RES-TMO

Fonds européen de développement régional (FEDER)
Europäischer Fonds für regionale Entwicklung (EFRE)

Report 7.2.1: Predictive models of data security vulnerabilities in the TMO

Bushra Canaan, Djaffar Ould Abdeslam

Université de Haute-Alsace (UHA), Institut de Recherche en Informatique, Mathématiques, Automatique et Signal (IRIMAS)

Introduction

This report is based on our technical contribution linked to the thesis of Bushra CANAAN on cyber-physical security in smart grids. It consists of citing all scientific publications funded by the RES-TMO project under the WP7 of data and energy security. It also mentioned the technical events, conferences and workshops that we have attended either to present our findings, discover the work of other colleagues or searching for potential collaborations from both the academic and the industrial fields.

Background and research gap

Over the last decade, energy infrastructures, particularly electricity infrastructures, have undergone significant changes, characterized by the shift from a system in which fossil-fuel-based generation adapts to user consumption to one in which different types of users – generators, consumers, and those who do both – are managed.

Another development is the vast digitization of the entire infrastructure in order to optimize, remotely supervise, and monitor an ever-more complicated system. Furthermore, to meet global energy demand growth and climate change, there is a growing need for energy efficiency and optimization. Demand-response services are offered to users to help them save energy by allowing them to optimize their use, such as by reducing or changing their electricity usage during peak periods. These services rely on networked smart devices, such as sensors and actuators that are extensively used in homes to monitor energy usage and limit energy equipment consumption to avoid overload. These smart devices, often known as the Internet of Things, are expected to number in the billions in the coming years. The benefits of this change are expected to include a more cost-effective, long-term, and reliable energy source.

Meanwhile, energy systems are becoming increasingly vulnerable to cyber-attacks. Because of the widespread use of ICT (Information and Communication Technologies) and new data interfaces such as new and connection-oriented meters, collectors, and other smart devices, the attack surface is expanding, providing new ports of entry for attackers. Furthermore, energy systems are high-impact targets for attackers, such as causing large supply disruptions or obtaining critical information. The increasing amount of private sensitive consumer data available to service providers, utilities, and third-party partners can potentially be a motivator for cyber-attacks. The energy sector looks to be one of the three most impacted sectors with the greatest incident costs, according to a research published by ENISA in August 2016 measuring the cost of cyber security incidents affecting vital information infrastructures.

Publications

Journal paper: Microgrid cyber-security: Review and challenges toward resilience

Abstract: The importance of looking into microgrid security is getting more crucial due to the cyber vulnerabilities introduced by digitalization and the increasing dependency on information and communication technology (ICT) systems. Especially with a current academic unanimity on the incremental significance of the microgrid's role in building the future smart grid. This article addresses the existing approaches attending to cyber-physical security in power systems from a microgrid-oriented perspective. First, we start with a brief descriptive review of the most commonly used terms in the latest relevant literature, followed by a comprehensive presentation of the recent efforts explored in a manner that helps the reader to choose the appropriate future research direction among several fields.

Published in Applied Sciences international peer-reviewed, open access journal (https://www.mdpi.com/journal/applsci).

Full text available online on the following link:

https://www.mdpi.com/2076-3417/10/16/5649/htm

Conference paper: Detecting Cyber-Physical-Attacks in AC microgrids using artificial neural networks

Abstract: In this paper, we are using a Nonlinear AutoRegressive eXogenous Neural Network NARX to diagnose the existence of cyber intrusion in a fully simulated microgrid. An online power estimator is placed at the point of common coupling to predict the normal active power signals. Whereas, Detected Faults or abnormalities in the estimated signal could indicate the presence of manipulated data and hence, cyber intrusion. The proposed method is able to capture different types of attacks including False Data Injection FDI and replay attacks.

Published in: 2021 IEEE 30th International Symposium on Industrial Electronics (ISIE)

Full text available on IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/9576466

Book Chapter: A regional cross-border approach to the energy transition

Political context and decarbonisation pathways, renewable energy potentials and two energy system models.

