Enhancing Power Grid Resilience against Cyber Threats in the Smart Grid Era

[1]Dr. R. Padmavathy, [2] Dr.Sanjeev Kumar Singh, [3]M.Sindhu, [4]L. Hussien Jasim, [5]Archana Saxena, and [6]Dr. Sukhvinder Singh Dari

[*]*New Prince Shri Bhavani college of Engineering and Technology,Anna University*
[†]*Department of Electrical & Electronics Engineering, IES University, Bhopal, MP 462044 India. IES College of Technology, Bhopal, Madhya Pradesh, India 462044*
[‡]*CSE, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai - 127*
[§]*College of technical engineering, The Islamic university, Najaf, Iraq.*
[**]*Department of Management,Uttaranchal Institute of Management, Uttaranchal University, Dehradun, Uttarakhand, India,*
[6]*Associate Professor, Symbiosis Law School Nagpur, Symbiosis International (Deemed University), Pune, India Email: sukhvinder.dari@gmail.com*

Abstract. In the age of smart grids, fortifying power grids against cyber threats has become of utmost importance. This paper reviews endeavours in the realms of defining, measuring, and scrutinising the resilience of smart grids. An exhaustive overview of both qualitative frameworks and quantitative metrics for resilience study is provided, underscoring the ideal characteristics of a resilience metric. The complexities in formulating and crafting such metrics in practical settings are also broached. Another focal point is the hierarchical outage management scheme, crafted to enhance the robustness of smart distribution systems, particularly those encompassing multi-microgrids. This scheme introduces a two-tiered approach: the preliminary stage revolves around resource scheduling via a model predictive control-based algorithm, whilst the subsequent stage centres on coordinating power transfers amongst microgrids. Moreover, the paper probes into the vulnerabilities of smart grids owing to the incorporation of information technology. A thorough exploration of security prerequisites, accounts of severe cyber-attacks, and a strategic methodology to detect and counteract these threats are elucidated. The paper wraps up by spotlighting future research trajectories, especially in forging a comprehensive framework for resilience and addressing challenges tied to multi-modal cyber/physical attacks and big data concerns.

[*] padmavathy.r@newprinceshribhavani.com
[†] research@iesbpl.ac.in
[‡] m.sindhu_cse@psvpec.in
[§] L.hussien.jasim@gmail.com\
[**] dr12archana@gmail.com

1 Introduction

The power grid, a cornerstone of modern infrastructure, ensures the continuous delivery of electricity to both residential and commercial consumers. Its significance is magnified by the ever-evolving demands and fluctuating operating conditions it must navigate. The transition towards a smart grid, propelled by rapid advancements in sensing, computing, and communication, encapsulates a multifaceted evolution. This includes the integration of renewable energy sources, the development of microgrids, and the mitigation of peak demand, among other advancements. These technological strides, combined with active agents that adapt to changing demands and prices, aim to enhance the generation, distribution, and consumption of electricity.

However, the operation of such a sophisticated grid, laden with novel technologies, is not without its challenges. Monitoring and controlling a vast, geographically dispersed cyber-physical system in an unpredictable environment presents both technological and organisational hurdles. Beyond the everyday fluctuations the grid contends with, it must also brace for extreme events, ranging from natural disasters like hurricanes to adversarial human-induced attacks. The aftermath of such events underscores the grid's resilience, or its ability to recover efficiently and swiftly, resuming its normal operations.

The concept of resilience, while paramount in the context of power grids, is not exclusive to them. It has been explored in various domains, from psychology and sociology to ecology and engineering. Each field offers its unique perspective on resilience, whether it's coping with crises, adapting to social and political changes, or recovering from performance deterioration after extreme events. In the realm of smart grids, resilience is multifaceted, encompassing both qualitative frameworks that study the grid's resilience and quantitative metrics that measure it. These metrics are pivotal in assessing grid architectures and enhancing their response to adversities.

