https://doi.org/10.2352/EI.2025.37.3.MOBMU-315

A REVIEW OF CYBER SECURITY AND CHALLENGES ASSOCIATED WITH MICROGRID SYSTEMS

Saiful Islam[1]***, Klaus Schwarz***[1]***, Kendrick Bollens***[1]***, Michael Hartmann***[1]***, Reiner Creutzburg***[1,2]

[1] SRH University, School of Technology and Architecture, Sonnenallee 221, D-12509 Berlin, Germany
[2] Technische Hochschule Brandenburg, Department of Informatics and Media, Magdeburger Str. 50, D-14770 Brandenburg, Germany
Email: saiful.islam@srh.de, klaus.schwarz@srh.de, kendrick.bollens@srh.de, michael.hartmann@srh.de, reiner.creutzburg@srh.de, creutzburg@th-brandenburg.de

Abstract

Microgrid systems encounter various challenges, including critical issues such as load scheduling and the generation of large amounts of data that need to be monitored to stabilize the system during operation. It is essential to ensure the real-time collection and protection of data throughout the process. In this context, infrastructure such as cloud computing and data security plays a crucial role in addressing these challenges. Data generated from a microgrid includes different attributes such as meteorological information, energy production data, and distributed energy resources data, which help monitor the balance between supply and demand. This data also plays a crucial role in energy forecasting, predictive maintenance, and analyzing the critical performance of grid-connected or standalone microgrid systems. The paper discusses the significance of the data collected from distributed energy resources and provides a critical analysis of current solutions and future perspectives on data sharing in microgrids and their challenges.

Keywords: Microgrid, Cyber security, Data collection, Load Scheduling, Sharing energy.

Introduction

The concept of Microgrid (MG) is well-established in the realm of renewable energy systems (RES). It plays a crucial role in integrating distributed energy resources (DERs). The primary challenge with renewable energy sources lies in their unpredictability due to factors such as irradiation, wind velocity, and temperature. After the system is installed, it's essential to monitor its operation and energy production, identify potential faults, and make necessary adjustments to address any issues. This can be achieved by analyzing the data generated by the system. Modern technologies offer a wide range of technical systems. MG was first introduced in 2001 by Bob Lasseter [49]. Monitoring the data and predicting future production levels are also key considerations.

In theory, MG should be constantly connected to the utility grid, enabling surplus energy from that to be fed into the primary grid and any energy deficit in the system to be supplemented by the utility grid. The main components of MG include DERs, power converters, energy storage, loads, master controllers, intelligent switches, protective devices, communication systems, and control and automation systems. MGs can be categorized into AC microgrids, DC microgrids, and hybrid AC/DC microgrids. Among these, the AC MG is popular due to its plug-and-play approach for all DERs, but it requires additional power conversion devices. Hybrid AC/DC microgrids can be further classified into AC-coupled, DC-coupled, and AC-DC-coupled microgrids. Therefore, an MG can be understood as a decentralized network architecture with locally connected production, transmission, regulation, and utilization that can operate independently or in conjunction with other microgrids or the primary grid [48], [44], [51].

Various energy data analysis techniques are employed in MG systems to monitor their condition and operational stability. The data can be utilized for fault identification, prediction of energy production, optimal system sizing, and more. The collected data can be used to analyze measurable patterns in variable load conditions in an MG as well as for forecasting Direct Normal Irradiance (DNI), Global Horizontal Irradiance (GHI), and the electrical measure (power transmitted by MG).

However, the reliance on digital communication protocols, smart devices, and data-driven control systems has introduced significant cybersecurity vulnerabilities, with False Data Injection Attacks (FDIA) posing a serious threat to energy management system integrity. Researchers are also developing resilient control methods and robust cybersecurity frameworks to protect these vital infrastructures. Concurrently, integrating blockchain and Internet of Things (IoT) technologies transforms energy transactions and metering in microgrids, enhancing security, transparency, and scalability, particularly in peer-to-peer (P2P) trading applications.

The evolution of MGs is further propelled by integrating artificial intelligence (AI), machine learning (ML), big data analytics, and digital twins, which enable real-time monitoring, enhance operational efficiency, and bolster resilience against cyber-attacks. However, vulnerabilities in widely-used communication protocols like IEC61850 must be addressed to safeguard smart grids and electric vehicle (EV) charging stations from cyber threats. Educational programs and testbed environments are being developed to prepare professionals for these challenges to provide hands-on experience with real-world datasets and simulation platforms. As cybersecurity and data privacy concerns grow, ongoing research focuses on optimization strategies, anomaly detection, and privacy-preserving solutions to ensure the resilience and security of modern energy systems. A holistic approach to MG management is essential, integrating advanced technologies with robust cybersecurity measures to secure the future of energy.

Cyber security in Microgrid

In the study referenced as [36], the authors tackle the cybersecurity challenges faced by smart distribution systems, particularly focusing on the detection of FDIA using data from Phasor Measure-

