Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995

JGKI: Volume 3, Issue 2, February 2025, online: ISSN 3079-1995
www.jgkijournal.com

ARTICLE OPEN ACCESS Check for updates

Examination of the Effects of False Data Injection Attacks on Smart Grid

[1]*Fuad Hasan Shishir, [2]Md Zahid Hasan, [3]Md Ekramul Haque
[1]North China Electric Power University, Electrical Engineering and it's Automation, China
[2] Fulton Montgomery Community college, Computer Networking & Cyber Security,
[3] Hohai University, College of Energy and Electrical Engineering, Nanjing, China
fuadhasanshishir98@gmail.com; mdzahidhasan205878@gmail.com; ekramulhaque.hhu100@gmail.com;

Abstract
With the development of advanced information and communication technology, traditional power grids have been transformed into smart grids. An important feature of smart grids is the mutual influence between information systems and physical systems, forming a highly coupled power information physical system, which makes smart grids face more severe information security threats than traditional grids. False Data Injection Attack (FDIA) is an emerging form of covert power grid attacks. The paper comprehensively discusses the attack model, suppression schemes, and impact of false data injection on smart grids, and the topic has practical significance. The main work of the paper includes the following aspects: Firstly, the paper provides an overview of the basic concepts and key technologies of smart grids, as well as information security issues. Next, we will comprehensively discuss the FDIA model and its classification. Then, a neural network-based FDIA suppression model was designed and simulated for testing. Finally, the impact of FDIA on smart grids was comprehensively discussed. The main contribution of the paper is the design of a system model for FDIA detection, localization, and data recovery based on a neural network framework. The results of the paper can provide reference for a comprehensive exploration of the impact of FDIA on smart grids.

Keywords: smart grid, false data injection attack, deep neural net

Introduction

The introduction chapter lays the basis for addressing the critical issue of False Data Injection Attacks (FDIA) on smart grids. It outlines the purpose and significance of the research, emphasizing the growing reliance on smart grids as a reliable source of electricity to meet increasing demand. The chapter highlights the necessity for improved security measures to safe these grids from FDIA. It reviews the present state of research on FDIA detection and mitigation, discussing various methodologies employed globally. This chapter sets the stage by providing a clear motivation for the study and detailing the methodology used throughout the research.

1.1 Purpose and significance of the topic

1. Purpose

This study's main purpose is to solve the serious problem of false data injection attacks, or FDIAs, on smart grids. Making sure smart grids are secure has become crucial because of the growing reliance on them as a dependable supply of electricity to satisfy the rising demand. By contrasting different FDIA models, examining the effects of FDIA, and creating a strong neural network-based framework for the identification, localization, and recovery of tampered data, the goal of this study is to enhance smart grid security. The report outlines the methods employed throughout the research and provides a clear justification for addressing FDIAs by offering a thorough background and literature evaluation. Additionally, the study includes an in-depth analysis of smart grids, laying the groundwork for a thorough examination of FDIAs and their impacts on smart grid actions.

2. Significance

The significance of this study relies in its ability to substantially improve the security and resilience of smart grid systems against False Data Injection Attacks. Smart grids are integral to modern power distribution, offering enhanced efficiency, reliability, and sustainability. However, their vulnerability to FDIAs poses a significant threat to their operations and the broader electrical infrastructure. By providing a comprehensive analysis of FDIA models and developing a sophisticated neural network-based detection and recovery framework, this research contributes to the advancement of smart grid security. The study's detailed background and literature review establish a strong foundation for understanding the importance of addressing FDIAs. Consequently, this study not only addresses a critical cyber security issue but also paves the way for more secure and reliable smart grid systems, which are essential for meeting future energy demands sustainably.

1.2 The current situation at home and abroad

In 2009, Liu et al. initially proposed the notion of False Data Injection (FDI) attacks [1]. To gain a comprehensive understanding of this matter, it is necessary to go into the previous research and investigations that have been conducted. He, Youbiao et al. utilized deep learning techniques to detect FDI attack patterns by analyzing historical measurement data, allowing for immediate identification [2]. In 2012, Lin, Jie et al. conducted a study on weaknesses in distributed energy routing and put out innovative FDI attacks targeting the energy routing mechanism [3]. Tufail, Shahid et al. investigated the consequences of

