WP7 - Data security in smart grids in the RMT

I. Detailed report on the European legislation for the security of energy data
II. Report on the survey responses of electricity network operators in the three regions
III. Predictive models of data security vulnerabilities in the TMO
IV. Recommendation report on trinational protection against cyber attacks to enhance energy security
Moving from Geopolitics security

The energy grid is evolving faster than ever and utilities have been struggling to keep up:

• Distributed energy resources (DERs) have changed the way the energy grid has worked for the past 150 years.

• The intermittent nature of Distributed Energy Resources must be counteracted with highly scalable data analytics that allow us to detect, predict and prevent any issues.

• Governing and sharing data efficiently is complicated by overwhelming amounts of data and the involvement of too many teams.
CPS: CYBER PHYSICAL SECURITY

Security criteria

- More Sophisticated attacks that bypasses the barriers of software protection
Types of Attacks

- Despite the fact that cyber intrusions on cyber-physical systems (CPSs) can be found under different terms.
- These attacks can still be classified according to the one or multiple security criteria they are jeopardizing.

<table>
<thead>
<tr>
<th>Security objective</th>
<th>Attack target</th>
<th>Attack way</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Password, code algorithm</td>
<td>Decode</td>
</tr>
<tr>
<td></td>
<td>Network channel</td>
<td>Tapping</td>
</tr>
<tr>
<td>Integrity</td>
<td>Electrical parameter</td>
<td>Incorrect value</td>
</tr>
<tr>
<td></td>
<td>Switcher</td>
<td>Fake order</td>
</tr>
<tr>
<td></td>
<td>Time info</td>
<td>Fake time info</td>
</tr>
<tr>
<td>Availability</td>
<td>Communication system</td>
<td>DDoS</td>
</tr>
<tr>
<td></td>
<td>Communication system</td>
<td>Communication delay</td>
</tr>
</tbody>
</table>

- DoS (Denial of service)
- FDI (False Data Injection)

Objectives:
- Degrade: Reduce the efficiency of the attacked system
- Paralysis: Stop the attacked system
- Destroy: The attacked system is physically damaged
Challenges

- Complexity – interoperability
- Difficulty to trace attack impacts
- Multidisciplinary solution - cope with Energy market
Why Microgrids?

- Microgrid works as a subsystem or building blocks in the smart grid environment
- Decentralization
- Self-controlled entity as they have a complete control system
- Compatible: they operate in synchronous with the main grid
- Stable while changing the mode of operation
- Low-cost (management costs, long distance transmission lines)
• (PMS) is more critical in microgrids
• Microgrids represent a tempting target for attackers
State of the art on the latest technical approaches used in attack detection, risk or impact estimation, in addition to resilience and protection methods.

Microgrid Cyber-Security: Review and Challenges toward Resilience

by Bushra Canaan, Bruno Colicchio and Djaffar Ould Abdesslam

IRIMAS Laboratory, University of Haute Alsace, 61 rue Albert Camus, 68093 Mulhouse, France

* Author to whom correspondence should be addressed.

Appl. Sci. 2020, 10(16), 5640; https://doi.org/10.3390/app10165649
Received: 25 July 2020 / Revised: 9 August 2020 / Accepted: 12 August 2020 / Published: 14 August 2020

(This article belongs to the Special Issue Advances and Technologies in High Voltage Power Systems Operation, Control, Protection and Security)
Technological contribution

Recurrent Neural networks (RNN)
AutoRegressive eXogenous Neural Network (NARX)
Levenberg-Marquardt algorithm
The offline training method

IDS
IDS based on artificially intelligent models
AC microgrid:
- The connected microgrid is a more common
- The fear of triggering a cascading failure
- Same hypothesis
Detecting Cyber-physical-attacks in AC microgrids using artificial neural networks

Bouchra CANSAN
IRMAS Research Institute
Pôle Innov. Université d’Hass, Almeria
Albor-Andalusia University of Almería
Almería, Spain
bouchra.cansan@uh.es
bouchra.cansan@uh.es

Bruno COLICCHIO
IRMAS Research Institute
University of Hass Almeria
Almeria, Spain
brouna.cansan@uh.es
brouna.cansan@uh.es

Djefle OULD ABDESSAM
IRMAS Research Institute
University of Hass Almeria
Almeria, Spain
djefle.ould-abdesslam@uh.es

Abstract— In this paper, we are using a Nonlinear Auto-Regressive Exogenous Neural Network NARX to diagnose the existence of cyber intrusions in a fully modeled microgrid. An online server application is placed at the point of common coupling to predict the normal active power signals. Whereas, Deformed Faults or observations in the extracted 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.

Keywords—Cyber-physical security, Recurrent Neural Networks (RNN), NARX, AC microgrids, FDI

1. Introduction

Security concerns in smart grids require new approaches to detect data manipulation attacks (FDI) [1]. Proper detection is critical in a large-scale smart grid architecture. The current cyber-physical system of modern electrical or energy networks is a challenging challenge. However, security assessment of dynamic systems with highly nonlinear characteristics might even be difficult to access or measure in a system. Thus, recently the security of the cyber-physical system is a crucial challenge.
THANK YOU FOR LISTENING