Physical Systems Workshop (SOSCYPSS)*, 2016, pp. 1–5.
- [20] X. Cao, P. Cheng, J. Chen, and Y. Sun, "An online optimization approach for control and communication codesign in networked cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 439–450, 2013.
- [21] J. Chakravorty and A. Mahajan, "Fundamental limits of remote estimation of autoregressive Markov processes under communication constraints," *IEEE Transactions on Automatic Control*, 2016.
- [22] S. Knorn and S. Dey, "Optimal energy allocation for linear control with packet loss under energy harvesting constraints," *Automatica*, vol. 77, pp. 259–267, 2017.
- [23] L. Wang, G. Guo, W. Yue, and Y. Zhuang, "Scheduling-and-control codesign for NCSs with bandwidth and transmission energy constraints," in *Proceedings of Chinese Control and Decision Conference (CCDC)*, 2016, pp. 308–313.
- [24] I. Akkaya, P. Derler, S. Emoto, and E. A. Lee, "Systems engineering for industrial cyber-physical systems using aspects," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 997–1012, 2016.
- [25] D. Wang, Z. Wang, B. Shen, F. E. Alsaadi, and T. Hayat, "Recent advances on filtering and control for cyber-physical systems under security and resource constraints," *Journal of the Franklin Institute*, vol. 353, no. 11, pp. 2451–2466, 2016.