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

foreign direct investment (FDI) attacks on artificial intelligence (AI)-driven smart grids [4]. In their study, Zhang et al. proposed the utilization of a data-driven learning method for the identification of undetectable Fault-Induced Delayed Activation (FDIA) occurrences in distribution systems [5]. Yu, Wei et al. created a data detection system that can identify fraudulent information by utilizing specialized strategies for various sorts of attacks [6]. Xu, Ruzhi et al. devised

a highly effective detection method to counteract FDIA [7]. Chen, Po-Yu and colleagues proposed a real-time method to identify FDI attacks in smart grids. This method improves detection performance by utilizing spatial-temporal correlations among grid components [8]. This solution uses a deep learning-based architecture to detect inserted data measurements [9]. Tran et al. suggested a technique based on a nonlinear physical-constraint model capable of producing covert FDI attacks [10]. Habib et al. established a comprehensive model addressing the implications of FDI attacks on the grid, economy, and society [11]. Pei et al. presented a robust deviation-based detection technique that integrates a supplementary Kalman filter alongside the original weighted least squares estimator [12]. Ayad, Abdelrahman et al. examined the use of Recurrent Neural Networks (RNN) to detect FDI attacks [13]. Drayer, Elisabeth et al. devised a strategy to identify previously undetectable FDI attacks [14]. Dehghani, Moslem et al. suggested a novel detection approach employing singular value decomposition (SVD) and fast Fourier transform (FFT) [15]. Youssef, El-Nasser et al. offered a summary of research on stealth FDI attacks against state estimation [16]. Anwar, Adnan, and Abdun Naser Mahmood evaluated the features and importance of FDI attacks using a literature analysis and case study [17]. Wang et al. suggested a unique data analytical method using the margin setting algorithm (MSA) for detecting FDIAs [18]. Nath, Samrat et al. presented a fastest invasion detection approach for time-varying dynamic models [19]. Li, Yang et al. developed an FDIA detection approach based on safe federated deep learning, combining Transformer, federated learning, and the Paillier cryptosystem [20]. Rahman, Moshfeka and Yuanliang Li developed a stealthy FDIA technique utilizing multi-objective evolutionary optimization, demonstrating large impacts with minimum meter sacrifice [21]. Dayaratne et al. proposed a high-impact FDIA and examined how adversaries can employ strategic information integrity assaults to achieve financial benefits using real-time pricing schemes [22]. Musleh, Ahmed S. et al. conducted a comprehensive investigation of FDI attacks in smart grids, utilizing a detection system based on Principle Component Analysis (PCA) for real-time analysis [23]. Li, Beibei et al. suggested a secure and resilience-enhanced system (SeCDM) to detect and mitigate FDI hazards in smart grids [24]. Lastly, Iqbal et al. compared three FDI detection strategies, resulting in the development of an H2 control method to detect and manage erroneous data injection in a 12th-order smart grid model [25]. These different research initiatives illustrate the complexity and dynamic nature of FDI threats, underlining the necessity for continuing developments in detection and mitigation measures to secure smart grids.

1.1 The content arrangement of the paper.

In this section the arrangement of the paper has been illustrated the summary of the contents including introduction, Understanding Smart Grids, FDIA Model Analysis, Suppression Method, Discussion and Conclusion & Future Outlook. Based on the previous research, different types of FDIA attack model investigated, impact of the attack evaluated on smart grids in this paper. Finally, a suppression method is proposed and concluded with future outlook of the topic. Chapter-wise overview provided in bellow:

Chapter 2

"Understanding Smart Grids," gives a comprehensive description of the technology and its significance in modern power distribution. It discusses the evolution of smart grids, key components such as Advanced Metering Infrastructure (AMI), sensors, communication networks, control systems, and Distributed Energy Resources (DERs). The chapter also delves into the benefits of smart grids, including enhanced reliability,

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

efficiency, integration of renewable energy sources, consumer empowerment, and economic benefits. Additionally, it addresses the challenges associated with implementing smart grids, such as high initial costs, cybersecurity risks, data privacy concerns, and regulatory and policy issues.

Chapter 3: FDIA Models Analysis

In "FDIA Models Analysis," the third chapter, the paper delves into the fundamentals of False Data Injection Attacks (FDIA), explaining their basic concepts and operational mechanisms. It presents a detailed analysis of various FDIA models, their methodologies, and how they compromise smart grid security. The chapter classifies FDIAs based on attack models, network architecture, construction methods, attack targets, and data-driven approaches. It explores different types of FDIA, including state estimation attacks, load redistribution attacks, price manipulation attacks, and data integrity attacks. This chapter gives a full review of the various FDIA models and their potential impacts on smart grid operations.