Given the global emphasis on power grid resilience, our review seeks to collate and analyse the significant contributions made in this domain. We aim to bridge the three areas highlighted in the abstract: the comprehensive understanding of smart grid resilience, the hierarchical outage management scheme, and the vulnerabilities introduced by the integration of information technology. By doing so, we hope to provide a holistic perspective on the challenges and opportunities that lie ahead in ensuring the resilience of power grids in the smart grid era.

2 Review and discussion

In a study by Das et al. (2020), the challenges and intricacies of analysing the resilience of smart grids were explored [1]. The smart grid, characterized by its geographically distributed system and dynamic behaviour, presents several challenges when it comes to quantifying its response and recovery to adversarial events.

Desirable Properties of Resilience Metrics [4]:

1. Account for spatio-temporal variations in the grid.
2. Be goal-oriented, addressing specific questions at different organizational scales.
3. Incorporate and process system uncertainty while being robust.
4. Be easily calculable/estimable from data.
5. Address multiple modes of adversities that might act on the grid simultaneously.

Table 1. Challenges in Smart Grid Resilience Analysis [5-9]

Challenges	Brief Description
Temporal and Spatial Scale	Difficulty in developing metrics due to the grid's vast geographical spread and interconnected nature.
Organizational Aspect	Different scales of the grid have unique resilience-related concerns.
Technical Issues	Some metrics, like STAIFI, show variances in real-world applications.
Cyber-Layer Introduction	Cyber-layer adds potential security vulnerabilities.
Data Availability	Lack of comprehensive datasets hinders metric acceptance in the industry.

Table 2 below highlights the primary areas where innovation can significantly enhance the resilience of smart grids. Each opportunity points towards a specific challenge or aspect that, when addressed, can lead to a more robust and resilient grid system.

Table 2. Opportunities for Innovation in Smart Grid Resilience [8.9]

Opportunities	Brief Description
Technological Factors	Unattended aspects can lead to holistic frameworks and policies.
Severity & Recovery	Importance of event intensity and recovery extent in resilience.
Multi-modal Attacks & Information	Cyber-layer offers both vulnerabilities and enhanced awareness.
Big Data Challenges	Potential of analytics amidst data granularity and diversity issues.
Interdependence & Heterogeneity	Grid's relation with other infrastructures and varied node importance.

The challenges and opportunities highlighted in the study underscore the multifaceted nature of the smart grid system. While the challenges emphasize the intricacies of ensuring its resilience, especially with the introduction of a cyber-layer and the associated vulnerabilities, the opportunities point towards areas ripe for innovation. Addressing technological gaps, harnessing big data analytics, understanding the interdependence of various infrastructures, and considering the severity of events and their recovery are all pivotal in shaping the future of smart grid resilience.

In tying this to our review article, the findings from Das et al. (2020) offer a comprehensive roadmap. Not only do they shed light on the existing challenges, but they also illuminate

the path forward, highlighting areas where innovation can significantly enhance the resilience of smart grids. The integration of cyber-layers, while introducing new vulnerabilities, also presents a myriad of opportunities for bolstering the grid's resilience. As the energy sector evolves, fostering collaboration between academia and industry and ensuring access to reliable data will be paramount. The insights from this study serve as a foundation for further research and discussions in this domain, emphasizing the need for a holistic approach that melds technical, organizational, and data-driven perspectives.

Another study by Farzin et al. (2016) delves into the enhancement of power system resilience through a hierarchical outage management in multi-microgrids [2]. The primary objective of the study is to propose a hierarchical outage management scheme that bolsters the resilience of a smart distribution system comprising multiple microgrids against unexpected disaster events.The key findings from the study are summarized as follows [10-15]:

- Framework Introduction: After pinpointing the main features and requirements for a resilient outage management scheme, the study introduces a framework that delineates the roles and tasks of different management entities in a multi-microgrid system.

- Optimisation Model: The general optimisation model needed is formulated as a mixed integer linear programming problem. A novel index is introduced to quantify the performance of the proposed method.

- Resilience in Power Systems: Power systems globally have traditionally been designed based on reliability principles. However, recent natural disasters have underscored the need for a shift from a purely reliability-oriented perspective to one that also emphasises resilience.