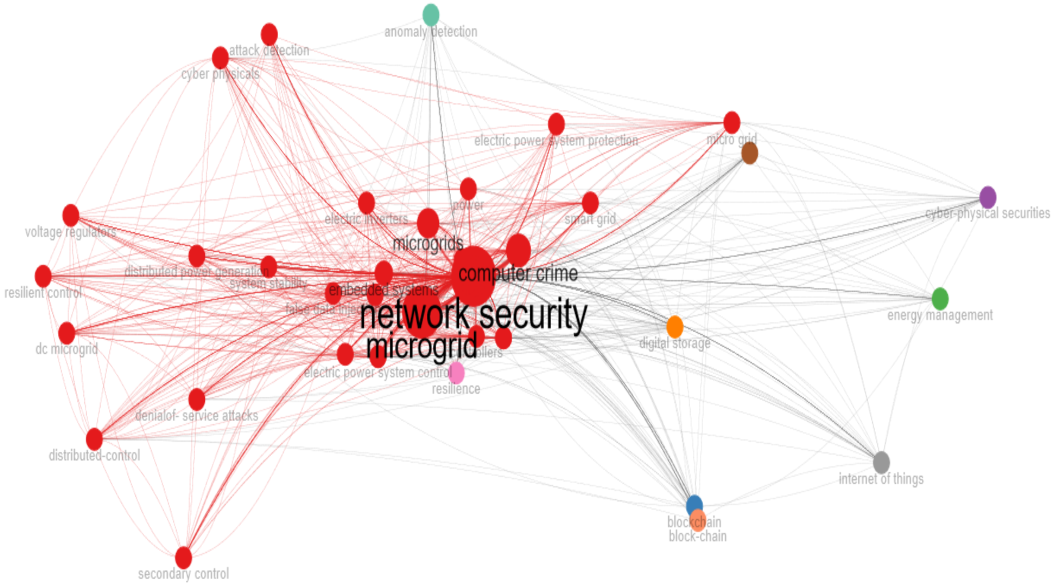

Figure 1: Network visualization of the trend topics related to cyber security in MG systems

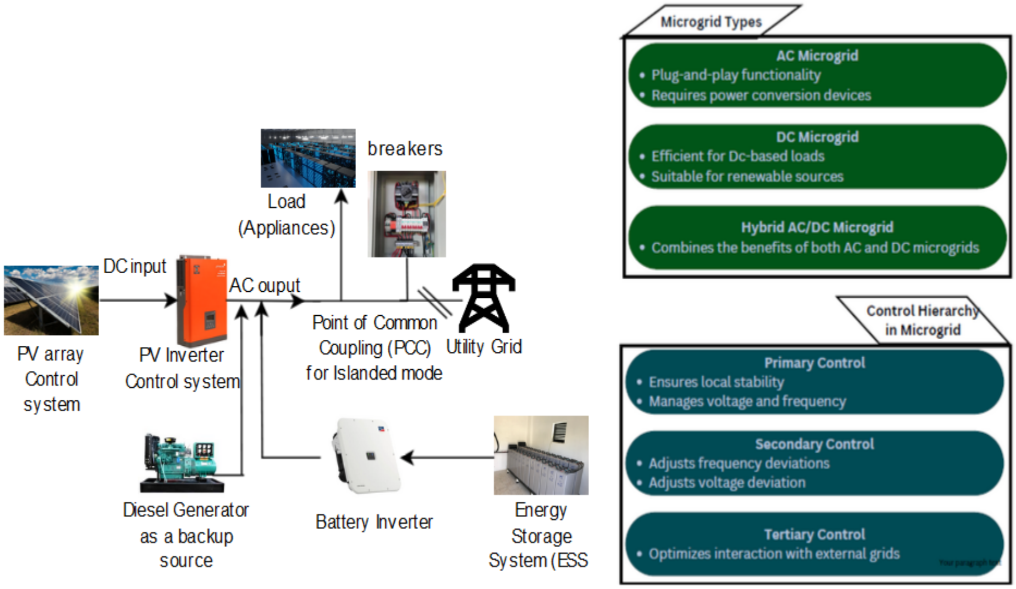

Figure 2: Microgrid Architecture and Control Hierarchy Overview

Trend topics	Frequency	Year (Q1)	Year (Median)	Year (Q3)
electric power system security	8	2017	2018	2020
electric power systems	8	2017	2018	2021
distributed control	15	2018	2019	2020
electric substations	11	2017	2019	2020
voltage control	10	2018	2019	2021
electric power transmission networks	99	2018	2020	2022
security of data	22	2020	2020	2021
control systems	12	2018	2020	2022
distributed energy resources	41	2019	2021	2022
network security	358	2021	2022	2023
microgrid	299	2022	2023	2024
cyber-attacks	144	2022	2023	2024
intelligent systems	8	2021	2024	2024
cost-effectiveness	7	2022	2024	2024

Table 1: Trend Topics and Their Frequency Over Time

ment Units (PMUs). They consolidate existing techniques for detecting FDIAs, placing an emphasis on unsupervised learning methods suitable for managing large, unlabeled data sets. The findings indicate that unsupervised learning methods surpass traditional approaches, offering enhanced accuracy and improved feature extraction. By highlighting critical security vulnerabilities, the authors underscore the potential of unsupervised learning as a promising strategy to strengthen the security of MG.

In [53], vulnerabilities in smart Direct Current (DC) MGs are analyzed, focusing on side-channel and DDoS attacks. The study reveals how attackers exploit packet generation behaviors and suggest countermeasures like traffic camouflage and rootkit traps to enhance security. In [45], a framework for analyzing resiliency in critical systems, including the Miramar military microgrid, is presented. Utilizing a co-simulation platform, it evaluates resiliency under the IEEE standard and stresses the need for situational awareness and proactive measures against cyber threats.

The study mentioned in [42] focuses on cybersecurity in grid-tied power electronic converters, particularly voltage source converters (VSCs), which are essential for stable power grid operations. The research identifies vulnerabilities within the control and communication layers of VSCs that could be exploited, potentially leading to operational failures. By utilizing both theoretical analysis and simulations, the authors propose robust control techniques, such as watermarking and model verification, to enhance resilience against cyberattacks targeting VSCs. This research highlights the urgent need for advanced control solutions to secure power electronic converters.