Chapter 4: Neural Network Based Suppression Method

Chapter 4, titled "Suppression Method," introduces neural network-based solutions for detecting and mitigating FDIA. It explains the use of Self-Attention Deep Convolutional Neural Networks (SA-DCNN) for recognizing and locating FDIA, emphasizing the advantages of embedding the Self- Attention system into DCNN to improve detection accuracy. The chapter also explores the use of Autoencoders with Long Short-Term Memory (AE-LSTM) networks for recovering tampered data. This approach aims to restore normal data by generating corrected data with the same distribution pattern as the input. The combination of AE and LSTM models captures the spatiotemporal correlation of power grid operating data, enhancing the effectiveness of data-driven algorithms in restoring false data to normal.

Chapter 5: Discussion

This Chapter ''Discussion'' part focuses on the operational, economic, and security implications of FDIA on smart grids. It examines how FDIA can disrupt normal operations by manipulating energy routing and causing grid imbalances. The chapter discusses the effects of FDIA in the economy, such as the manipulation of real-time pricing mechanisms and increased operational costs. It highlights the threat to state estimation and how advanced FDIA can bypass traditional detection mechanisms, making it challenging to identify and mitigate such attacks promptly. The chapter also addresses the increased vulnerability of smart grids, the impact of FDIA on dynamic micro-grid partitioning, and the potential for cascading failures. It highlights the vital need for comprehensive cyber-security measures to safeguard the dependability and efficiency of smart grids.

Chapter 6: Conclusion & Future Outlook

The final chapter, "Conclusion & Future Outlook," summarizes the research findings on the impact of FDIA on smart grids and the effectiveness of neural network-based frameworks in mitigating these

attacks. It reiterates the significance of improving smart grid security and resilience through advanced detection and recovery solutions. The chapter outlines future research directions, emphasizing the need for enhanced detection mechanisms, integration of emerging technologies, adaptive security strategies, interdisciplinary research, and global collaboration. It calls for the development of comprehensive security strategies to detect and mitigate FDIA, safeguarding the operational integrity and economic stability of smart grid systems. It points out the vital need for strong cyber-security measures to ensure the dependability and efficiency of smart grids.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

Chapter 2 Understanding Smart Grids

This delivers a complete overview of smart grids, discussing their definition, key components, benefits, and challenges. This chapter explains how the integration of advanced technologies enhances the safety and effectiveness of power distribution systems.

2.1 Introduction to Smart Grids

The generation, distribution, and use of energy have experienced a drastic metamorphosis due to smart grids. Modern information and communication technologies (ICT) integrated with the conventional electrical grid results in a power infrastructure that is resilient, intelligent, and efficient. Real-time monitoring, automatic decision-making, and communication in both directions between companies and customers are made possible by this integration, which has several advantages, including increased efficiency, increased dependability, and the utilization of renewable energy resources. This section offers a thorough overview of smart grids, going over their definition, essential elements, advantages, and drawbacks.

Definition and Concept

A Smart grid is an electrical system that uses digital technology to track, control, and manage the flow of electricity from various generation sources to satisfy the various energy demands of customers. It incorporates various technologies, like smart meters, advanced sensors, automated control systems, and advanced communication networks. The main aim of a smart grid is to make the power grid more trustworthy, efficient, and sustainable by enabling real-time information flow and improved interaction between all stakeholders involved in the electricity supply chain.

The traditional electrical grid was designed over a century ago and has seen incremental improvements over the years. However, it has inherent limitations, such as a lack of real-time monitoring, limited control over power flows, and difficulties in integrating renewable energy sources. Smart grids address these limitations by leveraging modern ICT to create a more dynamic and flexible grid infrastructure. Fig. 2-1 shows Smart Grid [26].

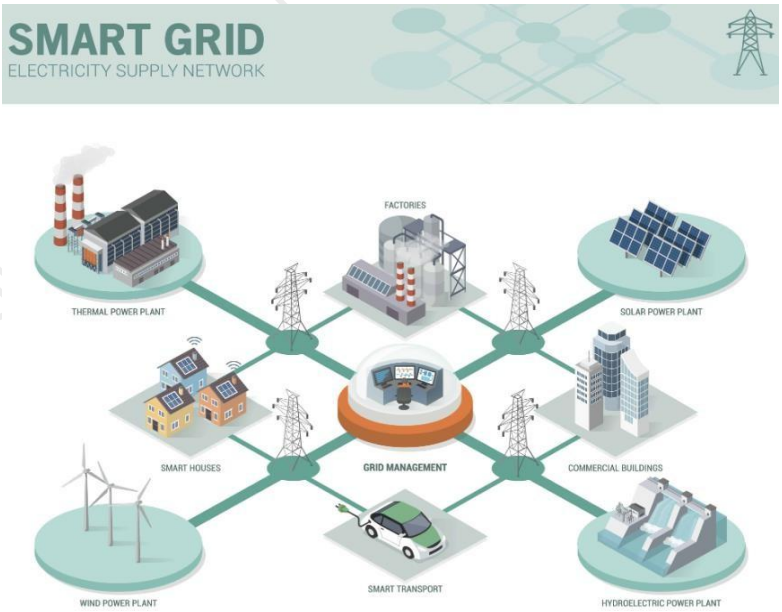


Fig. 2-1 Smart Grid

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

2.1.1 Key Components of Smart Grids

The smart grid ecosystem relies on several essential elements to accomplish its goals. These components are as follows:

1. Advanced Metering Infrastructure (AMI): AMI includes smart meters, networked communication, and data management systems. Smart meters provide detailed, real-time data on power use enables utilities to track usage patterns, implement price changes, and improve billing accuracy. Consumers also gain from enhanced insight into their energy usage, allowling them to make more educated decisions about their consumption.

2. Sensors and Measurement Devices: Sensors, such as phasor measurement units (PMUs), provide high-resolution, time-synchronized data on various grid parameters, including voltage, current, frequency, and phase angles. These measurements are crucial for continuous tracking and analysis, helping to maintain grid stability and prevent outages.

3. Communication Networks: Reliable and secure communication networks are essential for the real-time exchange of data between different grid components. These networks can utilize various technologies, including fiber optics, wireless, and power line communication (PLC). The communication infrastructure ensures seamless data flow, enabling automated control and coordination across the grid.

4. Control Systems: Advanced control systems are used to monitor and control the grid in real-time. These systems take data from sensors and other devices, analyze it, and make decisions to optimize grid performance. They can also automate responses to disturbances, improving the grid's reliability and resilience.

5. Energy Management Systems (EMS): EMS are software tools utilities use to monitor, manage, and enhance the performance of the electrical grid. They provide functionalities such as load prediction, generation scheduling, and fault detection.

6. Distributed Energy Resources (DERs): Energy-storing devices, wind turbines, and solar panels are examples of renewable energy sources included in DERs. These resources are often distributed across the grid and can be located on consumer premises. Integrating DERs into the grid requires advanced control and coordination to ensure stability and reliability.

7. Consumer Interfaces: Smart grids provide consumers with interfaces, such as in-home displays and mobile applications, to monitor their energy usage and interact with the grid. These interfaces enable consumers to take part in demand response programs, adjust their spending based on price signals, and contribute to overall grid efficiency.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

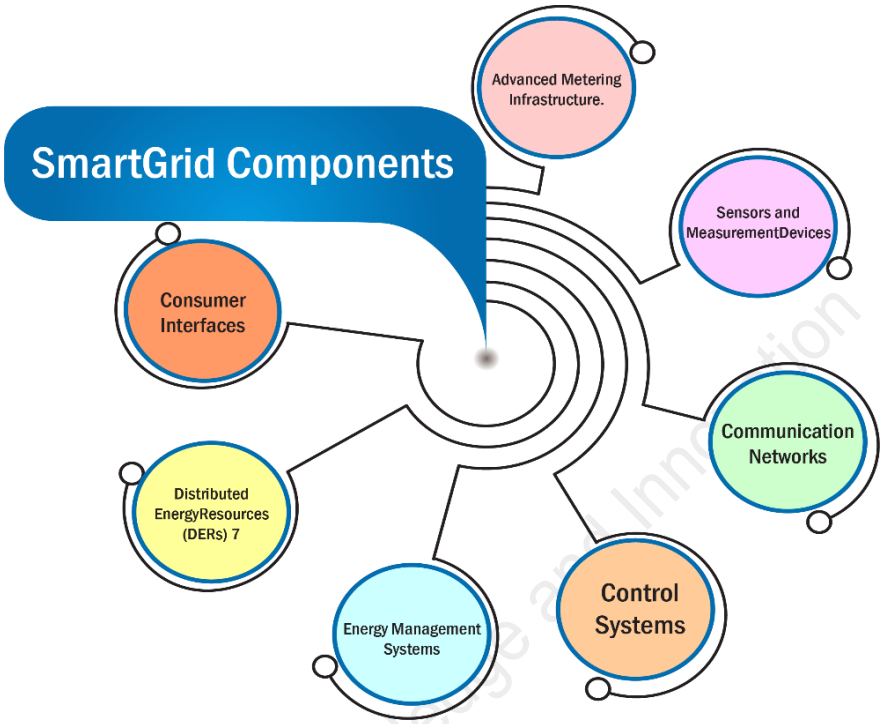


Fig. 2-2 Smart Grid Components

2.1.2 Benefits of Smart Grids

The deployment of smart grid technology offers numerous benefits to both utilities and consumers, including:

1. Enhanced Reliability and Resilience: Smart grids improve the reliability of the power supply by enabling real-time monitoring and rapid response to faults. Automated control systems can isolate and address issues quickly, reducing the duration and impact of outages. The ability to integrate distributed generation sources also enhances the grid's resilience to disruptions.