- Microgrids as a Solution: Microgrids are seen as viable solutions to tackle power system resilience challenges. They can isolate themselves from damaged parts of the grid during disturbances and maintain power supply through optimal resource management.

- Hierarchical Outage Management Scheme: The proposed scheme comprises two hierarchical levels. The microgrid central controllers (MGCCs) operate at the lower level, managing the associated microgrids. The Distribution System Operator (DSO) functions at the upper level, coordinating the microgrids to enhance the reliability and resilience of the entire distribution system.

- Benefits of the Proposed Scheme: The hierarchical outage management scheme allows microgrids to autonomously schedule their resources, reduces the complexity of optimisation for the DSO, and minimises data exchange between the DSO and the microgrids.

Building upon the findings of Farzin et al. (2016), it's evident that the hierarchical outage management scheme in multi-microgrids offers a promising avenue for enhancing power system resilience. In the context of our review article, this study provides a tangible framework that aligns with our exploration of innovative solutions in power system resilience. The shift from a purely reliability-oriented perspective to a resilience-focused approach, as highlighted by Farzin et al., underscores the evolving nature of power systems

management. The emphasis on microgrids as a solution to resilience challenges resonates with our article's theme of exploring decentralised and autonomous systems for improved grid reliability. The proposed hierarchical scheme, with its two-tiered structure, offers a structured approach that can be integrated into broader discussions on power system management, making it a pivotal reference in our review.

Another study by El Mrabet et al. (2018) delves into the cyber-security challenges and vulnerabilities associated with the smart grid [3]. The smart grid, which leverages information technology to deliver energy intelligently, has been exposed to numerous security threats due to the inherent weaknesses of communication technology.The study aimed to provide an overview of the security requirements of the smart grid, describe several severe cyber-attacks, and propose a cyber-security strategy to detect and counter these attacks. Here are the summarized key findings from the study [16-21]:

- The smart grid aims to provide flexibility and reliability by facilitating the integration of new power resources, enabling corrective capabilities during failures, reducing carbon footprint, and minimising energy losses.
- The smart grid comprises several distributed and heterogeneous applications, including Advanced Metering Infrastructure (AMI), Supervisory Control and Data Acquisition (SCADA), and automation substation.
- AMI is responsible for collecting, measuring, and analysing energy, water, and gas usage, allowing two-way communication between the user and the utility.
- SCADA is used to measure, monitor, and control an electrical power grid, especially in large-scale environments.
- The substation, a key element in the power grid network, performs functions like receiving power from generating facilities, regulating distribution, and limiting power surges.
- Different communication protocols are required for the diverse applications in the smart grid. For instance, home appliances use ZigBee and Z-wave protocols, while SCADA applications use protocols like DNP3 and Modbus.
- Modbus, a widely-used protocol in industrial architecture, is vulnerable due to its lack of authentication and encryption features.
- DNP3, another commonly used communication protocol, was initiated as a serial protocol to manage communication between master and slave stations.

The paper concludes by emphasising the need for a comprehensive cyber-security approach that encompasses various detection techniques and countermeasures to protect the entire smart grid system. The authors also discuss challenges and future research directions in the realm of smart grid cyber-security.

This study by El Mrabet et al. (2018) offers valuable insights into the intricacies of smart grid cyber-security. The detailed exploration of vulnerabilities, coupled with the proposed strategies for detection and counteraction, aligns with our review article's focus on understanding and enhancing the resilience of smart grids. The findings from this study further underscore the importance of a holistic approach to cyber-security, emphasising the need for collaboration between academia and industry in developing robust solutions. The highlighted challenges and future directions can serve as a foundation for subsequent research and discussions in our domain.