In [40], a deep reinforcement learning method is introduced to enhance cybersecurity in MGs, focusing on rootkit attack detection and mitigation. A Q-learning agent models the MG as a stochastic environment, responding dynamically to cyber threats based on historical data and proving effective even against attackers controlling multiple nodes.

Reference [19] surveys cybersecurity challenges in Active Distribution Networks (ADNs), emphasizing vulnerabilities linked to increasing reliance on information and communication technologies. It discusses key components like Phasor Measurement Units (PMUs) and Advanced Metering Infrastructure (AMI) and calls for better monitoring and intrusion detection to address evolving threats as distributed energy resources become more integrated into the grid.

The study in [23] employs a deep neural network (DNN)-based controller to improve cybersecurity in cyber-physical microgrids, effectively detecting and mitigating covert FDI attacks.

In [41], the HArMoNICS framework creates a digital twin of a Smart Polygeneration Microgrid (SPM) for cybersecurity testing in IoT systems. It uses Docker containers to assess vulnerabilities and ensure GDPR compliance, while identifying security gaps and suggesting solutions like formal verification.

The text discusses key advancements in cybersecurity for MG communications.

Reference [4] introduces a distributed key management protocol that enables secure communication without a central server, enhancing smart meter security and eliminating single points of failure. This adaptable system highlights the need for reliable key management in smart energy operations. In [11], the authors evaluate the IEC 61850 Sampled Measured Values (SMV) protocol to identify security vulnerabilities and propose a bi-layer algorithm that detects spoofed packets using a neural network and statistical indicators. This underscores the need for additional cybersecurity layers in smart grids.

Reference [9] proposes a strategy to counter FDIA on DC MGs, focusing on voltage and current measurements. By employing artificial neural networks, the approach maintains stability and resilience against cyber threats, demonstrating the importance of layered detection mechanisms.

In [14], the authors present a cyber-resilient automatic generation control (AGC) system aimed at safeguarding frequency stability in AC MGs against FDI attacks. By relying on real-time power data instead of frequency measurements, the AGC system remains effective during rapid load changes and fluctuations in renewable energy sources. Additionally, the approach includes a method for detecting cyberattacks that combines dynamic watermarking with observer-based correction, demonstrating its effectiveness in simulations involving dual MGs. This research highlights the potential of AGC to maintain frequency stability and encourages further exploration of its application in larger networks.

Reference [18] discusses a resilient control strategy designed to counter FDIA in DC system, particularly within secondary control systems. The method employs a proportional-integral (PI) controller with an adaptive gain to address false data injected through sensor and communication links, ensuring operational accuracy. Simulation results demonstrate the effectiveness of the PI controller in re-

Table 2: Analysis of the different techniques used to solve MG security-related problems

Year	Problem statement	Mode of operation	Objective of the model	MG modeling	Reference
2023	False data injection attack	Standalone	It proposes a distributed adaptive secondary controller for AC microgrids to achieve the control objective of restoring the rated frequency and voltage when the controllers are affected by FDIA.	voltage source inverter/LC filter/DC-AC power supply	[38]
2022	Data integrity attacks/time-delay attacks	Standalone	A modified model predictive control (MPC) scheme is being proposed for the secondary frequency control of MGs	PV/Wind/FC/ESS/DG	[52]
2023	False data injection attack	AC-DC microgrid	A technique uses traffic signatures to detect Denial of Service (DoS) attacks and a power system anomaly-based approach to identify False Data Injection (FDI) attacks.	SCADA system/PLCs/Modbus RS485	[30]
2021	Anamoly detection	Standalone/Grid-connected	A MATLAB-based simulation for detecting cyber attacks in AC microgrids/Active power with respect to frequency changes/reactive power with respect to voltage	AC MGs	[1]
2022	MG data flows and data transactions with cybersecurity controls	Standalone/Grid-connected	Introduced the concept of transactive energy management for networked microgrids using blockchain technology as a cybersecurity mesh application	MGs feeders/Grid	[32]
2023	Intelligent control and monitoring methods for MG	Standalone/Grid-connected	Improved energy security of the entire power system of Belarus	PV/Biogas/Grid	[29]
2023	Smart systems applied in energy management for secure operation of the DC MG	Standalone	Proposed a ML based architecture which incorporates cybersecurity considerations, to increase security during the operation of the MG	PV/ESS	[39]
2023	Field-Programmable Gate Arrays (FPGAs) -based embedded systems to enhance the cyber security of MGs	Standalone/Grid-connected	Implemented resistant systems to securely transferring critical data, such as energy billing and local control of the electrical power quality	AC-DC MGs	[33]
2023	Distributed denial-of-service (DDoS) attack	Standalone	Proposed a dynamic model based on epidemiological theory for DDoS attacks in an islanded microgrid scenario containing two types of nodes	PV/ESS/Wind/EV	[27]
2022	FDI attacks on islanded DC microgrids	Standalone	A multiagent deep reinforcement learning (RL)-based algorithm is proposed to automatically discover the vulnerable spots in the conventional index-based cyberattack detection schemes	DC MG	[3]

jecting false data and maintaining stable operations even under attack. This approach significantly contributes to the resilience of MG control systems and holds promise for the future integration of more robust detection mechanisms to strengthen DC systems against cyber threats.

In [10], a coordinated control and energy management model is proposed for multi-microgrid systems that incorporate renewable energy and storage elements. This model ensures stability in terms of voltage, frequency, and inertia, while also detecting FDIA attacks. By employing a centralized data aggregation approach, the system effectively mitigates cyber threats and facilitates load redistribution among unaffected MGs. Simulation results demonstrate the model's effectiveness, and the study recommends further adaptation of this control system for various network configurations to enhance system resilience against cyber threats.

