A data-driven covert attack strategy in the closed-loop cyber-physical systems

DOI: 10.1016/j.jfranklin.2018.05.046
Journal of the Franklin Institute, 2018, 355, 6454-6468.

#	Paper	IF	Citations
11	A neural-network enhanced modeling method for real-time evaluation of the temperature distribution in a data center. *Neural Computing and Applications*, **2019**, 31, 8379-8391	4.8	10
10	A Multiplicative Coordinated Stealthy Attack for Nonlinear Cyber-Physical Systems with Homogeneous Property. *Mathematical Problems in Engineering*, **2019**, 2019, 1-13	1.1	1
9	Data-driven Stealthy Actuator Attack against Cyber-Physical Systems. **2020**,		1
8	Optimal ? -stealthy attack in cyber-physical systems. *Journal of the Franklin Institute*, **2021**, 358, 151-171	4	3
7	A secure strategy for a cyber physical system with multi-sensor under linear deception attack. *Journal of the Franklin Institute*, **2021**, 358, 6666-6683	4	1
6	Mode division-based anomaly detection against integrity and availability attacks in industrial cyber-physical systems. *Computers in Industry*, **2022**, 137, 103609	11.6	3
5	Data-Driven Covert-Attack Strategies and Countermeasures for Cyber-Physical Systems. **2021**,		0
4	A Survey on Network Security for Cyber-Physical Systems: From Threats to Resilient Design. *IEEE Communications Surveys and Tutorials*, **2022**, 1-1	37.1	3
3	A Probing Signal-based Replay Attack Detection Method Avoiding Control Performance Degradation. **2022**, 20, 3637-3649		0
2	Security of networked control systems subject to deception attacks: a survey. 1-22		3
1	Multiplicative Attacks with Essential Stealthiness in Sensor and Actuator Loops against Cyber-Physical Systems. **2023**, 23, 1957		0