3 Future Scope of Research

The evolution of smart grids, with their intricate interplay of technology, organisational structures, and cyber-security, presents a dynamic landscape for research. As we delve deeper into the nuances of smart grid resilience, it becomes evident that there are myriad avenues yet to be explored. The following pointers highlight potential areas of research that could shape the future of smart grid systems:

- **Holistic Cyber-Security Protocols:** With the increasing integration of cyber-layers into the smart grid, there's a pressing need to develop comprehensive security protocols that encompass all facets of the grid, from AMI to SCADA systems.
- **Interdependent Infrastructure Analysis:** As smart grids become more intertwined with other critical infrastructures, understanding the cascading effects of failures and developing resilience strategies for such interdependencies will be crucial.
- **Big Data and AI in Resilience Enhancement:** Leveraging big data analytics and artificial intelligence to predict, detect, and counteract vulnerabilities in real-time could revolutionise smart grid resilience.
- **Consumer-Centric Resilience Strategies:** As consumers become more integrated into the smart grid through home automation systems and renewable energy sources, research into strategies that prioritise consumer needs and feedback will be essential.
- **Green Energy Integration:** With the global push towards sustainable energy, understanding the challenges and opportunities presented by the large-scale integration of renewable energy sources into the smart grid will be pivotal.

4 Knowledge Gaps

While the body of research on smart grid resilience is expansive, there remain certain areas where knowledge is either limited or fragmented. Identifying these gaps is not only crucial for a comprehensive understanding of the current landscape but also for directing future research efforts. Here are some prominent knowledge gaps in the realm of smart grid resilience:

- **Real-World Metric Validation:** While numerous resilience metrics have been proposed, there's a dearth of studies that validate these metrics using real-world data, hindering their practical applicability.
- **Cyber-Physical Attack Dynamics:** The simultaneous occurrence of physical and cyber-attacks on the grid, and their combined impact, is an area that's not been extensively explored.
- **Consumer Behaviour Analysis:** The role of consumers in the smart grid's resilience, especially in adverse scenarios, is not well-understood. Research into consumer behaviour during outages, cyber-attacks, or other adversities could provide invaluable insights.
- **Economic Implications of Resilience Strategies:** While technical and operational aspects of resilience are often discussed, the economic implications of implementing certain resilience strategies remain underexplored.
- **Standardisation of Resilience Metrics:** There's a noticeable lack of standardisation in resilience metrics, making it challenging to compare and contrast findings across different studies.

By addressing these future research avenues and knowledge gaps, we can pave the way for a more resilient, efficient, and consumer-centric smart grid system.

5 Conclusion

The journey into understanding the resilience of smart grids, as illuminated by our review of three pivotal studies, has underscored the multifaceted nature of this domain. The integration of technology, organisational structures, and the ever-evolving cyber landscape presents both challenges and opportunities. As we reflect upon our exploration, the following key findings emerge:

- **Complexity of Smart Grid Systems:** Das et al. (2020) highlighted the intricate challenges posed by the vast geographical spread, organisational scales, and the introduction of a cyber-layer. This complexity necessitates a holistic approach to resilience, considering both technical and organisational aspects.
- **Desirable Resilience Metrics:** For a metric to be effective, it must account for spatio-temporal variations, be goal-oriented, robust against uncertainties, and easily calculable from available data. Furthermore, it should address multiple adversities that might act on the grid simultaneously.
- **Opportunities for Innovation:** Farzin et al. (2016) emphasised the potential in addressing unattended technological aspects, the significance of event severity in resilience, and the dual nature of the cyber-layer, which can be a source of vulnerability and enhanced grid visibility.
- **Interplay of Renewable Energy and Smart Grids:** El Mrabet et al. (2018) shed light on the challenges and prospects of integrating renewable energy sources into smart grids. This integration, while promising, requires careful consideration of stability, reliability, and efficiency.
- **Knowledge Gaps and Future Research:** Despite the extensive research, there remain areas where knowledge is fragmented or limited. Addressing these gaps, from real-world metric validation to understanding consumer behaviour, will be pivotal in future studies.
- **Relevance to the Broader Landscape:** Tying back to our abstract, it's evident that the resilience of smart grids is not merely a technical challenge. It's an interplay of technology, organisational dynamics, and data-driven insights. The findings from the reviewed articles provide a comprehensive foundation, setting the stage for further discussions and research in this domain.

In essence, as smart grids continue to evolve, so too will the challenges and opportunities they present. Through collaborative efforts between academia and industry, and by building upon the insights from foundational studies like the ones reviewed, we can chart a path towards a more resilient and sustainable energy future.