2. Improved Efficiency: Smart grids optimize the generation, distribution, and consumption of electricity, reducing losses and improving overall efficiency. Advanced metering and control systems enable better demand management, reducing peak loads and minimizing the need for costly infrastructure upgrades. Utilities can also implement dynamic pricing, encouraging consumers to shift their usage to off-peak times.

3. Integrated Renewable Energy Sources: One of the key advantages of smart grids is the integration of intermittent and decentralized renewable energy sources like solar and wind power. Advanced control systems and energy storage solutions help manage the variability of these sources, ensuring a stable and reliable power supply. This integration promotes the transition to a more sustainable energy system and decreases dependence on fossil fuels.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

4. Empowerment of Consumers: Smart grids provide consumers with greater visibility into their energy usage and enable them to take part in demand response programs. Consumers can monitor

their consumption in real-time, receive alerts about high usage, and adjust their behavior to save money and lessen their environmental impacts. Smart meters and dynamic pricing also lead to more accurate billing and improved customer satisfaction.

5. Enhanced Security: Smart grids incorporate advanced cyber security measures to protect against both physical and cyber threats. By continuously monitoring the grid and detecting anomalies, utilities can prevent and respond to attacks more effectively. This improves the electrical system's overall resilience and security.

6. Economic Benefits: The deployment of smart grid technology creates economic opportunities through job creation, increased investments in renewable energy, and the development of new technologies. Improved grid efficiency and reduced operational costs also lead to lower electricity prices for consumers.

2.1.3 Challenges of Smart Grids

In spite of the numerous benefits, the implementation of smart grids also represents several challenges that have to be presented:

1. High Initial Costs: The deployment of smart grid necessitates weighty investment in setup, including advanced meters, sensors, communication networks, and control systems. These initial costs can be a barrier to adoption, particularly for smaller utilities or those in developing regions.

2. Cybersecurity Risks: The increased connectivity and digitalization of the grid, make it further vulnerable to get cyber-attacks. Ensuring security of the smart grid requires robust cybersecurity measures, continuous monitoring, and regular updates to address emerging threats. The complexity of securing a vast and interconnected system poses a significant challenge.

3. Data Privacy Concerns: Smart grids collect large amounts of data on consumer energy usage, raising concerns about data privacy. Utilities must implement strong data protection measures to ensure that consumer information is secure and used appropriately. Regulatory frameworks are also needed to address privacy issues and build consumer trust.

4. Integration of Diverse Technologies: Smart grids involve the integration of various technologies, each with its own standards and protocols. Ensuring interoperability between different components and systems is essential for seamless operation. Developing common standards and promoting collaboration between stakeholders is crucial to address this challenge.

5. Regulatory and Policy Issues: The successful deployment of smart grids requires supportive regulatory and policy frameworks. To stimulate investment in smart grid technology, governments and regulatory agencies must offer incentives and clear standards. Regulatory barriers, such as outdated policies and conflicting regulations, can hinder progress and need to be addressed.

6. Technical Challenges: The implementation of smart grid technology involves complex technical challenges, such as ensuring the accuracy and reliability of sensors, managing large volumes of data, and optimizing control algorithms. Ongoing investigate and progress are needed for addressing these key challenges and improve the performance of grid systems.

7. Consumer Engagement: Engaging consumers and encouraging them to contribute in request reply programs and energy-saving initiatives is critical for the success of smart grids. Utilities need

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

to provide clear information, incentives, and support to help consumers understand and benefit from smart grid technology.

2.2 Technology in Smart Grids

The technology underpinning smart grids is multifaceted, encompassing various kinds of hardware and software components designed to optimize grid performance and facilitate real-time communication. These technologies can be broadly categorized into sensing and measurement, control and automation, and communication infrastructure.

Sensing and Measurement:

Advanced sensors and smart meters, are integral to the functioning of smart grids. PMUs provide high-resolution, time-synchronized data on grid conditions, allowing for precise monitoring of voltage and current at various points in the network. This data is crucial for real-time analysis and decision-making, helping to make sure grid stability and trustworthiness.

Smart meters, on the other hand, provide detailed information on electricity consumption at the consumer level. These devices provide mutual connection between the usefulness and the user, facilitating dynamic pricing, demand response programs, and more accurate billing. Smart meters also empower users to manage their power usage and make knowledgeable verdicts on reducing consumption and costs.