The study in [47] introduces a method for detecting stealth cyber-attacks in DC systems using a Long Short-Term Memory Stacked Autoencoder (LSTM-SAE). This unsupervised model captures temporal correlations in voltage and current data, enhancing detection accuracy and reducing false alarms. Tested in simulations and real-world settings, it demonstrates deep learning's potential to improve microgrid cybersecurity and calls for further research to optimize LSTM-SAE applications.

Reference [6] presents a strategy to combat FDI attacks in cyber-physical MGs. By employing local credibility assessments and adaptive communication, it isolates compromised data while maintaining stability. Simulation results prove its effectiveness in restoring voltage stability and preventing malicious data spread, underscoring the need for further research on resilient control strategies against emerging cyber threats.

The study in [20] introduces a Decentralized Transaction System (DTS) that employs blockchain technology for secure energy trading in MGs. This system enables energy producers and consumers, particularly EV owners, to trade surplus energy confidentially. Utilizing a consortium blockchain on the Ethereum platform, the DTS integrates smart contracts to ensure secure transactions and user privacy. The research highlights the potential of blockchain for scalable energy systems and suggests enhancing it with big data analytics while maintaining privacy.

In [24], the authors present a blockchain-IoT solution that modernizes electricity metering to improve security, transparency, and billing efficiency. By integrating Hyperledger Fabric with IoT devices, they develop a real-time billing system that automates invoices and emails consumers directly. This method decentralizes data management and utilizes cryptographic measures for protection. The study shows that the approach is resilient to cyber threats and enhances consumer trust and operational efficiency, while also calling for further research on blockchain maturity, regulatory issues, and device compatibility.

In [22], a blockchain-based MG system in Saudi Arabia focuses on safe and efficient energy distribution. The study presents a framework for peer-to-peer (P2P) energy trading and renewable energy certificates (RECs). Results indicate improvements in cybersecurity, trust, and efficiency while aiding renewable energy integration. The authors suggest pilot projects to assess the feasibility of blockchain-enabled MGs, emphasizing its potential for modernizing the energy sector.

The paper in [8] examines the role of advanced digital technologies, including Security Orchestration, Automation, and Response (SOAR),ML, AI, and Blockchain, in strengthening MG cybersecurity. Microgrids, essential for renewable energy integration, face security vulnerabilities that these technologies can address. Blockchain, in particular, is highlighted for enabling secure, transparent energy transactions that reduce risks of unauthorized access or fraud. Findings suggest that a combination of SOAR, ML, AI, and Blockchain can form a robust security framework for MGs, promoting reliable, efficient operation while enhancing resilience to cyber threats. This study emphasizes the need for continued research and practical application of these technologies to safeguard future system infrastructures.

In [5], the authors propose a Cloud-Based Intrusion Detection and Prevention System (CB-IDPS) for securing Industrial Control Systems (ICS) using Software Defined Networking (SDN) and Network Function Virtualization (NFV). The system addresses scalability, resilience, and visibility challenges in ICS networks while maintaining low-latency performance. By routing traffic through SDN to a cloud environment for inspection, the CB-IDPS enhances threat detection and prevention. Its three-layer architecture integrates SDN, a virtual private cloud on AWS, and security components like firewalls and intrusion detection systems. Performance evaluations show it meets ICS delay constraints, achieving 31 ms round-trip times and minimal processing delays, ensuring robust, real-time network security.

The study in [46] addresses the need for an advanced security architecture for MG systems, essential for Smartgrid 2.0. It identifies five key vulnerabilities related to wireless networks, service applications, gateways, Intelligent Electronic Devices (IEDs), and Programmable Logic Controllers (PLCs). The authors critique existing standards from NIST and ITU-T for failing to tackle these issues. They propose a security architecture incorporating cryptography and access control to enhance system integrity and stress the importance of a comprehensive security strategy for MG development.

In [17], the authors introduce BlockDeepNet, a blockchain-based deep reinforcement learning framework designed to bolster the resilience of smart power systems against cyberattacks. This decentralized approach detects and mitigates threats to smart grids using a Block Deep Q-network architecture and Benford's Law for anomaly detection.

Consisting of five layers—physical, data, blockchain, decentralized deep reinforcement learning, and application—BlockDeepNet enables comprehensive responses to cyber threats. Results show significant improvements in smart grid reliability, with resilience indices of 2.36 for communication failures, 0.91 for replay attacks, and 1.34 for false data injections. The framework effectively addresses various types of attacks, allowing for swift recovery with minimal disruption, highlighting the importance of decentralized strategies for cybersecurity in critical infrastructures.

The study in [2] presents a new deep learning methodology aimed at improving the cyber resilience of DC shipboard microgrids by integrating hybrid signal processing techniques with a focus on detecting FDIAs. The authors utilize Wavelet Transform (WT) and Singular Value Decomposition (SVD) in conjunction with a one-dimensional convolutional neural network (1D-CNN) to enhance the detection capabilities within DC Smart Microgrids (SMGs). The proposed method leverages WT for effective feature extraction from signal fluctuations and SVD for dimensionality reduction, ultimately feeding these features into the 1D-CNN for high-accuracy attack detection. The findings indicate that this integrated approach achieves an impressive detection accuracy of 95.75%, outperforming existing techniques and demonstrating robustness across varying data injection scenarios. The notably low validation loss of 0.104% further supports the effectiveness of the proposed methodology. Overall, this research significantly contributes to advancing the security of DC SMGs, highlighting future avenues for refining detection techniques and assessing their applicability in real-world operational contexts.

