# A Survey of Network Attacks on Cyber-Physical Systems

DOI: 10.1109/access.2020.2977423
IEEE Access, 2020, 8, 44219-44227.

| # | Paper | IF | Citations |
|---|---|---|---|
| 39 | . *IEEE Access*, **2020**, 8, 68883-68894 | 3.5 | 8 |
| 38 | Homomorphic Encryption of Supervisory Control Systems Using Automata. *IEEE Access*, **2020**, 8, 147185-147198 | 3.5 | 30 |
| 37 | On the Use of Fibonacci Sequences for Detecting Injection Attacks in Cyber Physical Systems. *IEEE Access*, **2021**, 9, 41787-41798 | 3.5 | 4 |
| 36 | Zero Assignment via Generalized Sampler: A Countermeasure Against Zero-Dynamics Attack. *IEEE Access*, **2021**, 9, 109932-109942 | 3.5 | 1 |
| 35 | CPS Attacks Mitigation Approaches on Power Electronic Systems With Security Challenges for Smart Grid Applications: A Review. *IEEE Access*, **2021**, 9, 38571-38601 | 3.5 | 5 |
| 34 | Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence. *Sustainability*, **2021**, 13, 3196 | 3.6 | 12 |
| 33 | Universal Zero Dynamics: The SISO Case. **2021**, | | 0 |
| 32 | Cyberattack Resilient Control for Power Electronics Dominated Grid with Minimal Communication. **2021**, | | 1 |
| 31 | Detection and Isolation of DoS and Integrity Cyber Attacks in Cyber-Physical Systems with a Neural Network-Based Architecture. *Electronics (Switzerland)*, **2021**, 10, 2238 | 2.6 | 4 |
| 30 | A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications. *IEEE Communications Surveys and Tutorials*, **2021**, 23, 1125-1159 | 37.1 | 18 |
| 29 | Feature Selection Improves Tree-based Classification for Wireless Intrusion Detection. **2020**, | | 2 |
| 28 | GPU-based Classification for Wireless Intrusion Detection. **2020**, | | 0 |
| 27 | 3C3C Model of Distribution Internet of Things Based on MQTT. **2020**, | | |
| 26 | A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid. *International Journal of Electrical Power and Energy Systems*, **2022**, 136, 107720 | 5.1 | 3 |
| 25 | A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid Part I: Background on CPPS and necessity of CPPS testbeds. *International Journal of Electrical Power and Energy Systems*, **2022**, 136, 107718 | 5.1 | 6 |
| 24 | Optimization-Based Assessment of Initial-State Opacity in Petri Nets. *AIRO Springer Series*, **2021**, 127-138 | 0.3 | 1 |
| 23 | Novel Hybrid Model for Intrusion Prediction on Cyber Physical Systems Communication Networks based on Bio-inspired Deep Neural Network Structure. *Journal of Information Security and Applications*, **2022**, 65, 103107 | 3.5 | 1 |

| | | | |
|---|---|---|---|
| 22 | An optimization-based approach to assess non-interference in labeled and bounded Petri net systems. *Nonlinear Analysis: Hybrid Systems*, **2022**, 44, 101153 | 4.5 | 1 |
| 21 | A Survey on Dynamic Corrective Control of Asynchronous Sequential Machines. *Applied Sciences (Switzerland)*, **2022**, 12, 2562 | 2.6 | |
| 20 | Mitigation of black hole attacks in 6LoWPAN RPL-based Wireless sensor network for cyber physical systems. *Computer Communications*, **2022**, | 5.1 | 0 |
| 19 | Recommendation Method of Honeynet Trapping Component Based on LSTM. **2021**, | | |
| 18 | A Generalized Comprehensive Security Architecture Framework for IoT Applications Against Cyber-Attacks. *Lecture Notes in Electrical Engineering*, **2022**, 455-471 | 0.2 | |
| 17 | Event-triggered model-free adaptive control for nonlinear cyber-physical systems with false data injection attacks. *International Journal of Robust and Nonlinear Control*, **2022**, 32, 2442-2452 | 3.6 | 1 |
| 16 | Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures). *IEEE Access*, **2022**, 1-1 | 3.5 | 0 |
| 15 | A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. *IEEE/CAA Journal of Automatica Sinica*, **2022**, 9, 784-800 | 7 | 12 |
| 14 | Design and implementation of robust corrective control systems with permanent sensor faults. *Information Sciences*, **2022**, | 7.7 | |
| 13 | 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 |
| 12 | Intelligent and secure framework for critical infrastructure (CPS): Current trends, challenges, and future scope. *Computer Communications*, **2022**, | 5.1 | |
| 11 | Secret Inference and Attacktability Analysis of Discrete Event Systems. *Information Sciences*, **2022**, | 7.7 | |
| 10 | Universal Zero Dynamics Attacks Using Only Input-Output Data. **2022**, | | 0 |
| 9 | State-Feedback Control for Cyber-Physical Discrete-Time Systems under Replay Attacks: An LMI Approach. **2022**, 2022, 1-9 | | 0 |
| 8 | Robust input/output model matching of asynchronous sequential machines under intermittent actuator faults. **2022**, | | 0 |
| 7 | Multi-loop networked control system design subject to interchange attack. | | 0 |
| 6 | Intrusion Response Systems for Cyber-Physical Systems: A Comprehensive Survey. **2022**, 102984 | | 0 |
| 5 | DDoS Attacks on Smart Manufacturing Systems: A Cross-Domain Taxonomy and Attack Vectors. **2022**, | | 0 |

| | | |
|---|---|---|
| 4 | Cyber Physical System: Security Challenges in Internet of Things System. **2022**, | 0 |
| 3 | Modular Supervisory Control for the Coordination of a Manufacturing Cell with Observable Faults. **2023**, 23, 163 | 0 |
| 2 | An Improved Light Weight Countermeasure Scheme to Efficiently Mitigate TCP Attacks in SDN. **2022**, 501-511 | 0 |
| 1 | Towards Secure Consensus of Multi-Agent Systems via a Virtual Network and Heterogeneous Controller Gains. **2022**, 55, 236-241 | 0 |