Annual Conference of the IEEE Industrial Electronics Society (IECON 2022)

Special Session on

"Machine Learning for Cyberphysical Security and Resilience in Smart Grids"

Organized by

Mohamed Benbouzid (Mohamed.Benbouzid@univ-brest.fr)
University of Brest, France

Mohamed Amine Ferrag (ferrag.mohamedamine@univ-guelma.dz)
University of Guelma, Algeria

Tarek Berghout (t.berghout@univ-batna2.dz)
University of Batna 2, Algeria

Call for Papers

Theme:

In modern smart grids that rely on connectivity between cyber and physical systems, privacy preservation of data traffic during system monitoring is one of the top priorities of shareholders. In fact, cyberspace adversaries attempt to access networking platforms to commit criminal activities such as disrupting or maliciously control the entire process of electricity delivery including generation, distribution and even customer services such as billing, resulting in serious damage including financial loss, loss of reputation, and a potential loss of life. Therefore, continuous training of individuals on up-to-date security precautions in addition to the use of advanced modeling technologies is necessary precautions to ensure reliable data traffic and power transmission. Exploring the available literature, it is undeniable that machine learning has become the latest in the timeline and one of the leading artificial intelligence technologies capable of detecting, identifying and responding by mitigating adversary attacks in smart networks.
In this context, the objective of this special session is to address and disseminate the state of the art research and ongoing development results on the implementation of machine learning-based strategies for cyberphysical security and resilience in smart grids.

Topics of interest include, but are not limited to:

1	Exploring advanced techniques for centralized, decentralized and federated learning.
2	Cybersecurity models for offline learning, and cloud, fog and edge computing.
3	Discussing both small-scale and deep machine learning algorithms.

Good quality papers may be considered for publication in the IEEE Trans. on Industrial Electronics, subject to further rounds of review.

4	Machine learning for data confidentiality, integrity and availability.
5	Machine learning for attack identification under both industrial and Internet of Things (IoT) control protocols used in smart grids.
6	Risks analysis in smart grids (i.e. phishing, denial of service, malware spreading, Eavesdropping and traffic analysis).
7	Machine learning for attack identification in different levels such as electricity generation, transmission, distribution and consumption.
8	Machine learning for user behavior modeling.

Sponsoring IES Technical Committee(s):

IEEE IES Technical Committee on Renewable Energy Systems https://res.ieee-ies.org/

Submissions Procedure:
All the instructions for paper submission are included in the conference website**: https://iecon2022.org/**

Deadlines:

Full paper submission:	April 15, 2022
Paper acceptance notification:	June 17, 2022
Camera-ready paper submission:	July 29, 2022

Good quality papers may be considered for publication in the IEEE Trans. on Industrial Electronics, subject to further rounds of review.