Reference [15] reviews digital transformation in microgrids, focusing on design, operation, optimization, and cybersecurity challenges. It highlights MGs as secure, sustainable energy solutions for urban and rural areas, emphasizing technologies like IoT, big data, blockchain, and AI. The paper points out major barriers to digitalization, particularly the need for robust cybersecurity to address emerging threats. Recommendations include encryption, access control, and personnel training. Overall, it emphasizes the importance of innovative cybersecurity strategies to maximize the benefits of digital technologies in energy management.

In the research paper by [28], the authors introduce a distributed scheduling approach for Integrated MicroGrids (IMG) that uses battery storage and renewable energy sources while ensuring data privacy through the Paillier cryptosystem. The objective is to minimize operational costs across interconnected MGs. Using the Alternating Direction Method of Multipliers (ADMM) for optimization, the method demonstrates significant reductions in operational costs, fuel consumption, and battery degradation, converging within 40 to 50 iterations per time slot. The findings show that the approach achieves results comparable to centralized solutions while effectively preserving privacy in distributed energy resource management.

The paper by [37] introduces a resilient control strategy for DC MGs to combat FDI attacks on secondary control systems. It develops a PI controller with adjustable gain to detect and mitigate false data from sensor and communication link attacks. The methodology ensures data integrity during threats, and simulation results confirm its effectiveness in maintaining system performance. This research advances the resilience of DC microgrids against cyber threats and sets the stage for future robust control studies.

The paper by [43] reviews Demand-Side Management (DSM) methodologies in modern power grids, emphasizing its role in energy transition and optimization. The authors stress the importance of robust communication networks and advanced machine learning, while suggesting future research should address regulatory, privacy, and cybersecurity challenges.

In the review paper by [13], the authors examine the cyber resilience of power electronics-enabled power systems, focusing on vulnerabilities across the generation, transmission, and storage domains. The study introduces a cybersecurity framework specifically designed for closed-loop controllers, highlighting the importance of proactive measures to enhance system security. The findings reveal significant risks posed by cyber-attacks on power electronics devices and underscore the need for robust cybersecurity frameworks. This comprehensive analysis assists stakeholders in developing strategies to strengthen the resilience of power systems against emerging cyber threats.

The paper by [21] reviews advancements and the control challenges associated with microgrid, smart grid, and virtual power plant (VPP) systems, highlighting their importance in achieving energy sustainability. The research points out the necessity for sophisticated control algorithms to effectively integrate renewable energy resources. Through a detailed analysis, the findings reveal that advanced strategies, such as predictive modeling and stochastic methods, are crucial for optimizing these systems. The study concludes that ongoing development and implementation of these advanced control strategies are essential for ensuring a reliable energy supply and addressing future energy management challenges.

In the research paper by [7], a secure stochastic energy management scheme for hybrid AC-DC microgrids (HMGs) is presented. This scheme integrates renewable energy sources, plug-in hybrid electric vehicles (PHEVs), and energy storage devices. The study implements a deep learning-based intrusion detection system (IDS) to address false data injection attacks on metering infrastructures. The findings indicate that the proposed smart charging strategy significantly reduces operational costs, particularly through effective energy storage management. The study concludes that combining IDS with optimal scheduling strategies enhances the reliability and security of smart grids. It also recommends off-peak charging for PHEVs to further minimize costs.

The paper by [35] explores the transformative impact of the Internet of Things (IoT) on human society, particularly its potential to revolutionize energy usage and support the development of MGs. The research discusses how interconnected devices can enhance energy efficiency and contribute to a more resilient energy infrastructure. While the IoT offers significant opportunities for improving energy systems, the study highlights the necessity for regulatory changes to facilitate its integration. The authors recommend that future research should focus on identifying specific policies that will promote the growth of IoT in the energy sector.

In the research paper by [50], the authors explore the integration of power system simulators with communication network emulators to enhance the analysis of cyber-physical security in smart grids. The main objective is to improve the understanding of vulnerabilities and defense mechanisms in interconnected energy and communication systems. The study discusses various interfacing methods, including network emulation and hardware-in-the-loop integration, with a focus on real-time simulation protocols such as TCP/IP to analyze potential cyber-attacks within a secure testbed environment. Additionally, the paper highlights a proposed mitigation strategy aimed at preventing under-frequency load shedding during cyber-attacks. This research emphasizes the need for a robust framework for cyber-physical security analysis, asserting that integrated simulations of power and communication systems allow for more effective identification of vulnerabilities and testing of countermeasures.

The research paper by [34] introduces the Software-defined Intelligent Grid Research Integration and Development Platform (SI-GRID), now in its second generation with a shadow network for enhanced monitoring. SI-GRID provides a flexible testbed for verifying control schemes, protection measures, and cybersecurity in MGs. Key findings indicate it will enable benchmarking of MG controls and assess cyber-attack impacts. The platform aims to create a dataset of attack scenarios to evaluate countermeasures, facilitating the transition of MG science from labs to real-world applications.

The research by [16] explores Wireless Sensor Networks (WSNs) in smart micro-grid systems, particularly their cybersecurity benefits. A survey of 70 participants reveals a positive view of WSNs, with over half acknowledging their cybersecurity potential. However, concerns about their effectiveness in error reduction highlight the need for further research.

The paper by [25] presents E+BOX, a control solution designed to tackle technical and regulatory challenges in critical infrastructure. It focuses on cost efficiency, cybersecurity, and worker safety, employing real-time simulation and hardware-in-the-loop (HIL) testing. The findings highlight E+BOX's effectiveness in optimizing distributed energy resources and suggest further exploration of its capabilities in different regulatory environments.