Control and Automation:

Automation technologies are crucial for self-healing capabilities of the smart grid's infrastructure. Automated switches that reclosers can quickly isolate faults and restore power, minimizing the impact of outages. Distributed control systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems provide centralized monitoring and control, allowing operators to handle the grid proficiently and respond to emerging issues [98].

Advanced control algorithms and artificial intelligence are used more frequently employed to optimize grid operations. Artificial Intelligence can scrutinize big quantities of data/info from sensing systems and other sources for forecast potential problems and recommend corrective actions. Machine learning algorithms may additionally expand the accuracy of load forecasting, empowering better planning and resource allocation.

Communication Infrastructure:

Dependable and secure communication structure is the backbone of smart grids. This infrastructure enables the real-time exchange of data between various grid components, including sensors, meters, control systems, and utility operators. Technologies like fiber optics, wireless networks, and power line communication (PLC) are commonly used to establish robust communication links.

The communication network system within a smart grid has to be resilient, moreover secure to prevent disruptions and protect against cyber threats. This requires implementing advanced encryption, authentication, and intrusion detection systems. Confirming the security and integrity of information is paramount to maintaining grid security and reliability.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

Integration of Renewable Sources:

Smart grids are designed to accommodate a various range of electric energy sources, counting renewable energy for instance wind, solar, and hydroelectric power. Join in these recurrent and decentralized different energy sources into the grid postures significant encounters but also offers substantial benefits in terms of sustainability and energy independence.

Distributed Energy Resources (DERs) for example solar panels on the rooftop and wind turbines from different places can be linked to the grid, allowing for the efficient distribution within locally generated power. Energy storing systems, like battery, play an essential role in harmonizing supply of the energy, and demand. They keep additional energy generated throughout low demand periods and releasing it all through peak demand.

Grid operators use advanced forecasting and optimization algorithms to control the variable nature of renewable sources. These algorithms able to predict weather patterns and regulate grid actions consequently to ensure a steady and reliable power supply.

Electric Vehicles (EVs) and Smart Charging:

The proliferation of electric vehicles (EVs) represents both encounters and chances for smart grids. The amplified demand for electricity because of EV charging able to strain the grid, particularly throughout peak hours. EVs able to serve as distributed energy resources, providing storage and support for grid stability.

Smart charging infrastructure allows for the effective supervision of EV charging, optimizing the use of available grid capacity. The Vehicle-to-Grid (V2G) system allows electric vehicles (EVs) to return stored energy to the power grid, helping to balance supply and demand. This bidirectional energy flow enhances grid resilience and facilitates the integration of renewable energy sources.

Advanced Metering Infrastructure (AMI):

Advanced Metering Infrastructure (AMI) is a critical component of smart grids, enabling the collection, analysis, and management of energy usage data. AMI systems consist of smart meters, communication networks, and data management software. These systems deliver real-time data on energy consumption, helping utilities optimize grid operations and improve customer service.

AMI supports request reply programs, whereas customers can regulate their energy usage in reply to price signals or incentives. This helps to reduce peak demand and expand grid efficiency. Additionally, AMI enables more accurate and timely billing, decreasing the need for manual meter readings and enhancing customer satisfaction.

The Distributed Energy Resources (DERs):

Distributed Energy Resources (DERs) are limited power production or storage technologies that provide an alternative to or improvement upon the traditional electric power system. Systems that combine heat and power, wind turbines, solar panels, and battery storage are examples of distributed energy resources (DERs). These resources are often located close to where electricity is used, such as at a home or business, and can be cast-off to deliver backup power at the time of outages or to reduce demand on the grid during peak periods.

The incorporation of DERs into the grid requires advanced control and coordination to ensure stability and reliability. Grid operators use sophisticated software and algorithms to manage the

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

variability of these resources and to optimize their use in conjunction with central generation and grid resources.

Grid Management Software:

Smart grids rely on sophisticated software to monitor and manage grid operations. This software can include Energy Management Systems (EMS), Advanced Distribution Management Systems (ADMS), Distributed Energy Resource Management Systems (DERMS)[99]. These systems provide utilities with the tools they need to monitor grid performance, manage distributed resources, and optimize grid operations.

EMS are harnessed to keep eye on and control the stream of electricity across the transmission and distribution networks. They offer instantaneous data on grid conditions, enabling workers to detect and take action to problems quickly. DERMS are used to manage distributed energy resources, optimizing their use in conjunction with central generation and grid resources. ADMS provide a comprehensive sight of the distribution network, permitting operators to manage grid performance, sense and retort to outages, and enhance grid operations.

