energies

MDPI

Editorial

Cybersecurity in Smart Grids

Taha Selim Ustun

Fukushima Renewable Energy Institute, AIST (FREA), Koriyama 963-0298, Japan; selim.ustun@aist.go.jp

check for updates

Citation: Ustun, T.S. Cybersecurity in Smart Grids. *Energies* **2022**, *15*, 5458. https://doi.org/10.3390/en15155458

Received: 20 July 2022
Accepted: 27 July 2022
Published: 28 July 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

The increasing use of communication in power-system operation and control is a double-edged sword. On the one hand, it enables the use of power-system equipment in a more efficient manner. An extensive use of communication also makes it possible to implement advanced optimization and control techniques, rendering power systems more stable and reliable. On the other hand, this increased connectivity creates unprecedented cybersecurity vulnerabilities in power systems [1]. If left unchecked, these vulnerabilities can be manipulated to manipulate the electricity market, modify smartmeter readings, disrupt power generation as well as power delivery [2]. In the worst case scenario, these can result in power outages or blackouts.

In an effort to counter these negative aspects of using communication in power systems, researchers recently focused on implementing cybersecurity in smart grids. Smart grids inherently have more measurements taken and transmitted to control centers, and sensitive control signals are sent more frequently. All these steps need to be secured against such attacks by mitigating their respective vulnerabilities.

This book includes chapters that present works focusing on different aspects of smart grid cybersecurity [3–13].

2. Review of Contributions

Researchers in [3] presented a Virtual Power Plant (VPP) management approach based on IEC 61850 standard. They have further incorporated an eXtensible Message Presence Protocol (XMPP). The presented solution provides a standard and secure communication architecture for VPPs.

Another secure communication modeling, this time for a microgrid, is studied in [4]. It models communications between different microgrid components for secure and reliable microgrid operations. Real message exchanges designed as per IEC 62351 in the lab are captured and presented.

IEC 62351 is cybersecurity standard that is designed to complement popular IEC 61850 communication standards to mitigate its vulnerabilities. Due to its recent publication, IEC 62351 requires investigation and development work, as in [5]. The researchers developed a software package, S-GoSV (Secure GOOSE and SV). It uses different digital signatures recommended by this standard. The results show that these do not conform with the strict timing requirements of IEC 61850. The authors have tried different algorithms and proposed amendments in the IEC 62351 standard.

It is important to detect attacks or abnormalities in smart grids. A convolutional neural network (CNN) and a long short-term memory (LSTM) architecture is utilized in [6] for electricity theft detection.

Researchers in [7] developed a new metering scheme that is both secure and anonymous. This is required to counter the privacy concerns associated with high-resolution data collected by smart meters. The new scheme is based on the technique of direct anonymous attestation and identity-based signatures.

Some demand-side response programs utilize Short Messaging Services (SMSs) for control messages. However, SMiShing attacks, i.e., SMS phishing attacks, can take advantage of these systems and disrupt operations, as shown in [8]. Some attacks have been modeled and simulated on the European Low Voltage System designed by IEEE. Simulation results show that such attacks my lead to blackouts on the European continent.

In addition to smart-meter security, power-system equipment security is very important. Work in [9] develops an approach for detecting cyber attacks based on network traffic self-similarity.

Generic Object-Oriented Substation Event (GOOSE) messages of IEC 61850 standard are utilized in power-system protection, and their reliable transmission is very important for smart grids. A well-known method to disrupt this is by using Denial of Service (DoS) attacks. In order to mitigate this, an Anomaly Detection (AD) method to detect DoS attacks against GOOSE network communication is developed in [10].

False Data Injection (FDI) attacks are recognized to be large threat with respect to smart-grid operations. Work in [11] provides a thorough review on FDI attacks, their impact on the different layers of smart grid operation and different techniques that can be utilized to mitigate them.

Recognizing the importance of mitigating FDI attacks, researchers in [12] developed a novel two-tier secure smart-grid architecture to secure power-system measurements in smart grids. Elliptic curve cryptography is utilized for security.

In addition to theoretical work, cybersecurity studies require projects with lab implementation and hardware demonstrations [13]. The impact of cyberattacks on grid-connected storage devices and their ramifications on the overall power system is investigated. Real-lab results are presented to better understand these impacts and further design security systems.

3. Conclusions

Cybersecurity in smart grids is a relatively new but very fertile research area. As observed from the diversity of the contributions, there are different aspects of security that needs to be studied and investigated. Since it is a real-time system, smart grids have more strict timing and performance requirements. Attacks on these systems can have multi-layer impacts involving economic, physical and social factors. Therefore, this exciting research field is attracting constant attention from researchers with diverse backgrounds.