References

1. Das, L., Munikoti, S., Natarajan, B., & Srinivasan, B. (2020). Measuring smart grid resilience: Methods, challenges and opportunities. Renewable and Sustainable Energy Reviews, 130, 109918.
2. Farzin, H., Fotuhi-Firuzabad, M., &Moeini-Aghtaie, M. (2016). Enhancing power system resilience through hierarchical outage management in multi-microgrids. IEEE Transactions on Smart Grid, 7(6), 2869-2879.

3. El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. Computers & Electrical Engineering, 67, 469-482.
4. Watson, J. P., Guttromson, R., Silva-Monroy, C., Jeffers, R., Jones, K., Ellison, J., ... & Walker, L. T. (2014). Conceptual framework for developing resilience metrics for the electricity oil and gas sectors in the United States. Sandia national laboratories, albuquerque, nm (united states), tech. rep.
5. Willis, H. H., & Loa, K. (2015). Measuring the resilience of energy distribution systems. RAND Corporation: Santa Monica, CA, USA, 38.
6. Brown, R. E., Gupta, S., Christie, R. D., Venkata, S. S., & Fletcher, R. (1997). Distribution system reliability assessment: momentary interruptions and storms. IEEE Transactions on power Delivery, 12(4), 1569-1575.
7. Ouyang, M., Dueñas-Osorio, L., & Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. Structural safety, 36, 23-31.
8. Ashok V., Geetha N.B., Rajkumar S., Pauline T.,"Experimental Investigations for Thermal Energy Management by Encapsulation of Nano -Enhanced Bio Phase Change Material in buildings",Energy Sources, Part A: Recovery, Utilization and Environmental Effects,44(2),2022
9. Dhaya R., Ujwal U.J., Sharma T., Singh P., Kanthavel R., Selvan S., Krah D.,"Energy-Efficient Resource Allocation and Migration in Private Cloud Data Centre",Wireless Communications and Mobile Computing,2022( ),2022
10. Arghandeh, R., Von Meier, A., Mehrmanesh, L., & Mili, L. (2016). On the definition of cyber-physical resilience in power systems. Renewable and Sustainable Energy Reviews, 58, 1060-1069.
11. Mylrea, M., &Gourisetti, S. N. G. (2017, September). Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In 2017 Resilience Week (RWS) (pp. 18-23). IEEE.
12. Panteli, M., & Mancarella, P. (2015). The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience. IEEE Power and Energy Magazine, 13(3), 58-66.
13. Li, G., Zhang, P., Luh, P. B., Li, W., Bie, Z., Serna, C., & Zhao, Z. (2013). Risk analysis for distribution systems in the northeast US under wind storms. IEEE Transactions on Power Systems, 29(2), 889-898.
14. Xu, Y., & Singh, C. (2013). Power system reliability impact of energy storage integration with intelligent operation strategy. IEEE Transactions on smart grid, 5(2), 1129-1137.
15. Wang, Y., Chen, C., Wang, J., &Baldick, R. (2015). Research on resilience of power systems under natural disasters—A review. IEEE Transactions on power systems, 31(2), 1604-1613.
16. Framework, N. I. S. T. (2010). Roadmap for smart grid interoperability standards. National Institute of Standards and Technology, 26.
17. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2012). A survey on smart grid potential applications and communication requirements. IEEE Transactions on industrial informatics, 9(1), 28-42.
18. Sandeep Kumar Reddy, Saravanan T., N.T. Velusudha& T. Sunder Selwyn,(2023) "Smart Grid Management System Based on Machine Learning Algorithms for Efficient Energy Distribution",E3S Web Conf. 387 02005 (2023)

19. Faisal, M. A., Aung, Z., Williams, J. R., & Sanchez, A. (2014). Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study. IEEE Systems journal, 9(1), 31-44.
20. Knapp, E. D., & Samani, R. (2013). Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure. Newnes.
21. Brearley B.J., Bose K.R., Senthil K., Ayyappan G.,"KNN approaches by using ball tree searching algorithm with minkowski distance function on smart grid data",Indian Journal of Computer Science and Engineering,13(4),2022