Energy Storage Systems:

In smart grids, energy storage devices play an important role, providing a mechanism to accumulate extra energy produced throughout periods of low demand and to issue it during periods of in height demand. These systems can comprise batteries, compressed air energy storage, flywheels, and pumped hydro storing. Energy storing systems supports to steadiness supply and demand, expand grid stability, and support the addition of renewable energy sources.

When integrating intermittent and variable renewable energy sources like wind and solar, battery devices play a critical part. By holding extra energy generated during high renewable output times and releasing it during low output periods, batteries provide a consistent and predictable power supply. Lithium-ion and flow batteries are examples of advanced battery technologies with long cycle lives and high energy density, which makes them ideal for grid applications.

Demand Reply Programs:

Demand reply program is a key component of smart grids, enabling utilities to manage demand and to steadiness supply and demand in actual. This program encourages customers to decrease or shift electricity consumption at the time of peak periods, helping to reduce strain on the grid and to evade the need for costly infrastructure promotions.

Demand reply programs can include time-of-use electricity pricing, where electricity fees differ liable on the time of day, and straight load control programs, where values remotely manage certain appliances, for example air conditioners or even water heaters, to decrease demand during apex periods. These programs provide benefits to both utilities and consumers, helping to reduce electricity costs and improve grid reliability.

Micro-grids:

Small-scale power grids known as "micro-grids" can meaning separately from the main grid or in tandem with it. A wide range of power generating sources, including solar panels (PVs), wind turbines, diesel engines, and energy storage devices, can be encompassed in them. Micro-grids enable the integration of renewable energy sources and offer a way to increase grid resilience.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

Micro-grids can operate in island mode, where they are disconnected from the primary grid and provide power to a specific area, such as a campus or a community. They can also operate in grid- connected mode, where they are linked to the primary grid and provide power to the wider grid. Micro-grids offer several benefits, including improved reliability, enhanced resilience, and the ability to integrate renewable energy sources.

2.3 Security Aspects of Smart Grids

The integration of advanced technologies and the increased connectivity of smart grids introduce new security challenges. Ensuring the security of smart grids is critical to protecting the infrastructure from cyber-attacks and maintaining the reliability of the electricity supply.

Cyber-security Threats:

Smart grids are vulnerable to a range of cyber-security threats, including malware, phishing attacks, and Denial of Service (DoS) attacks. These threats can undermine the integrity and accessibility of the grid, leading to disruptions in power supply and potential damage to critical infrastructure.

False Data Injection Attacks (FDIAs) are a particularly concerning threat to smart grids. In an FDIA, attackers inject false data into the grid's regulator systems, causing the system to make incorrect decisions. This can lead to significant disruptions in grid operations, including blackouts and equipment damage. Detecting and mitigating FDIAs requires advanced monitoring and analytics capabilities.

Physical Security:

In addition to cyber-security, physical security is essential for protecting smart grid structure. Substations, transformers, and other critical components must be safeguarded against physical attacks and natural disasters. Implementing strong security measures, such as surveillance systems, access controls, and physical barriers, can help to protect these assets.

Data Privacy:

Smart grids gather vast amounts of data on consumer energy usage, raising concerns about data privacy. Protecting consumer data from unlawful access and ensuring compliance with privacy regulations is essential. This requires implementing strong data encryption, secure data storage, and access controls.

Resilience and Reliability:

Ensuring the resilience and dependability of smart grids is critical to maintaining a stable electricity supply. This involves implementing robust grid management practices, redundancy measures, and emergency response plans. Advanced analytics and AI can assist in anticipating and addressing potential issues, improving the overall resilience of the grid.

Regulatory and Policy Frameworks:

Effective regulatory and policy frameworks are necessary for ensuring the security and reliability of smart grids. Governments and regulatory agencies are essential for establishing standards, providing oversight, and promoting best practices. Collaborative efforts between utilities, technology

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

providers, and policymakers are necessary to address the complex security challenges facing smart grids.

Security Standards and Best Practices:

Adopting industry standards and best practices is crucial for enhancing the security of smart grids. The International Electrotechnical Commission (IEC) has developed comprehensive frameworks and guidelines for smart grid security. These standards offer a systematic method to identifying and mitigating security risks, ensuring the confidentiality, integrity, and availability of grid data and operations.

Understanding the complex nature of smart grids, their technological components, and associated security challenges is essential for developing effective strategies to enhance their performance and reliability. By utilizing advanced technologies and implementing robust security measures, smart grids can provide a more efficient, reliable, and sustainable electricity supply, meeting the growing demand for energy in a secure and resilient manner.