Funding: This research received no external funding.

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

References

1. Ustun, T.S. Cybersecurity Vulnerabilities of Smart Inverters and Their Impacts on Power System Operation. In Proceedings of the 2019 International Conference on Power Electronics, Control and Automation (ICPECA), New Delhi, India, 16–17 November 2019; pp. 1–4.
2. Ustun, T.S.; Hussain, S.M.S.; Ulutas, A.; Onen, A.; Roomi, M.M.; Mashima, D. Machine Learning-Based Intrusion Detection for Achieving Cybersecurity in Smart Grids Using IEC 61850 GOOSE Messages. *Symmetry* **2021**, *13*, 826. [CrossRef]
3. Nadeem, F.; Aftab, M.; Hussain, S.; Ali, I.; Tiwari, P.; Goswami, A.; Ustun, T. Virtual Power Plant Management in Smart Grids with XMPP Based IEC 61850 Communication. *Energies* **2019**, *12*, 2398. Available online: https://www.mdpi.com/1996-1073/12/12/2398 (accessed on 19 July 2022). [CrossRef]
4. Ustun, T.; Hussain, S. Secure Communication Modeling for Microgrid Energy Management System: Development and Application. *Energies* **2020**, *13*, 68. Available online: https://www.mdpi.com/1996-1073/13/1/68 (accessed on 19 July 2022). [CrossRef]
5. Farooq, S.; Hussain, S.; Ustun, T. S-GoSV: Framework for Generating Secure IEC 61850 GOOSE and Sample Value Messages. *Energies* **2019**, *12*, 2536. Available online: https://www.mdpi.com/1996-1073/12/13/2536 (accessed on 19 July 2022). [CrossRef]
6. Hasan, M.; Toma, R.; Nahid, A.; Islam, M.; Kim, J. Electricity Theft Detection in Smart Grid Systems: A CNN-LSTM Based Approach. *Energies* **2019**, *12*, 3310. Available online: https://www.mdpi.com/1996-1073/12/17/3310 (accessed on 19 July 2022). [CrossRef]
7. Xie, S.; Zhang, F.; Lin, H.; Tian, Y. A New Secure and Anonymous Metering Scheme for Smart Grid Communications. *Energies* **2019**, *12*, 4751. Available online: https://www.mdpi.com/1996-1073/12/24/4751 (accessed on 19 July 2022). [CrossRef]
8. Ustundag Soykan, E.; Bagriyanik, M. The Effect of SMiShing Attack on Security of Demand Response Programs. *Energies* **2020**, *13*, 4542. Available online: https://www.mdpi.com/1996-1073/13/17/4542 (accessed on 19 July 2022). [CrossRef]
9. Kotenko, I.; Saenko, I.; Lauta, O.; Kribel, A. An Approach to Detecting Cyber Attacks against Smart Power Grids Based on the Analysis of Network Traffic Self-Similarity. *Energies* **2020**, *13*, 5031. Available online: https://www.mdpi.com/1996-1073/13/19/5031 (accessed on 19 July 2022). [CrossRef]

10. Elbez, G.; Keller, H.; Bohara, A.; Nahrstedt, K.; Hagenmeyer, V. Detection of DoS Attacks Using ARFIMA Modeling of GOOSE Communication in IEC 61850 Substations. *Energies* **2020**, *13*, 5176. Available online: https://www.mdpi.com/1996-1073/13/19/5176 (accessed on 19 July 2022). [CrossRef]
11. Unsal, D.; Ustun, T.; Hussain, S.; Onen, A. Enhancing Cybersecurity in Smart Grids: False Data Injection and Its Mitigation. *Energies* **2021**, *14*, 2657. Available online: https://www.mdpi.com/1996-1073/14/9/2657 (accessed on 19 July 2022). [CrossRef]
12. Aziz, I.; Jin, H.; Abdulqadder, I.; Alturfi, S.; Alobaidi, W.; Flaih, F. T2S2G: A Novel Two-Tier Secure Smart Grid Architecture to Protect Network Measurements. *Energies* **2019**, *12*, 2555. Available online: https://www.mdpi.com/1996-1073/12/13/2555 (accessed on 19 July 2022). [CrossRef]
13. Culler, M.; Burroughs, H. Cybersecurity Considerations for Grid-Connected Batteries with Hardware Demonstrations. *Energies* **2021**, *14*, 3067. Available online: https://www.mdpi.com/1996-1073/14/11/3067 (accessed on 19 July 2022). [CrossRef]