frontiers | Frontiers in Energy Research

TYPE Editorial
PUBLISHED 14 August 2023
DOI 10.3389/fenrg.2023.1261340

OPEN ACCESS

EDITED AND REVIEWED BY
ZhaoYang Dong,
Nanyang Technological University,
Singapore

*CORRESPONDENCE
Huan Xi,
huanxi@xjtu.edu.cn

RECEIVED 19 July 2023
ACCEPTED 07 August 2023
PUBLISHED 14 August 2023

CITATION
An D, Xi H, Yang J and Zhang H (2023), Editorial: Future electricity system based on energy internet: energy storage system design, optimal scheduling, security, attack model and countermeasures.
Front. Energy Res. 11:1261340.
doi: 10.3389/fenrg.2023.1261340

Editorial: Future electricity system based on energy internet: energy storage system design, optimal scheduling, security, attack model and countermeasures

Dou An[1], Huan Xi[2]*, Jianhua Yang[3] and Hanlin Zhang[4]

[1]MOE Key Laboratory for Intelligent Networks and Network Security, Xi'an, China, [2]School of Energy and Power Engineering, Xi'an Jiaotong University, Xi'an, China, [3]School of Computer Science, Columbus State University, Columbus, IN, United States, [4]College of Computer Science and Technology, Qingdao University, Qingdao, Shandong, China

KEYWORDS

energy internet, energy storage system design, optimal scheduling, security design, data integrity attack

Editorial on the Research Topic
Future electricity system based on energy internet: energy storage system design, optimal scheduling, security, attack model and countermeasures

1 Introduction

Energy Internet, a futuristic evolution of electricity system, is conceptualized as an energy sharing network. The energy internet integrates advanced sensors, efficient measurement technologies, advanced control methods, efficient energy utilization/conversion/storage system to achieve economical, efficient, and environmentally friendly operation of the power grid system. The energy internet also contains a large amount of heterogeneous information, which requires the more support of information technology in the system design than traditional power systems. Moreover, due to the open network environment of the energy internet, any anomaly or malicious attack in the system can bring unpredictable and significant losses to the overall grid operation.

The Research Topic entitled "Future Electricity System Based on Energy Internet: Energy storage system design, Optimal Scheduling, Security, Attack Model and Countermeasures" aims to investigate energy storage system design, optimal scheduling, attack detection model and the state restoration strategy from the perspective of the energy internet. Moreover, the Research Topic also includes efficient energy utilization, conversion and storage technologies, and cyber-physical attacks against the smart grid from the adversaries' perspective. The researches of this Research Topic are helpful in improving the security and the operation efficiency of power grid system and can be conveniently applied to the real-world security management system of the energy internet. There are in total 13 articles accepted for this Research Topic after careful peer-to-peer review, and they cover the following four categories.

1.1 Data integrity attacks against the dynamic state estimation and the interactive energy information

Zhang and Yang (2022) proposed a deep learning-based detection approach against false data injection attacks for dynamic state estimation. In this study, the Kalman filter was used to dynamically estimate the state values from IEEE standard bus systems. A long short-term memory network was utilized to extract the sequential observations from states at multiple time steps. Simulation results in multiple IEEE standard bus systems demonstrated that the proposed detection approach outperforms benchmarks in improving the detection accuracy of malicious attacks. Zhang et al. (2023) developed a detection model of scaling attacks in smart grid considering consumption pattern diversity (*SA2CPD*) to ensure that scaling attacks can be effectively detected when users have multiple consumption patterns. The proposed detection approach leveraged K-means method to distinguish different consumption patterns, divided time periods in every day into two categories based on the binarization values, and used one of them with the greatest information gain to construct a decision tree for judgment. Both theoretical and simulation results based on the GEFCom2012 dataset show that the *SA2CPD* model has a higher *F1 score* than the decision tree model without considering consumption pattern diversity, the KNN model and the Naive Bayes model. Li et al. (2023) formalized the bidding decision problem of EVs into a Markov Decision Process, designed a local Fast Gradient Sign Method which affects the environment and the results of reinforcement learning by changing its own bidding form the perspective of attackers and designed a reinforcement learning training network containing an attack identifier based on the deep neural network. Comprehensive simulation results shown that the proposed attack method will reduce the auction profit by influencing reinforcement learning algorithm, and the protection method will be able to completely resist such attacks.

