Editorial: Secure and Safe MetaControl for Cyber Physical Systems

Qing-Long Han, *Fellow, IEEE*

Welcome to the twelfth issue of 2023 in the IEEE/CAA Journal of Automatica Sinica (JAS). In the sixth issue of 2023, I systematically addressed the latest development of MetaVehicles, and sorted out some important contributions published in the IEEE/CAA JAS focusing on control, estimation, and optimization of automated vehicles with reliability, security, efficiency, and intelligence. When shifting the perspective to cyber-physical systems (CPSs), the styles or paradigms of control and filtering are going through major changes benefiting from the widespread applications of both cloud computing and digital twins. Particularly, the desired performance and management functions of CPSs under the virtual and real framework will be achieved via Metaverse technologies and strict system analysis involving behavior recognition of users, decision-making processes as well as parameter design and optimization. It is evident that the system's performance and cost are synthetic reflections of its behavior in both cyberspace and the real world [1]. This kind of control paradigm can be referred to as MetaControl [2]. It should be pointed out that MetaControl is built upon cyberspace and hence security threats are naturally inherited and inevitably enhanced due to the ever-increasing complexity and diversity of system functionalities while faults in the physical space are also a big concern. As such, new methods of control, filtering, and optimization should be creatively developed to satisfy the requirement of external security in cyberspace and internal safety in the physical space of CPSs.

At IEEE/CAA JAS, we value and demonstrate the latest advancement in secure and safe MetaControl for cyber-physical systems. In this editorial, I collected eighteen articles published in IEEE/CAA JAS in the recent three years, relevant to this interesting topic. Specifically, I classify them into the following three groups.

1) Passively secure control and filtering

It should be pointed out that malicious attacks that occur in CPSs could appear differences in the form, strength, and stealthiness due to the tight integration of virtual cyberspace and real physical space in comparison with traditional control systems. Therefore, it is essential to provide innovative design concepts to generate control commands or reconstruct system states based on only measured, but potentially corrupted information. To tolerate unpredictable anomalies caused by cyberattacks, one of the mainstream lines is to design an admissible control or filtering policy. In contrast to traditional schemes, the basic idea is to choose suitable parameters to meet the more conservative security requirements.

A survey of state-of-the-art results of cyber attacks on CPSs is presented to discuss various defense strategies for availability, integrity, and confidentiality attacks [3]. From the perspective of energy conversion, an effective defense framework is provided in [4], where the passivity-based robust controller has the capability of dynamically adjusting the system energy changes caused by unknown attacks. A sufficient condition is obtained to disclose the impact on security from the maximum duration of continuous replay attacks and the ratio between duration lengths of active and silent attacks [5]. Such a condition provides a conservative boundary of attack tolerance while guaranteeing the desired platooning performance. By using a similar idea, some interesting results about denial-of-service (DoS) attacks are derived for load frequency control of power systems [6] and for consensus control of nonlinear multi-agent systems [7]. The resilient longitudinal platooning control under intermittent DoS attacks is investigated to guarantee anticipated attack resilience while satisfying the desired platoon stability [8].

2) Actively secure control and filtering

Different from the passive strategy, another alternative strategy is to design a preferable attack-compensated scheme via attack detection and identification or an information protection rule via encryption, watermark, or blockchain techniques to prevent the severe deterioration of the system's performance [9]. As such, the development of advanced attack detection mechanisms, especially from the viewpoint of MetaControl, is indispensable to precisely and sensitively identify and locate the occurrence of cyberattacks. Furthermore, some novel analysis methods should be established to disclose the impact on system performance from various protection techniques while maintaining data privacy. Deep learning delivers superior performance to increase the capability of attack detection in MetaControl benefiting from its superiority in extracting useful information from training data. A review is provided to systematically summarize the methodologies of deep learning-based attack detection in the CPS context [10].

The mechanism against eavesdropping is to exploit the encryption-based communication mechanism, which will result in nontrivial challenges in secure control and filtering. Some results are reported in IEEE/CAA JAS. A zonotopic watermark signal, making the residual vector exit the healthy residual set, is designed to detect replay attacks [11]. A

Citation: Q.-L. Han, "Editorial: Secure and safe MetaControl for cyber physical systems," IEEE/CAA J. Autom. Sinica, vol. 10, no. 12, pp. 2177-2178, Dec. 2023.

Q.-L. Han is with the School of Science, Computing and Engineering Technologies, Swinburne University of Technology, Melbourne, VIC 3122, Australia (e-mail: qhan@swin.edu.au).

Digital Object Identifier DOI: 10.1109/JAS.2023.124014

computationally efficient scheme of attribute-based searchable encryption is developed by resorting to blockchain technology [12]. Furthermore, an encryption-decryption scheme is proposed to avoid the eavesdropping of transmitted signals via adding artificial noises into raw measurements [13]. Based on such a signal, a finite-horizon energy-to-peak state estimator is designed to satisfy the predetermined l_2-l_∞ performance.

