Early-Stage Anomaly Detection in IT-OT Power Grid Communication Networks Using Wavelet Transform and Hybrid Deep Learning

Tohid Behdadnia[1,2], Klaas Thoelen[1,2], Geert Deconinck[1,2]

[1]KU Leuven, [2]EnergyVille

In cyber-physical power systems, the imperative convergence of information technology (IT) and operational technology (OT) engenders enhanced operational efficiency, yet increases susceptibility to cyberattacks. This scenario accentuates the necessity for deploying effective anomaly detection (AD) mechanisms to protect these critical infrastructures against the devastating impacts of cyberattacks. Traditional AD algorithms often focus on identifying anomalies through analyzing spatial and temporal patterns derived from the physical system measurements, an approach that typically proves effective only after a cyberattack has been successfully executed at the later stages of the cyberkill chain. This reactive approach fails to respond to evolving cyber threats. To tackle this issue, this article introduces an innovative framework for early-stage AD in integrated IT-OT power grid communication networks. Our approach models the IT-OT network as a traffic dispersion graph and applies wavelet transform to decompose the real-time traffic throughput of each information node into its constituent sub-bands to extract time-frequency features. These features are then weighted and prioritized using a graph attention mechanism and fed into a bidirectional long short-term memory for temporal analysis, ultimately classifying the nodes as normal or abnormal. Our experiments confirm the methodology's precise detection and localization of active cyberattack sites, outperforming existing state-of-the-art AD models.

979-8-3315-8138-1