The paper by [12] examines the vulnerabilities of the IEC61850

Table 3: Findings and Discussion on Cybersecurity Challenges in Microgrid Systems

Cybersecurity Challenge	Proposed Solution and Discussion
False Data Injection Attacks (FDIAs)	Proportional-Integral (PI) controllers with adaptive gain, dynamic watermarking, and deep learning techniques like Long Short-Term Memory Stacked Autoencoder (LSTM-SAE) improve detection and maintain operational stability. Hybrid techniques like Wavelet Transform and 1D-CNN achieve detection accuracy exceeding 95%.
Distributed Denial of Service (DDoS) and Side-Channel Attacks	Mitigated with traffic camouflage, rootkit traps, and epidemiological models to secure communication and data flow.
Vulnerabilities in Communication Standards (e.g., IEC61850)	Addressed through distributed key management protocols and bi-layer neural network algorithms, ensuring secure encryption and analyzing communication patterns.
Data Integrity and Secure Transactions	Blockchain-based microgrid systems ensure secure, transparent transactions and robust data management.
Real-Time Threat Detection	Cloud-Based Intrusion Detection and Prevention Systems (CB-IDPS) provide scalable real-time threat detection and response.
Cyber-Physical System Integration	Digital twins and co-simulation platforms enable real-time monitoring, testing, and validation, improving the alignment between physical operations and cybersecurity requirements.
General Resilience to Cyber Threats	Combining advanced technologies like artificial intelligence, blockchain, and digital twins enhances system resilience and adaptability against evolving threats.

communication protocol in smart grids using Hardware-In-the-Loop (HIL) real-time testbeds. It evaluates the protocol's effectiveness in microgrid protection, focusing on communication delays and cyber attack resilience. Testing various IEC61850 protocols, including GOOSE and Sampled Values, reveals that while the protocol effectively isolates faults, it is vulnerable to man-in-the-middle attacks. The findings emphasize the need for further cybersecurity research in smart grid communications.

In a research paper by [26], the authors introduce a course called ”Introduction to Smart Grids” in the Electrical Engineering Technology program at Old Dominion University. The course focuses on smart grid technologies, including communication and distributed energy resources. The study concludes that integrating smart grid concepts into engineering curricula is vital for preparing future engineers and addressing workforce skill gaps.

The research paper by [31] presents a Massive Open Online Course (MOOC) on Electrical Microgrids, emphasizing Cybersecurity, State Estimation, and Optimization. Designed for students and professionals, the course uses real datasets from the Dominican Republic and MATLAB simulations to enhance skills in operating electrical microgrids. By incorporating machine learning and artificial intelligence, it provides hands-on experience for developing critical thinking in modern energy systems. Preliminary results indicate success in training machine learning classifiers to detect cyber-attacks, highlighting the MOOC's potential to enhance system efficiency and security. Future research could expand the curriculum to address emerging cybersecurity challenges.

Findings and Discussion

MG systems are essential to modern energy infrastructures, but they face significant cybersecurity challenges that require innovative and advanced solutions. The findings highlight various threats, such as FDIAs, Distributed Denial of Service (DDoS) attacks, and vulnerabilities in communication protocols, alongside their corresponding mitigation techniques. Table 3 summarizes the key cybersecurity challenges in microgrid systems and the proposed solutions to address them effectively.

Conclusion

In conclusion, microgrids represent a pivotal advancement in modern energy systems; however, their dependence on digital communication and control systems makes them susceptible to a wide array of cybersecurity threats. Addressing critical challenges such as FDIA and DDoS attacks necessitates advanced mitigation techniques, including deep learning, dynamic watermarking, and blockchain integration. For less severe issues, such as data integrity concerns and vulnerabilities in communication protocols, robust solutions like distributed key management and secure communication frameworks are essential.

This study underscores the importance of integrating cutting-edge technologies such as blockchain, artificial intelligence, and digital twins into microgrid systems to enhance their resilience. To achieve a secure and sustainable energy infrastructure, future research should prioritize scalable and adaptable solutions that can address the ever-evolving landscape of cyberthreats.

Acknowledgments

The European Union partially supported this work through ERASMUS MUNDUS, Project CyberMACS (Project No. 101082683) (https://cybermacs.eu).

Author Biography

M. Eng. Saiful Islam – Research Associate at SRH University of Applied Sciences HD. Department of School of Technology and Architecture (TEAC). Researcher in the field of Renewable Energy and Optimization techniques. He is currently a PhD student at Otto-

von-Guericke-University Magdeburg, Germany.

Klaus Schwarz received his B.Sc. and M.Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2017 and 2020, respectively. He is currently a Ph.D. student at the University of Granada, Spain, and is a lecturer at the SRH University in Berlin. His research interests include AI, IoT and smart home security, OSINT, mechatronics, additive manufacturing, embedded systems, artificial intelligence, and cloud security. As a faculty member at SRH Berlin University of Applied Sciences, he has developed a graduate program in Applied Mechatronic Systems focusing on Embedded Systems.

Prof. Dr. Michael Hartmann – Academic Director of Department of SRH School of Technology and Architecture (TEAC); Head of the Study Programs: Engineering and International Business; Engineering and Sustainable Technology Management.

Prof. Dr. Reiner Creutzburg - Retired Professor for Applied Computer Science at the Technische Hochschule Brandenburg in Brandenburg, Germany. Since 2019 he is a Professor of IT Security at the SRH Berlin University of Applied Sciences, Berlin School of Technology. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Devices (MOBMU) Conference at the Electronic Imaging conferences since 2005. In 2019, he was elected a member of the Leibniz Society of Sciences to Berlin e.V. His research interest is focused on Cybersecurity, Digital Forensics, Open-Source Intelligence (OSINT), Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications

References

[1] Qobad Shafiee Abbas Ahmadi. An estimation based detection method for deception cyber attack in ac microgrids. *IEEE 3rd International Conference on Sustainable Energy and Future Electric Transportation (SEFET)*, 2023.