3) Safe control and filtering

Besides the system stability, safety is one of the most important indicators of CPSs due to the inherent need the equipment protection or the reliability requirement of engineering systems suffering from sensor and/or actuator faults. It is a natural way to use fault detection and compensation to prevent performance degradation and enhance the reliability of CPSs [14]. Furthermore, advanced diagnostic techniques are urgently required for the complex physical and cyber nature of CPSs. Besides, human judgment and decision can be integrated into the control loop to further improve the monitoring and control capability in the era of MetaControl, such as the generation of reference trajectories and multimode switching for some complex tasks. Human-in-the-loop leader-following consensus control is investigated for multi-agent systems (MASs) with unknown matched nonlinear dynamics and actuator faults [15], where the leader's control command generated by a human operator is not available to all followers. Fault estimators with the aid of neural networks are employed to identify the actuator faults. A control scheme based on fault-estimation-in-the-loop is developed to realize the bounded consensus with an l_2-l_∞ constraint [16]. A comprehensive survey is presented in [17] to summarize the recent advances in model-based fault detection, diagnosis, and fault-tolerant control of MASs with homogeneous and homogeneous dynamics, where various observer structures, involving unknown input observers, sliding mode observers, joint state and fault estimators as well as fault estimators based on intermediate variables, were provided and their advantages were profoundly discussed.

When collision avoidance is a concern, an elaborate control signal should be designed to generate a conflict-free trajectory [18]. To this end, a control barrier function is a promising tool for synthesizing such a constrained control law. The dynamic system operational safety is investigated under relaxed safety judgment criteria by means of constructed barrier functions [19]. Furthermore, deep learning techniques can be applied to efficiently mine the feature information to model the complex behavior of CPSs. A sensorless deep-learning-based algorithm is proposed to estimate brake pressure to design safety-critical autonomous systems [20].

I hope you would enjoy this Editorial on the latest results about secure and safe MetaControl for cyber-physical systems. Many thanks for your attention, support, and contribution to IEEE/CAA JAS.

REFERENCES

[1] H. Geng, Z. Wang, Y. Chen, X. Yi, and Y. Cheng, "Variance-constrained filtering fusion for nonlinear cyber-physical systems with the denial-of-service attacks and stochastic communication protocol," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 6, pp. 978–989, Jun. 2022.

[2] F.-Y. Wang, "The DAO to MetaControl for MetaSystems in Metaverses: The system of parallel control systems for knowledge automation and control intelligence in CPSS," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 11, pp. 1899–1908, Nov. 2022.

[3] W. Duo, M. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 5, pp. 784–800, May 2022.

[4] Y. Zhao, Z. Chen, C. Zhou, Y.-C. Tian, and Y. Qin, "Passivity-based robust control against quantified false data injection attacks in cyber-physical systems," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 8, pp. 1440–1450, Aug. 2021.

[5] M. Xie, D. Ding, X. Ge, Q.-L. Han, and H. Dong, "Distributed platooning control of automated vehicles subject to replay attacks based on proportional integral observers," *IEEE/CAA J. Autom. Sinica*, DOI: 10.1109/JAS.2022.105941.

[6] X. Zhao, S. Zou, and Z. Ma, "Decentralized resilient H_∞ load frequency control for cyber-physical power systems under DoS attacks," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 11, pp. 1737–1751, Nov. 2021.

[7] X. Guo, D. Zhang, J. Wang, and C. Ahn, "Adaptive memory event-triggered observer-based control for nonlinear multi-agent systems under DoS attacks," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 10, pp. 1644–1656, Oct. 2021.

[8] X. Ge, Q.-L. Han, Q. Wu, and X.-M. Zhang, "Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 5, pp. 1234–1251, May 2023.

[9] K. Zhang, C. Keliris, T. Parisini, B. Jiang, and M. M. Polycarpou, "Passive attack detection for a class of stealthy intermittent integrity attacks," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 4, pp. 898–915, Apr. 2023.

[10] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 3, pp. 377–391, Mar. 2022.

[11] C. Trapiello, and V. Puig, "A zonotopic-based watermarking design to detect replay attacks," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 11, pp. 1924–1938, Nov. 2022.

[12] Mamta, B. B. Gupta, K.-C. Li, V. C. M. Leung, K. E. Psannis, and S. Yamaguchi, "Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 12, pp. 1877–1890, Dec. 2021.

[13] L. Zou, Z. Wang, B. Shen, H. Dong, and G. Lu, "Encrypted finite-horizon energy-to-peak state estimation for time-varying systems under eavesdropping attacks: Tackling secrecy capacity," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 4, pp. 985–996, Apr. 2023.

[14] C. Liu, B. Jiang, X. Wang, H. Yang, and S. Xie, "Distributed fault-tolerant consensus tracking of multi-agent systems under cyber-attacks," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 6, pp. 1037–1048, Jun. 2022.

[15] G. Lin, H. Li, H. Ma, D. Yao, and R. Lu, "Human-in-the-Loop consensus control for nonlinear multi-agent systems with actuator faults," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 1, pp. 111–122, Feb. 2022.

[16] Y. Ju, D. Ding, X. He, Q.-L. Han and G. Wei, "Consensus control of multi-agent systems using fault-estimation-in-the-loop: dynamic event-triggered case," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 8, pp. 1440–1451, Aug. 2022.

[17] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 2, pp. 319–333, Feb. 2021.

[18] X. Ge, Q.-L. Han, J. Wang, and X.-M. Zhang, "A scalable adaptive approach to multi-vehicle formation control with obstacle avoidance," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 6, pp. 990–1004, Jun. 2022.

[19] Z. Zhu, Y. Chai, Z. Yang, and C. Huang, "Exponential-alpha safety criteria of a class of dynamic systems with barrier functions," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 11, pp. 1939–1951, Nov. 2022.

[20] M. Al-Sharman, D. Murdoch, D. Cao, C. Lv, Y. Zweiri, D. Rayside, and W. Melek, "A sensorless state estimation for a safety-oriented cyber-physical system in urban driving: Deep learning approach," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 1, pp. 169–178, Jan. 2021.