



Securing the grid: A comprehensive analysis of cybersecurity challenges in PMU-based cyber-physical power networks

Bilkisu Jimada-Ojuolape^{a,b}, Jiashen Teh^{a,*}, Ching-Ming Lai^{c,*}

^a School of Electrical and Electronic Engineering, Universiti Sains Malaysia (USM), Engineering Campus, Nibong Tebal 14300, Penang, Malaysia

^b Department of Electrical and Computer Engineering, Faculty of Engineering and Technology, Kwara State University, Ilorin, Nigeria

^c Department of Electrical Engineering, National Chung Hsing University, Taichung 402, Taiwan

ARTICLE INFO

Key words:

Cyber-attacks
Cyber-physical power networks
Cyber security
Phasor measurement unit (PMU)
Power network security
Smart grid
Synchrophasors
Wide area monitoring systems (WAMS)

ABSTRACT

The threat of cyber-attacks poses a considerable risk to Phasor Measurement Unit (PMU) applications within Cyber-Physical Power Networks (CPPNs), leaving them susceptible to malicious attacks such as false data injection, time synchronization manipulation, and DoS attacks. Existing studies in the area of cyber security in CPPNs primarily address broader network security issues, overlooking specific challenges in networks with features like PMU integration, highlighting the urgent need to explore vulnerabilities in PMU-based networks for comprehensive understanding. In this study, a thorough analysis is conducted, exploring various cyber-attacks targeting PMU-based CPPNs. These attacks are categorized into data integrity, communication network vulnerabilities, device spoofing and tampering, and coordinated cyber-physical attacks and subsequently, discussed in detail, underscoring the pressing need for robust cybersecurity measures. The study not only provides valuable insights but also outlines future research directions, empowering power system researchers and operators to enhance the resilience of PMU-based CPPNs against evolving cyber threats. Like the need for more reliability studies that investigate impacts of cyber-attacks in PMU-based CPPNs. The findings offer a good foundation for devising effective planning and fortification strategies to navigate the challenges posed by emerging cybersecurity threats.

1. Introduction

In recent years, the landscape of power systems has undergone a transformative evolution, marked by the integration of cyber technologies into the traditional network. This amalgamation, often referred to as cyber-physical power systems, represents a paradigm shift in the way we generate, transmit, and distribute electrical power. Cyber-physical power networks (CPPNs) seamlessly blend the physical elements of power generation, transmission, and distribution with sophisticated digital technologies [1]. Traditional components, such as generators and transmission lines which form the physical layer, are now intricately connected through advanced communication networks, control systems and computing devices which form the cyber layer. This integration allows for real-time monitoring, protection, control, data exchange, and intelligent decision-making processes. Fig. 1 shows a modern CPPN infrastructure and advanced applications. CPPNs enhance the overall efficiency and reliability of the power infrastructure [2,3].

Central to the functionality of CPPNs are Intelligent Electronic

Devices (IEDs) and now more commonly Phasor Measurement Unit (PMUs) [4,5]. PMUs provide synchronized measurements of voltage and current phasors across the power grid, enabling precise monitoring and control, forming a synchrophasor-based wide area monitoring system on CPPNs [6–8]. On the other hand, other IEDs may act as intelligent sensors and actuators, facilitating communication and control functions within the system. The orchestration of these components is governed by advanced control algorithms that optimize the operation of the power grid. These algorithms leverage real-time data from PMUs and IEDs in general to make informed decisions, dynamically adjusting parameters for improved performance, reliability, and resilience [9]. While the integration of cyber technologies brings unparalleled benefits, it introduces a new set of challenges, particularly in the realm of cybersecurity. The interconnected nature of these systems makes them susceptible to malicious cyber threats that can potentially compromise the integrity and stability of the power infrastructure [10]. Some CPPN benefits, challenges and applications are shown in Fig. 2.

The progression of CPPNs introduces inherent vulnerabilities, including susceptibility to cyber-attacks that involve breaching

* corresponding authors.

E-mail addresses: jiashenteh@usm.my (J. Teh), pecmlai@gmail.com (C.-M. Lai).

<https://doi.org/10.1016/j.epsr.2024.110509>

Received 18 February 2024; Received in revised form 14 May 2024; Accepted 21 May 2024

0378-7796/© 2024 Elsevier B.V. All rights are reserved, including those for text and data mining, AI training, and similar technologies.