27th International Conference & Exhibition on
ELECTRICITY DISTRIBUTION
CIRED
ROME, ITALY
12-15 JUNE 2023

TUTORIAL N°1

Data Sharing and cybersecurity in smart grids

Background

In smart distribution grids, the digitalization strategy, led by the massive roll-out of smart meters collecting fine-grained energy flows, is key to stimulate innovation in data-driven Machine Learning (ML) technologies. However, despite the massive increase in ML research (showing its potential to improve current management strategies in energy systems), it is evident that ML models are not yet ready to be widely adopted, mainly due to data privacy concerns. Governments or organizations worldwide are increasingly committed to data privacy protection.
In this way, in the current liberalized environment that allows electricity users to decide whether sharing smart meter data or not, (individual and industrial) agents may conceal their database because it contains sensitive information (e.g., on energy usage, building occupancy or business operation). If agents use only their own local data, they inevitably lose the explanatory power contained in measurements from others, which may lead to opportunity costs.
Overall, data barrier becomes a fundamental concern for big data analytics for smart distribution systems. Thus, it is of vital importance to figure out how to preserve the privacy of consumers as well as promote secure data sharing among each other in energy systems.

At the same time, the European Commission is preparing a Network Code for cybersecurity with objective to develop a strategy for safeguarding interconnected European electrical grid. DSOs, who are already considered Operators of Essential Services (OES) under the NIS Directive, will need to be compliant with the Network Code. This requires a proper identification of critical business processes as well as understanding, assessing and managing related risks, and lastly the use of relevant cybersecurity controls to safeguard the operation of distribution grids.

Aim of the tutorial

The purpose of the tutorial is to present how do deal with privacy issues in smart distribution grids, regarding both data sharing in big data analytics and the cybersecurity aspects.

The first part of this tutorial will be dedicated on how to break the data barrier and promote data sharing. After giving a broad overview of new technologies for data sharing (blockchains, noise-injection techniques, etc.), efforts will be devoted to two aspects, i.e., i) privacy-preserving data analytical methods, and ii) data pricing or valuation approaches.

To that end, the relevant statistical methods and data-driven approaches in distribution systems will be introduced, along with recent advances in privacy-preserving settings (e.g., federated learning, differential privacy, etc.) to enable data sharing.
In complement, the data trading mechanisms and data value quantification methods in power and energy industries will be summarized and compared.

The second part of the tutorial is focused on the discussion of cybersecurity issues and techniques related to SCADA networks, intrusion detection, and the security of end and legacy devices. The objective is not only to understand the critical risks and technologies used today, but also to foresee innovations that can improve the cybersecurity and resilience of smart distribution networks of the future.

Content

1. Overview of technologies for data privacy (blockchains, noise-injection mechanisms, etc.)
2. Overview of traditional data analytics methods - Basics of machine learning
3. Investigate recent advances in privacy-preserving machine learning methods (e.g., federated learning, differential privacy, etc.) with illustrative applications in smart distribution grids;
4. Summarize practical implementations in data privacy and pricing;
5. Overview of the EC network code for cybersecurity
6. Overview of issues and techniques related with the cybersecurity of OT networks, with special emphasis on the resilience of SCADA networks, intrusion detection, and the security of legacy and end devices.

Expected benefits

Participants will gain an improved understanding of:

- A general vision of the different possibilities and technologies for data privacy, with a focus on data analytics (practical interest of machine learning) and support to decision (optimization).
- The different strategies for data sharing (collaborative learning, data markets & analytics markets)
- How to set-up collaborative learning between entities while keeping data privacy: introduction to (horizontal and vertical) federated learning and split learning
- The typical application scenarios for data sharing in power and energy systems
- The critical issues and countermeasures related with the security of SCADA networks, intrusion detection systems and legacy and end devices
- Some promising techniques that can impact the cybersecurity of future networks

Who should attend

Distribution system operators, regulators, companies/industries aiming to valorize their data, end-users interested in smart cooperation in modern distribution systems, academics interested in privacy-enhanced machine learning.

Support material

A copy of all the presentation material used in the tutorial will be supplied to delegates (electronic version).

About the presenters

Jean-François Toubeau : jean-francois.toubeau@kuleuven.be

Jean-François Toubeau received the Master degree and the Ph.D. degree in in electrical engineering from the University of Mons (Belgium) in 2013 and 2018, respectively.
He is currently a Senior Researcher with the University of Leuven (KU Leuven) Energy Institute, TME Branch (energy conversion).
His research interests include machine learning and decision-making in modern power systems.

Yi Wang : yiwang@eee.hku.hk

Yi Wang is currently an Assistant Professor with the Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong.
Yi Wang received the B.S. degree from Huazhong University of Science and Technology, Wuhan, China, in June 2014, and the Ph.D. degree from Tsinghua University, Beijing, China, in January 2019.
His research interests include data analytics in smart grids, energy forecasting, multienergy systems, Internet of Things, and cyber–physical–social energy systems.

Alysson Bessani: anbessani@ciencias.ulisboa.pt

Alysson Bessani is an Associate Professor of the University of Lisbon Faculty of Sciences, Portugal, and director of the LASIGE research unit. He received his Ph.D. in Electrical Engineering from UFSC (Brazil) in 2006, was a visiting professor at Carnegie Mellon University (2010) and a visiting researcher at Microsoft Research Cambridge (2014). Alysson coordinated/collaborated in ten international projects and co-authored more than 100 peer-reviewed publications on dependability, security, critical infrastructures protection, Byzantine fault tolerance, and cloud computing. He is also a co-founder of the Vawlt dependable & secure cloud storage startup (https://vawlt.io). More information about him can be found at http://www.di.fc.ul.pt/~bessani.