1.2 Artificial intelligence technology-based optimal scheduling of power grid

Cui et al. (2023) modeled charging scheduling problem as a Markov decision process (MDP) and utilized the twin delayed deep deterministic policy gradient algorithm (TD3) to ensure the maximum benefit of the electric vehicle aggregator (EVA), while maintaining minimal fluctuation in the microgrid exchange power. To verify the effectiveness of the proposed method, this paper set up two comparative experiments, using the disorder charging method and deep deterministic policy gradient (DDPG) method, respectively. Results shown that the strategy obtained by TD3 is optimal, which can reduce power purchase cost by 10.9% and reduce power fluctuations by 69.4%. Li et al. (2023) formalized the charging and discharging sequential decision problem of the parking lot into the Markov process and used a Deep Q-Network (DQN)-based reinforcement learning architecture to solve the MDP model. Simulation results with real-world power usage data shown that the proposed method will reduce the peak load by 10% without affecting the travel plan of all electric vehicles. Besides, compared with random charging and discharging scenarios, the proposed method achieved better performance in terms of state-of-charge (SoC) achievement rate and peak load shifting effect. Lv et al. (2023) proposed an optimization method for determining the capacity of energy storage system for smoothing the power output of renewable energy. In this paper, the energy storage configuration model was built according to the objective function and constraints and the genetic algorithm was used to solve the optimization model, obtain the corresponding parameters, and complete the configuration of energy storage capacity. Simulation results shown that at 1 and 10 min, the flattened volatility is about 2% and 5%, while the actual penetration volatility is about 20% and 30%.

1.3 Security design for renewable energy utilization

Zhang et al. (2022) proposed several secure multi-party computation (MPC) protocols that enable deep learning training and inference for electricity consumer characteristics identification while keeping the retailer's raw data confidential. Comprehensive experiments based on the Irish Commission for Energy Regulation dataset to verified that the proposed MPC-based protocols have comparable performance in multiple neural network models and optimization strategies. Zhai et al. (2023) put forward a lightweight and dynamic authenticated key agreement and management protocol based on identity cryptosystem and elliptic curve cryptography. The proposed protocol can significantly reduce the computation overhead of the resource-constrained smart meters. Systematic proof of this paper showed that the designed protocol not only guaranteed the confidentiality and integrity of transmitted messages, but also resisted various attacks from an adversary. Gai et al. (2023) proposed a certificateless public auditing scheme for cloud-based smart grid data, which can avoid complicated certificate management and inherent key escrow problems. In order to prevent the disclosure of the private data collected by the smart grid during the phase of auditing, the proposed method used the random masking technology to protect data privacy. The security analysis and the performance evaluation shown that the proposed scheme is secure and efficient. Deng et al. (2023) investigated the problem of system line failures caused by AC or DC blockages from the attacker's perspective and utilized the multiple-feed short-circuit ratio constraint method, output adjustment measures of the energy storage system, sensitivity control, and distance third-segment protection adjustment to reduce system losses from the perspective of dispatch-side defense. Besides, a deep reinforcement learning algorithm was proposed to obtain the Nash equilibrium of the game model. Simulation results verify the appropriateness of the two-stage dynamic zero-sum game model to schedule online defense strategies and the effectiveness and superiority of the energy storage system participating in defense adjustment.

1.4 Information technology for the energy internet system

Zhang et al. (2022) addressed the state estimation problem of linear dynamic systems with high-order autoregressive moving

average non-Gaussian noise and proposed a new filter based on correntropy instead of the commonly used minimum mean square error (MMSE) to deal with non-Gaussian noise. Simulation results verify the effectiveness of the proposed algorithm. Xia et al. (2022) designed a new discrete harmonic extractor called quadrature sine wave extractor (QSE), which used the idea of the observer to extract multiple harmonic components at the same time. Compared to the widely used proportional multi-resonant controller, the proposed QSE can reduce current harmonics and improve system stable performance by using it in the current control of grid-connected inverters. Comparative experiments on a three-phase grid-connected inverter verified the effectiveness of the proposed method. Han et al. (2022) proposed a novel automatic modulation classification (AMC) method for low SNR signals. First, the sampled I/Q data is converted to constellation diagram, smoothed pseudo Wigner-Ville distribution (SPWVD), and contour diagram of the spectral correlation function (SCF). Second, convolution auto-encoder (Conv-AE) is used to denoise and extract image feature vectors. Finally, multi-layer perceptron (MLP) is employed to fuse multimodal features to classify signals. Simulation results on RadioML 2016.10A public dataset proved that AMC-MLP provides significantly better classification accuracy of signals in low SNR range than that of other latest deep-learning AMC methods.

2 Conclusion

This Research Topic aims to collect and encourage research related to the exploitation and implementation of data integrity attacks, optimal scheduling and security design from the perspective of the energy internet, which aims to improve the security and the operation efficiency of power grid system. Fortunately, this Research Topic has received widespread interests and submissions from the researchers, which published 13 articles in total until its close date. The published articles cover following four categories: data integrity attacks against the dynamic state estimation and the interactive energy information, artificial intelligence technology-based optimal scheduling of power grid, security design for renewable energy utilization and information technology for the energy internet system. The published articles in this Research Topic can be conveniently applied to the real-world security management system of the energy internet.

Author contributions

DA: Writing-original draft, Writing-review and editing. HX: Writing-original draft, Writing-review and editing. JY: Writing-original draft. HZ: Writing-review and editing.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note