[2] Z. Ali, T. Hussain, and C. L. et al. Su. A new paradigm for adaptive cyber-resilience of dc shipboard microgrids using hybrid signal processing with deep learning method. *IEEE Transactions on Transportation Electrification*, 2024.

[3] Farzad Ferdowsi Nenad Mijatovic-Tomislav Dragi˘cevi´c Ali Jafarian Abianeh, Yihao Wan. Vulnerability identification and remediation of fdi attacks in islanded dc microgrids using multiagent reinforcement learning. *IEEE TRANSACTIONS ON POWER ELECTRONICS, VOL. 37, NO. 6*, 2022.

[4] M. I. Baza, M. M. Fouda, A. S. T. Eldien, and H. A. K. Mansour. An efficient distributed approach for key management in microgrids. In *11th International Computer Engineering Conference*, 2016.

[5] J. Brugman, M. Khan, S. Kasera, and M. Parvania. Cloud based intrusion detection and prevention system for industrial control systems using software defined networking. In *Resilience Week*, 2019.

[6] G. Cao, R. Jia, and J. Dang. Distributed resilient mitigation strategy for false data injection attack in cyber-physical microgrids. *Frontiers in Energy Research*, 2022.

[7] T. Cheng, X. Zhu, and X. et al. Gu. Stochastic energy management and scheduling of microgrids in correlated environment: A deep learning-oriented approach. *Sustainable Cities and Society*, 2021.

[8] S. de Dutta and R. Prasad. Cybersecurity for microgrid. In *International Symposium on Wireless Personal Multimedia Communications*, 2020.

[9] A. H. EL-Ebiary, M. Mokhtar, A. M. Mansour, and F. H. et al. Awad. Distributed mitigation layers for voltages and currents cyber-attacks on dc microgrids interfacing converters. *Energies*, 2022.

[10] H. Faraji and R. Hemmati. Coordinated control and energy management combined with cyberattack identification in multi-microgrid integrated with hybrid renewable-storage. *IET Smart Grid*, 2024.

[11] M. el Hariri, E. Harmon, T. Youssef, and M. et al. Saleh. The iec 61850 sampled measured values protocol: Analysis, threat identification, and feasibility of using nn forecasters to detect spoofed packets. *Energies*, 2019.

[12] M. Hemmati, H. Palahalli, G. S. Gajani, and G. Gruosso. Impact and vulnerability analysis of iec61850 in smartgrids using multiple hil real-time testbeds. *IEEE Access*, n.d.

[13] J. Hou, C. Hu, S. Lei, and Y. Hou. Cyber resilience of power electronics-enabled power systems: A review. *Renewable and Sustainable Energy Reviews*, 2024.

[14] T. Huang, D. Wu, and M. Ilic. Cyber-resilient automatic generation control for systems of ac microgrids. *arXiv preprint*, 2022.

[15] E. Irmak, E. Kabalci, and Y. Kabalci. Digital transformation of microgrids: A review of design, operation, optimization, and cybersecurity. *Energies*, 2023.

[16] B. Jain, S. Sirdeshpande, and M. S. et al. Gowtham. Exploratory data analysis based on microgrids generation for control communication and monitoring via wireless sensor network. In *2nd International Conference on Advance Computing and Innovative Technologies in Engineering*, 2022.

[17] P. R. Jeyaraj, E. Rajan Samuel Nadar, and L. Mihet-Popa. Deep-block network for cyberattack mitigation and assessment in smart grid power system with resilience indices. *Electric Power Components and Systems*, 2023.

[18] A. Karimi, A. Ahmadi, Z. Shahbazi, Q. Shafiee, and H. Bevrani. A resilient control method against false data injection attack in dc microgrids. In *7th International Conference on Control, Instrumentation and Automation*, 2021.

[19] M. Khalaf, A. Ayad, H. Kamal Tushar, M. Kassouf, and D. Kundur. A survey on cyber-physical security of active distribution networks in smart grids. *IEEE Access*, n.d.

[20] M. Khan, J. Imtiaz, and M. Najam Ul Islam. A blockchain based secure decentralized transaction system for energy trading in microgrids. *IEEE Access*, n.d.

[21] R. Khan, N. Islam, and S. K. et al. Das. Energy sustainability-survey on technology and control of microgrid, smart grid and virtual power plant. *IEEE Access*, 2021.

[22] M. M. Khubrani and S. Alam. Blockchain-based microgrid for safe and reliable power generation and distribution: A case study of saudi arabia. *Energies*, 2023.

[23] S. S. Koduru, V. S. P. Machina, and S. Madichetty. Cyber attacks in cyber-physical microgrid systems: A comprehensive review. *Energies*, 2023.

[24] K. Koštál, M. N. Bahar, S. Numyalai, and M. Ries. Beyond integration: Advancing electricity metering with secure and transparent blockchain-iot solutions. In *47th International Conference on Telecommunications and Signal Processing*, 2024.

[25] R. A. S. Kraemer, D. P. Dias, and A. C. et al. da Silva. Cost and cybersecurity challenges in the commissioning of microgrids in critical infrastructure: Coge case study. *Energies*, 2022.

[26] M. Kuzlu, O. Popescu, and V. M. Jovanovic. Development

of a smart grid course in an electrical engineering technology program, 2021.

