Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.

Resilience enhancement of cyber-physical systems against hybrid attacks

Zhaoyuan Yin[1], Chao Fang[2], Yiping Fang[3], Min Xie[1]

[1]Department of Advanced Design and System Engineering, City University of Hong Kong, Hong Kong SAR, China.
E-mail: zyyin2-c@my.cityu.edu.hk, minxie@cityu.edu.hk
[2]Department of Management Science, Xi'an Jiaotong University, ShaanXi, China.
E-mail: fangchao@xjtu.edu.cn
[3]Industrial Engineering Laboratory, CentraleSupélec, Université Paris-Saclay, France
E-mail: yiping.fang@centralesupelec.fr

Contributions to 33rd European Safety and Reliability Conference, *Southampton, United Kingdom,3-8 September 2023* are to be in American English.

With the advancement of information and communication technology, modern critical infrastructure systems, e.g., power grids, tend to be controlled automatically and remotely through cyber systems. Such coupling of physical and cyber systems promotes more efficient operations and inversely induces the vulnerability of two aspects in the face of potential cyber-physical attacks. Specifically, high-impact low-probability extreme weather events can trigger disruption scenarios where many components in the physical system fail, while malicious attackers with limited offensive resources prefer information interference such as denial-of-service (DoS) attacks and false data injection (FDI) attacks to affect the availability and integrity of cyber systems. Considering the serious consequences of natural disasters and malicious cyber-attacks, it is necessary to develop a resilience enhancement framework from the cyber-physical perspective. In this paper, a defender-attacker-defender model is proposed for the resilient strategy of cyber-physical systems against hybrid uncertain threats. The first defend-level problem aims to protect the cyber-physical systems by optimally allocating protection equipment, e.g., distributed energy resources and intelligent firewalls. The attack-level problem formulates the best cyber-attack strategy, including the timing and intensity of the DoS and FDI attacks. Both the first defense and attack strategies should consider the stochastic disruption scenarios caused by natural hazards. And the second defend-level problem targets to optimal operation of the cyber-physical system based on the available components and resources at each disruption scenario. To solve the proposed tri-level stochastic optimization problem, we implement the duality theory to reformulate the tri-level problem into a max-min problem, and then exploit a column-and-constraints generation algorithm to obtain the solution. Detailed case studies are conducted in IEEE 13-node and 33-node systems to showcase the effectiveness of the proposed framework. The numerical results indicate that the designed defense strategy can bolster the cyber-physical system resilience against hybrid threats.

Keywords: Cyber-physical systems, interdependence, hybrid attacks, resilience enhancement, optimization.

References

1. Bellè, A., Abdin, A. F., Fang, Y. P., Zeng, Z., & Barros, A. (2023). A data-driven distributionally robust approach for the optimal coupling of interdependent critical infrastructures under random failures. *European Journal of Operational Research*.
2. Li, S., & Shi, L. (2023). A tri-level optimization strategy incorporating wind power against coordinated cyber-physical attacks. *IET Generation, Transmission & Distribution*.