Abstract: A carbon-neutral energy system is the cornerstone of a decarbonised economy in line with the 2015 Paris Agreement. According to the literature, high-quality renewable energy sources (RES) in combination with increased energy efficiency, storage, sector coupling, demand-side management and digitalisation can be said to provide good prospects for a low carbon supply of electricity, heat and fuels for households, transport and industry. While most studies focus on the EU or national levels, policies are ultimately implemented at regional and local levels. This chapter provides an overview of key elements of viable energy decarbonisation pathways, while paying attention to the policy goals and context of the study area, presents preliminary findings on regional RES potentials and proposes two different models for modelling the energy system in the Upper Rhine Region (TMO). PERSEUS-EU aims to find the most cost-efficient pathways to reach EU policy goals integrating regional RES, while the Regional Energy Planning Model (REPM) analyses regional decarbonisation scenarios assessing the required energy storage and backup infrastructure. Our preliminary results indicate that regional potentials for wind, solar and geothermal energy generation for electricity and heat are considerable, even when considering existing constraints, and that cross-border cooperation can contribute to meeting long-term climate goals.

Available on : https://www.taylorfrancis.com/chapters/edit/10.4324/9781003199977-3/regional-cross-border-approach-energy-transition-ines-gavrilut-felix-kytzia-kristina-izmailova-zeina-najjar-barbara-koch-marco-andr%C3%A9s-guevara-luna-adrien-barth-alain-clappier-nad%C3%A8ge-blond-johannes-miocic-joris-dehler-holland-bushra-canaan

Accepted conference paper: Experimental HIl implementation of RNN for detecting cyber physical attacks in AC microgrids

Abstract— In this paper, a real-time cyber intrusion detection mechanism based on recurrent neural networks is implemented for detecting cyber-physical attacks targeting AC microgrids (MG). An AutoRegressive eXogenous Neural Network (NARX) model is deployed as an Intelligent Detection System (IDS), to detect cyber-physical anomalies in the behavior of exchanged active power in a

connected AC microgrid. Results are validated through a Hardware-in the loop simulation using the Opal RT real-time simulator and an external microcontroller board (Arduino) for Embedding the used Artificial Neural Network ANN.

This paper will be presented on the SPEEDAM 2022 (22-24 June, 2022) SORRENTO – ITALY

http://www.speedam.org/

Events, conferences and workshops

ZHAW: Zurich University of Applied Sciences DynPOWER workshop Winterthur(16 September 2019)

It is an event connected to the subsequent OPAL-RT 2019 user conference. Where a lot of international speakers have gathered proposing a wider overview on the activities related to power systems simulations namely, Frequency Challenges of the Future Power System, Tools for Power Systems Dynamic Performance: Analysis based on WAMS and Advances in Synchrophasor Monitoring, Dynamic Power System Mirror for Application in Energy Management Systems, Dynamic model selection of a modular multilevel converter for a HVDC grid stability test, WAMS/WAMPAC concepts and implementations in practice", Micro vs MEGA grids: trends influencing the development of the power system and finally Stability assessment for bulk power systems using unsupervised data mining.

RT Spotlight | Zürich - OPAL-RT: OPAL-RT's Local Conference on Power Systems & Power Electronics Real-Time Simulation (17-18 September 2019)

During the past 10 years, OPAL-RT's conferences have attracted hundreds of attendees from all over the world, to catch up with the latest trends in real-time simulation solutions for power systems and power electronics.

RT Spotlight Zürich has presented the OPAL-RT vision of the future of technology through their expert talks that covered market trends, product roadmaps, best practices with their product and new features. The event also hosted Keynote presentations from many international organizations in addition to Power Systems experts sharing their knowledge on the current industry trends and emerging technologies.

Extremely rich presentations were given by representatives from General Electric GE Grid Solutions, ABB Switzerland Ltd, Austrian Institute of Technology (AIT), UPV/EHU and APERT group, Ostfalia University of Applied Sciences, Oldenburger OFFIS - Institute for Computer Science, Ilmenau University of Technology, Swiss Federal Institute of Technology of Lausanne (EPFL), France's transmission system operator RTE, RWTH Aachen University, Zurich University of Applied Science ZHAW and Karlsruhe Institute of Technology.

In general, the conference has focused on 4 key aspects which incorporated Power Systems, Power Hardware-In-The-Loop (PHIL), Microgrids and Cybersecurity.

