DOI: 10.1049/cps2.12029

The Institution of Engineering and Technology WILEY

GUEST EDITORIAL

Guest editorial: Machine learning for secure cyber-physical industrial control systems

1 | INTRODUCTION

Information and communication technologies have increasingly been used to support the exchange of measurements and control signals in industrial control systems, making them important applications of cyber-physical industrial control systems (CPICSs) such as electrical power systems and intelligent transportation systems. While the communication infrastructure significantly facilitates the transmission of vast amounts of data over wide geographical areas, it makes CPICSs vulnerable to cyber-attacks; protecting CPICSs of critical infrastructures from cyber-attacks is crucial and challenging. In order to secure CPICSs, a variety of open challenges need to be tackled, including cyber-physical system modelling approaches, advanced intrusion detection systems, and resilient estimation and control methods. Machine learning (ML) and its emerging algorithms offer the potential of dealing with large-scale data analysis, data processing and decision-making in the security of CPICSs.

This special issue publishes state-of-the-art ML-based solutions for the open challenges in securing CPICSs of critical infrastructures.

2 | GAME THEORETIC VULNERABILITY MANAGEMENT FOR CYBER-PHYSICAL MICROGRID

When modelling cyber-attacks in CPICSs, most of existing works consider using external disturbances, which follow certain assumptions. While it is not sufficient to model cyber-attacks simply as disturbances, the paper 'Game theoretic vulnerability management for secondary frequency control of islanded microgrids against false data injection (FDI) attacks' by S. Liu et al. considers the dynamic interaction between the smart attacker (the spoofer) and the defender the microgrid control centre (MGCC). The authors propose a stochastic game between the MGCC and the attacker for enhancing the vulnerability of the MGCC to FDI attack (wireless spoof attack).

3 | RESILIENT CONTROL FOR BILATERAL TELEOPERATION SYSTEMS

As communication networks are implemented for information exchange between the master and slave sides of bilateral teleoperation systems, they are also exposed to cyber-attack threats. The paper 'Mode-dependent switching control of bilateral teleoperation against random denial-of-service attacks' by L. Hu et al. analyses the performance of bilateral teleoperation systems in the presence of random denial-of-service (DoS) attacks and constant transmission delays and proposes a mode-dependent switching controller to mitigate the influence of DoS attacks.

4 | DATA IMBALANCE IN MACHINE LEARNING-BASED CYBER-ATTACK DETECTION

While machine-learning algorithms are helpful in identifying cyber-attacks such as network intrusion, common network intrusion datasets are negatively affected by class imbalance; the normal traffic behaviour constitutes most of the dataset, whereas intrusion traffic behaviour forms a significantly smaller portion. The paper 'Network intrusion detection using ML approaches: Addressing data imbalance' by R. Ahsan et al. conducts a comparative evaluation on the impact of data imbalance of various ML algorithms and presents a hybrid voting classifier to improve the results.

5 | GENERATIVE ADVERSARIAL NETWORK (CGAN)-BASED ANOMALY DETECTION

To improve the anomaly detection performance when imbalanced datasets are used, the paper 'A comparative analysis of CGAN-based oversampling for anomaly detection' by R. Ahsan et al. proposes a CGAN-based anomaly detection solution by taking both data-level and algorithm-level structures into considerations.

6 | CONCLUSION

The papers selected for this Special Issue cover a diversity of ML-based solutions for securing CPICSs, such as cyber-physical energy systems and tele-robotic systems. Furthermore, novel solutions for the data imbalance challenge in cyber-layer intrusion detection systems are highlighted in this issue. In future, ML and reinforcement learning algorithms may attract significant interests in tackling challenges in large-scale data analysis, data processing and decision-making involved in the security of CPICSs.

Shichao Liu[1]
Ligang Wu[2]
Jose Ignacio Leon[3]
Bo Chen[4]

[1]*Department of Electronics, Carleton University, Ottawa, Ontario, Canada*
[2]*Harbin Institute of Technology, China*
[3]*Universidad de Sevilla, Spain*
[4]*Zhejiang University of Technology, China*

Correspondence
Shichao Liu, Department of Electronics, Carleton University, 1125 Colonel By Dr, Ottawa K1S 5B6, Ontario, Canada.
Email: shichaoliu@cunet.carleton.ca

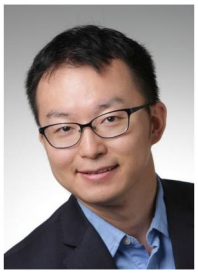
DATA AVAILABILITY STATEMENT

Not applicable.

ORCID

Shichao Liu https://orcid.org/0000-0002-3163-161X

AUTHOR BIOGRAPHIES



Shichao Liu received his Ph.D. degree from Carleton University, Canada, in 2014 and is currently an assistant professor in the Department of Electronics. Dr Liu is a senior member of IEEE, he is also an associate editor for *IEEE Access* and an editorial board member of *Smart Cities*. His research interests include modelling, stability analysis, intrusion detection, resilient control and game theoretic decision making of cyber-physical energy systems and the applications in microgrids and smart grids under attacks.

Dr. Wu received his Ph.D. degree in control theory and control engineering from Harbin Institute of Technology, China, in 2006. In 2008, he joined Harbin Institute of Technology as an associate professor, where he was promoted to professor in 2012. Dr. Wu received the Highly Cited Researcher Award by Thomson Reuters in 2015-2020. Dr. Wu currently serves as an associate editor for a number of journals, including the *IEEE Transaction on Automatic Control*, *IEEE Transactions on Industrial Electronics*, *IEEE/ASME Transactions on Mechatronics* and *IET Control Theory and Applications*. His research interests include switched hybrid systems, computational and intelligent systems, sliding-mode control, optimal filtering, and flight control. In 2020, he has been elevated to the IEEE Fellow grade with the following citation 'for contributions to slide mode control'.

Jose I. Leon received his PhD degree in telecommunications engineering from Universidad de Sevilla, Spain, in 2006. Currently, he is an associate professor with the Department of Electronic Engineering, Universidad de Sevilla. His research interests include modulation and control of power converters for high-power applications and renewable energy systems. He is currently serving as an associate editor of *IEEE Transactions on Industrial Electronics*. Dr. Leon was a co-recipient of the 2008 Best Paper Award in IEEE Industrial Electronics Magazine, the 2012 Best Paper Award of *IEEE Transactions on Industrial Electronics*, and the 2015 Best Paper Award of IEEE Industrial Electronics Magazine. He was the recipient of the 2014 IEEE J. David Irwin Industrial Electronics Society Early Career Award, the 2017 IEEE Bimal K. Bose Energy Systems Award and the 2017 Manuel Losada Villasante Award for excellence in research and innovation. In 2017, he has been elevated to the IEEE Fellow grade with the following citation 'for contributions to high-power electronic converters'.

Dr. Chen received his Ph.D degree in control theory and control engineering from Zhejiang University of Technology, China, in 2014. He is currently a full professor with the Institute of Cyberspace Security, Zhejiang University of Technology, China. He was a research fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from 2014 to

2015 and from 2017 to 2018. He was also a post-doctoral research fellow with the Department of Mathematics, City University of Hong Kong, China, from 2015 to 2017. He was a recipient of the outstanding thesis award of the Chinese Association of Automation (CAA) in 2015. His current research interests include information fusion, cyber-physical systems security and networked fusion systems.