[27] Dongfeng Fang Hui Zeng Lei Xiong, Qichao Xu. Modeling and analysis for the propagation of ddos attacks in microgrid system. *IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress*, 2023.

[28] N. Liu, C. Wang, M. Cheng, and J. Wang. A privacy-preserving distributed optimal scheduling for interconnected microgrids. *Energies*, 2016.

[29] Tatsiana Zoryna Liudmila Gurina. Distributed energy: Benefits of use and threats to cybersecurity. *International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, 2023.

[30] Peddoju Sateesh Kumar Ganesh Balu Kumbhar Ram Singh-Vivek Thakur Manoj Tripathy, Rajdeep Niyogi. A novel approach for detection of cyber attacks in microgrid scada system. *IEEE 3rd International Conference on Sustainable Energy and Future Electric Transportation (SEFET)*, 2023.

[31] R. Maria Melendez-Norona. Design of a massively open online course on electrical microgrids with real datasets, n.d.

[32] Andy Sugiarto Alex Valderrama Niroj Gurung Honghao Zheng-Aleksandar Vukojevic Mehrdad Sheikholeslami, Kip Gering. Data security in networked microgrids for transacting energy. *IEEE PES Transactive Energy Systems Conference (TESC)*, 2022.

[33] Radu Florin Porumb Bogdan-Adrian Enache George-Calin Seritan Mihai Alexandru Pisla, Marilena Stanculescu. Microgrid cyber security enhancement considerations mihai. *THE 13th INTERNATIONAL SYMPOSIUM ON ADVANCED TOPICS IN ELECTRICAL ENGINEERING*, 2023.

[34] B. Ollis, P. Irminger, and M. et al. Buckner. Software-defined intelligent grid research integration and development platform. In *IEEE Power and Energy Society Innovative Smart Grid Technologies Conference*, 2016.

[35] G. Parise, L. Parise, and M. Parise. Evolution of human society and of things assisted by iot. In *International Symposium on Technology and Society*, 2018.

[36] S. J. Pinto, P. Siano, and M. Parente. Review of cybersecurity analysis in smart distribution systems and future directions for using unsupervised learning methods for cyber detection. *Energies*, 16(4), 2023.

[37] N. Priyadharshini, S. Gomathy, and M. Sabarimuthu. A review on microgrid architecture, cyber security threats and standards. In *Materials Today: Proceedings*, 2021.

[38] Jian Li Qingyu Su, Haoyu Fan. Distributed adaptive secondary control of ac microgrid under false data injection attack. *Electric Power Systems Research, Volume 223*, 2023.

[39] C. Feregrino-Uribe R. Campos-Sanchez, L. Hernandez-Martinez. Iot architecture and security mecanisms for an energy management system in a smart microgrid. *20th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE)*, 2023.

[40] S. Rath, S. Sengupta, and T. Das. Improvise, adapt, overcome: Dynamic resiliency against unknown attack vectors in microgrid cybersecurity games. *arXiv preprint*, n.d.

[41] G. Roascio, G. Costa, E. Baccelli, and L. et al. Malina. Harmonics: High-assurance microgrid network infrastructure case study. *IEEE Access*, n.d.

[42] S. Sahoo, T. Dragicevic, and F. Blaabjerg. Cyber security in control of grid-tied power electronic converters - challenges and vulnerabilities. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2021.

[43] D. Said. A survey on information communication technologies in modern demand-side management for smart grids: Challenges, solutions, and opportunities. *IEEE Engineering Management Review*, 2023.

[44] Goran Rafajlovski Michael Hartmann Saiful Islam, Sanket Shrikant Patil and Reiner Creutzburg. Technical design and operational control of a decentralized microgrid in rural area. *in Proc. IS&T Int'l. Symp. on Electronic Imaging: Mobile Devices and Multimedia: Technologies, Algorithms & Applications*, 2021.

[45] P. S. Sarker, V. Venkataramanan, D. S. Cardenas, A. Srivastava, A. Hahn, and B. Miller. Cyber-physical security and resiliency analysis testbed for critical microgrids with ieee 2030.5. In *8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2020.

[46] J. T. Seo. Towards the advanced security architecture for microgrid systems and applications. *Journal of Supercomputing*, 2016.

[47] A. Takiddin, S. Rath, M. Ismail, and S. Sahoo. Data-driven detection of stealth cyber-attacks in dc microgrids. *IEEE Systems Journal*, 2022.

[48] K. M. Venkatachalam V. Saravanan. Overview of microgrid systems. *International Journal of Advances in Applied Sciences (IJAAS), Vol. 10, No. 4*, 2021.

[49] A. Vasilakis. The evolution of research in microgrids control. *Digital Object Identifier 10.1109/OAJPE.2020.3030348*, 2020.

[50] V. Venkataramanan, P. Wang, and A. et al. Srivastava. Interfacing techniques in testbed for cyber-physical security analysis of the electric power grid. In *Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2017.

[51] A. Yazdani and R. Iravani. Voltage-sourced converters in power systems. *Hoboken, NJ, USA: John Wiley & Sons, Inc*, 2010.

[52] Lingfeng Wang Zhengrong Chen, Zhaoxi Liu. A modified model predictive control method for frequency regulation of microgrids under status feedback attacks and time-delay attacks. *Electrical Power and Energy Systems 137*, 2022.

[53] X. Zhong, L. Yu, R. Brooks, and G. K. Venayagamoorthy. Cyber security in smart dc microgrid operations. In *2015 IEEE 1st International Conference on Direct Current Microgrids*, 2015.

JOIN US AT THE NEXT EI!

Imaging across applications . . . Where industry and academia meet!

• SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •
• INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •

www.electronicimaging.org