Starting with the newest developments in Power Systems testing, such as up-to-date simulation performance benchmark, real-time simulation on FPGA and advances in new applications such as MMC, DER and Travelling wave protection relays. Moving on to introducing the revolutionizing aspects that Power Hardware-in-the-loop (PHIL) simulation could offer to the industry, taking testing and validation of power system and power electronics controls, protection and proof of concept to the next level all along with discussing best practices, from selecting an amplifier to optimizing stability

when the loop is closed. As for the most relevant subjects regarding our work which involves the microgrids and applications of cyber security in the energy systems, the conference dedicated a good part explaining the simulation solutions for the most challenging microgrid applications from fast Power Electronic DER controls and protection to high level supervisory controls, besides the most advanced applications on Microgrid HIL from around the world and how OPAL-RT's solutions addressed it.

On September 18: The conference was warped up by a guided visit to the ZHAW Power System and Smart Grid lab, which provided the opportunity to discover how topics such as renewable generation, smart grids, energy management and energy storage systems is being addressed through Power-HIL.

ISIE2021-Kyoto the 30th International Symposium on Industrial Electronics (20-23 June 2021)

The ISIE annually gathers industry experts, researchers and academics to share ideas and experiences surrounding frontier technologies, breakthroughs, innovative solutions, research results, as well as initiatives related to industrial electronics and their applications.

ISIE 2021 worked on introducing conference participants that were exposed to standards development efforts in the Industrial Engineering society (IES) in one way or another to the propagation of the IES sponsored standards family and the achieved progress in industrial electronics and IoT/IIoT/CPS harmonization. In perspective to Provide stable or permanent verification and compliance Centers of Expertise (COE) for industry and academia use, distributed globally under IES Standards support.

With a large number of regular and special sessions, the conference mainly treated the theme of SDGs (Sustainable Development Goals). Especially, Goal.7 "Ensure access to affordable, reliable, sustainable and modern energy for all" and Goal.9 "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation".

A presentation from our part was given in the Modelling, Simulation, Protection and Control of Smart Grids II session on the 22th of June. The presentation had demonstrated our proposed method for detecting cyber physical attacks using artificial neural networks. It discussed cyber-attacks jeopardizing connected microgrids as examples of vulnerable Cyber physical systems (CPSs). Driven by the apprehension of triggering cascading failure events generated by a violated entity that communicates with the grid on both the physical and cyber levels, especially with the ambiguity surrounding governing norms that define microgrids functionality, ownership and operation access control.

In comparison to the partially reliable power primitive system, research into improving the security of the electrical power system is still in its early stages, with numerous unidentified security vulnerabilities. Given the importance and high transmissibility of the power grid, an attack could have a substantial impact not only on the energy supply, but it could go further including industrial outputs, health sector and actual people's livelihood.

Sustainable places Rome (28 September-1 October2021)

The scope of Sustainable Places is captured directly in its name. It involves designing, building and retrofitting the places we live and work in a more sustainable way.

Sustainable Places (SP) has facilitated the market uptake of innovation for the built environment as the reference platform for European research dissemination, local area professional training, clustering workshops, and most importantly stakeholder networking.

This event has compilated high-level keynote speeches, plenary morning sessions on grand challenges, thematic clustering research and development workshops, technical paper sessions, poster area, exhibition booths and digital booths, both virtual and in-person networking not to mention professional and academic collaboration and discussions.

In its 9th edition SP has concentrated on energy communities, smart districts & cities, citizen engagement, urban planning & real estate, renewables, storage & energy efficiency and digitalization in addition to smart readiness and artificial intelligence. Themes that are strongly correlated with the RES-TMO project objectives.

Several RES-TMO colleagues has presented their work on the different work packages of the project. In our turn, we gave a presentation on the problem of securing Cyber-physical systems (CPSs) in future smart grids and energy communities, where, attempts to breach systems grow. Especially for systems that control critical infrastructure such as utilities that have become increasingly attractive targets for bad actors, whether for financial or political gain.

Opal RT workshop: Hardware in the Loop simulation, control and protection of Grids/ Microgrids (7 April 2022)

The university of haute Alsace and our lab IRIMAS has organized a workshop in collaboration with Opal RT under the theme of implementing Hardware in the Loop tests in the research of cyber physical security. Presentations on the general principles of HIl testing, case studies and our own testing results has been displayed followed by a lab tour allowing participants to discover our Microgrid installation and different filiation of the IUT of Mulhouse.