19th International Conference on Innovative Computing, Information and Control (ICICIC2025)
August 26-29, 2025, Kitakyushu, Japan

PS-27: ICICIC2025-200

Detection and Classification Framework for Multimodal Cyber-Physical Attacks on Microgrids

Yu Qiao and Peng Shi*

School of Electrical and Mechanical Engineering, The University of Adelaide, SA 5000, Australia
*Corresponding author: peng.shi@adelaide.edu.au

Introduction

As a cyber-physical system, microgrids are highly coupled between the communication and physical layers, making them vulnerable to cyberattacks such as DoS and FDI. Current mainstream detection methods generally rely on single-modal data (e.g., based solely on physical measurements or communication logs) and are unable to systematically simulate the dynamic correlations between multimodal information, thus limiting detection capabilities.

Mathematical Formulas

Design an independent linear projection layer or shallow neural network for each modality and map it to the embedding space dimension:

$$E_{phys}(x_{t,phys}) = W_{phys}\, x_{t,phys} + b_{phys}$$
$$E_{comm}(x_{t,comm}) = W_{comm}\, x_{t,comm} + b_{comm}$$

Research Questions

How to develop a method to effectively fuse heterogeneous time series data from the physical layer and communication layer of microgrids. And detect cyberattacks under varying network configurations and attack scenarios.

Figure

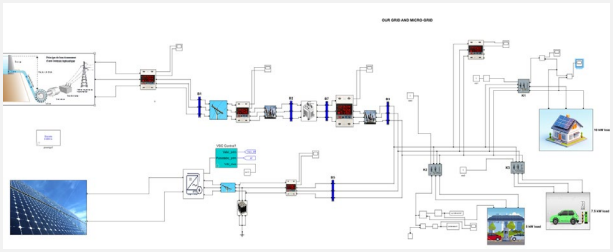

Figure 1. Microgrid simulation architecture with cyber-physical data interface[j]

Simulink-based MG model with PV, hydro, loads, and transformers, connected to a Python cyber emulator for real-time CPS co-simulation and attack-injected dataset generation.

Methodologies

We design a Transformer-based neural architecture that accepts dual-modality sequential inputs from physical and communication layers. Each modality is first encoded via learned embeddings and fused with positional encodings. The unified sequence is then processed by a Transformer encoder to extract temporal dependencies and cross-domain correlations. The final output layer classifies each input window into one of four categories: normal, fault, FDI, or DoS.

Table

Table 1. Multimodal input feature composition

Modality	Features
Physical Layer	Voltage (V), Current (I), Frequency (f)
Communication Layer	Packet Length, Inter-arrival Time, Entropy, Command Type
Temporal Encoding	Time-of-day, Day-of-year (sin/cos positional encoding)
Label (Target)	Normal, Fault, FDI, DoS

Conclusion

This study proposes a microgrid anomaly detection and classification framework based on multimodal Transformer. By taking the heterogeneous time series data of the physical layer and the communication layer as unified input and using the powerful self-attention mechanism of Transformer, it can effectively capture complex abnormal patterns. The most significant contribution of this method is that it does not require an explicit topological structure and can learn the implicit associations between different microgrid components and modes from the data itself, which is of great significance for actual microgrid systems with dynamically changing topological structures or incomplete information.