energies

MDPI

Editorial

Secure and Efficient Communication in Smart Grids

Mostafa M. Fouda [1,2,*] and Mohamed I. Ibrahem [3,4]

[1] Department of Electrical and Computer Engineering, College of Science and Engineering, Idaho State University, Pocatello, ID 83209, USA
[2] Center for Advanced Energy Studies (CAES), Idaho Falls, ID 83401, USA
[3] School of Computer and Cyber Sciences, Augusta University, Augusta, GA 30912, USA
[4] Department of Electrical Engineering, Faculty of Engineering at Shoubra, Benha University, Cairo 11672, Egypt
* Correspondence: mfouda@ieee.org

This Special Issue on "Secure and Efficient Communication in Smart Grids" received a total of 11 submitted articles, of which 5 were accepted and published after each passing an independent peer-review process.

A brief summary of the contents associated with each of the selected papers belonging to this Special Issue is included below:

In 'Privacy-Preserving Charging Coordination Scheme for Smart Power Grids Using a Blockchain', the authors Hany Habbak, Mohamed Baza, Mohamed M. E. A. Mahmoud, Khaled Metwally, Ahmed Mattar, and Gouda I. Salama [1] proposed a privacy-preserving charging coordination scheme using a blockchain. The blockchain achieves decentralization and transparency, which help to mitigate security issues related to centralized architectures. Additionally, a verifiable aggregation mechanism combined with an aggregated signing technique was used to ensure data source integrity, the identity of the sender, and the privacy of the consumer. Security analysis, experiments, and simulations on both sides (off-chain and on-chain) were carried out to analyze the security of our scheme and to evaluate its performance in terms of communication and computation overheads. The results confirm that the communication overhead in terms of message sizes is acceptable.

In 'Real-Time Locational Detection of Stealthy False Data Injection Attack in Smart Grid: Using Multivariate-Based Multi-Label Classification Approach', the authors Hanem I. Hegazy, Adly S. Tag Eldien, Mohsen M. Tantawy, Mostafa M. Fouda, and Heba A. TagElDien [2] introduced a multivariate-based multi-label locational detection (MMLD) mechanism to detect the presence and locations of False Data Injection Attacks (FDIAs) in real-time measurements with high precision and accuracy. The proposed architecture is a parallel structure that combines Long Short-Term Memory (LSTM) with Temporal Convolutional Neural Network (TCN). It was trained with Keras utilizing Tensorflow libraries, and its performance was verified on an IEEE standard bus system from the MATPOWER package. Extensive testing has shown that the proposed MMLD mechanism effectively improves the accuracy of locating stealthy FDIAs in both small and large systems under various attack conditions. Moreover, a customized loss function was proposed to address the challenge of class imbalance. The simulation results demonstrated that the proposed approach has a slight advantage in terms of complexity and scalability over benchmark models, as well as a faster rate of convergence during training. Overall, this work introduces an effective and efficient technique for detecting and locating FDIAs in real-time measurements with high precision and accuracy.

In 'Data Mining-Based Cyber-Physical Attack Detection Tool for Attack-Resilient Adaptive Protective Relays', the authors Nancy Mohamed and Magdy M. A. Salama [3] proposed a rough-set-based detection tool that can identify incorrect settings for overcurrent relays in active distribution smart grid networks to enhance the security of communication-based overcurrent relays used in adaptive protection schemes. The tool has been evaluated

Citation: Fouda, M.M.; Ibrahem, M.I. Secure and Efficient Communication in Smart Grids. *Energies* **2023**, *16*, 5613. https://doi.org/10.3390/en16155613

Received: 4 July 2023
Revised: 18 July 2023
Accepted: 21 July 2023
Published: 26 July 2023

in terms of the accuracy and consistency of the settings the relays receive, and maintaining the data integrity requirements in addition to error rate, sensitivity, and execution time.

In 'Application of Doubly Connected Dominating Sets to Safe Rectangular Smart Grids', the authors Joanna Cyman and Joanna Raczek [4] introduced and studied a two-dimensional rectangular grid graph as a model for smart grids to determine the smallest possible number of locations (nodes and points) on the grid that could serve as energy sources to other nodes while ensuring a reduction in electricity loss and providing safe communication and resistance to failures and increases in energy demand. The authors studied minimum doubly connected dominating sets in grid graphs, showed that the proposed solutions are the best possible in terms of the number of source points for the case of narrow grid graphs, and gave upper and lower bounds for the case of wide grid graphs. The significance of the proposed research is its application to the safety, economy, ecology, and reliability of the future energetic world.

In 'Load Forecasting Techniques and Their Applications in Smart Grids', the authors Hany Habbak, Mohamed Mahmoud, Khaled Metwally, Mostafa M. Fouda, and Mohamed I. Ibrahem [5] provided a comprehensive survey of state-of-the-art Load Forecasting (LF) techniques and their applications in smart grids (SGs). The existing literature and most recent techniques presented include traditional LF techniques, clustering-based techniques, Artificial intelligence (AI)-based techniques, LF techniques based on time series data, and meta-heuristic-based LF techniques. AI technology, specifically machine and deep learning algorithms, have improved LF precision in SGs. Future advancements should involve the integration of AI models with statistical models and the consideration of real-time data, sensors, distributed energy resources, and renewable energy sources for increased accuracy and sustainability.

Several applications and their vulnerabilities also discussed eleven trust models used for SM security, which are among the widely used techniques for safeguarding the data privacy of SMs' observed data in SG networks. Moreover, a comparison between the existing methods for protecting the data privacy of SMs was conducted. Finally, insightful suggestions were made for the interested researchers, taking into account the critical role that SM protection plays in catastrophe management, whether on the level of infrastructure or human life.

Author Contributions: Writing original draft and preparation, M.I.I.; writing, review and editing, M.M.F. All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Habbak, H.; Baza, M.; Mahmoud, M.M.E.A.; Metwally, K.; Mattar, A.; Salama, G.I. Privacy-Preserving Charging Coordination Scheme for Smart Power Grids Using a Blockchain. *Energies* **2022**, *15*, 8996. [CrossRef]
2. Hegazy, H.I.; Tag Eldien, A.S.; Tantawy, M.M.; Fouda, M.M.; TagElDien, H.A. Real-Time Locational Detection of Stealthy False Data Injection Attack in Smart Grid: Using Multivariate-Based Multi-Label Classification Approach. *Energies* **2022**, *15*, 5312. [CrossRef]
3. Mohamed, N.; Salama, M.M.A. Data Mining-Based Cyber-Physical Attack Detection Tool for Attack-Resilient Adaptive Protective Relays. *Energies* **2022**, *15*, 4328. [CrossRef]
4. Cyman, J.; Raczek, J. Application of Doubly Connected Dominating Sets to Safe Rectangular Smart Grids. *Energies* **2022**, *15*, 2969. [CrossRef]
5. Habbak, H.; Mahmoud, M.; Metwally, K.; Fouda, M.M.; Ibrahem, M.I. Load Forecasting Techniques and Their Applications in Smart Grids. *Energies* **2023**, *16*, 1480. [CrossRef]