2.4 Summary

This chapter digs into the diverse world of smart grids, illuminating their definition, important components, benefits, problems, and the technological breakthroughs that underpin them. An updated electrical system known as a smart grid uses digital technology to enhance power flow management and control from generation to consumption. The combination of smart meters, advanced sensors, automated control systems, and robust communication networks collectively aim to make the grid more dependable, efficient, and sustainable. Essential components including Advanced Metering Infrastructure (AMI), sensors and measuring devices, communication networks, control systems, and energy management systems are highlighted for their roles in achieving these goals.

The chapter underlines the many benefits of smart grids, including better stability and resilience, improved efficiency, seamless integration of renewable energy sources, consumer empowerment, heightened security, and economic rewards. These innovations permit real-time monitoring, improved demand control, and more accurate billing, ultimately contributing to overall grid efficiency and sustainability. However, adopting smart grids is not without its obstacles. High initial costs, cyber-security threats, data privacy concerns, integration of varied technologies, regulatory and legislative challenges, technical complexities, and the need for customer interaction are important hurdles that must be overcome to ensure the effective adoption of smart grids.

Advanced sensing and measuring technologies, control and automation systems, communication infrastructure, and integration of renewable energy sources are critical for optimizing grid performance and facilitating real-time communication. Energy storage devices, demand response programs, and the growth of micro-grids further boost the grid's capability to balance supply and demand, improve security, and enable the integration of renewable energy.

Security considerations, notably cyber-security risks and physical security measures, are crucial in securing the smart grid system. Ensuring data privacy, resilience, and reliability through rigorous regulatory and legislative frameworks, industry principles, and best practices is crucial for sustaining a stable and secure electrical supply. It is vital to have a solid grasp of smart grid technologies, their advantages, and the issues they present in order to design successful strategies for boosting grid performance and dependability. Through the use of modern technologies and applying tight security measures, smart grids can fulfill the growing demand for energy in a secure, efficient, and sustainable manner, paving the way for a resilient and future-ready electrical infrastructure.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

Chapter 3 FDIA Attack models

3.1 Fundamentals of FDIA

False Data Injection Attacks (FDIAs) are becoming an important concern in the realm of cyber- security, especially within smart grids and other critical infrastructures. These attacks involve the deliberate insertion of incorrect data into a system to manipulate its operations, mislead decision- making processes, or cause physical harm. Understanding the fundamentals of FDIAs is essential for developing effective security measures to protect modern technological systems from such malicious activities.

Concept and Mechanism of FDIA

FDIAs take advantage of vulnerabilities in a system's data acquisition and communication processes. By injecting false data, attackers can distort the system's perceived state, leading to incorrect outputs or actions. This type of attack is especially deceptive, as it can be executed without directly tampering with the physical components of the system.

Reconnaissance

Initially, the attacker collects information about the target system. This includes understanding the system's structure, data flow, and communication protocols. Attackers typically employ passive monitoring techniques during this phase to avoid detection and to build a comprehensive map of the system's operations.

Vulnerability Identification

Next, the attacker identifies weak spots in the system where data can be intercepted and altered. Common vulnerabilities include unsecured communication channels, inadequate encryption practices, and the absence of robust data validation mechanisms. By pinpointing these weaknesses, attackers can determine the most effective points of entry for injecting false data.

Data Manipulation

Following data manipulation, the attacker monitors the system to observe the effects of the injected false data. The range of potential impacts can vary widely, from minor operational disruptions to severe physical damage, depending on the attacker's objectives. This phase allows the attacker to gauge the effectiveness of their actions and make any necessary adjustments.

Impact Assessment

Following data manipulation, the attacker monitors the system to observe the effects of the injected false data. The range of potential impacts can vary widely, from minor operational disruptions to severe physical damage, depending on the attacker's objectives. This phase allows the attacker to gauge the effectiveness of their actions and make any necessary adjustments.

Persistence and Evasion

Advanced attackers use strategies to maintain their presence within the system over time while avoiding detection. This can involve the use of sophisticated malware designed to be stealthy, exploiting zero-day vulnerabilities that are unknown to the system's defenders, or frequently changing their methods to stay ahead of security measures. These tactics help attackers remain hidden within the system and continue their activities without interruption.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

Types of Attack Models

False Data Attack Models:

There are several threat models for false data injection (FDI) attacks targeting the cyber-physical infrastructure of the Smart Grid. Some of these models necessitate full knowledge of network data and topological configurations, while others can function with limited resources. Moreover, data-driven approaches are employed to develop stealthy FDI attacks. This section examines these various FDI attack models.

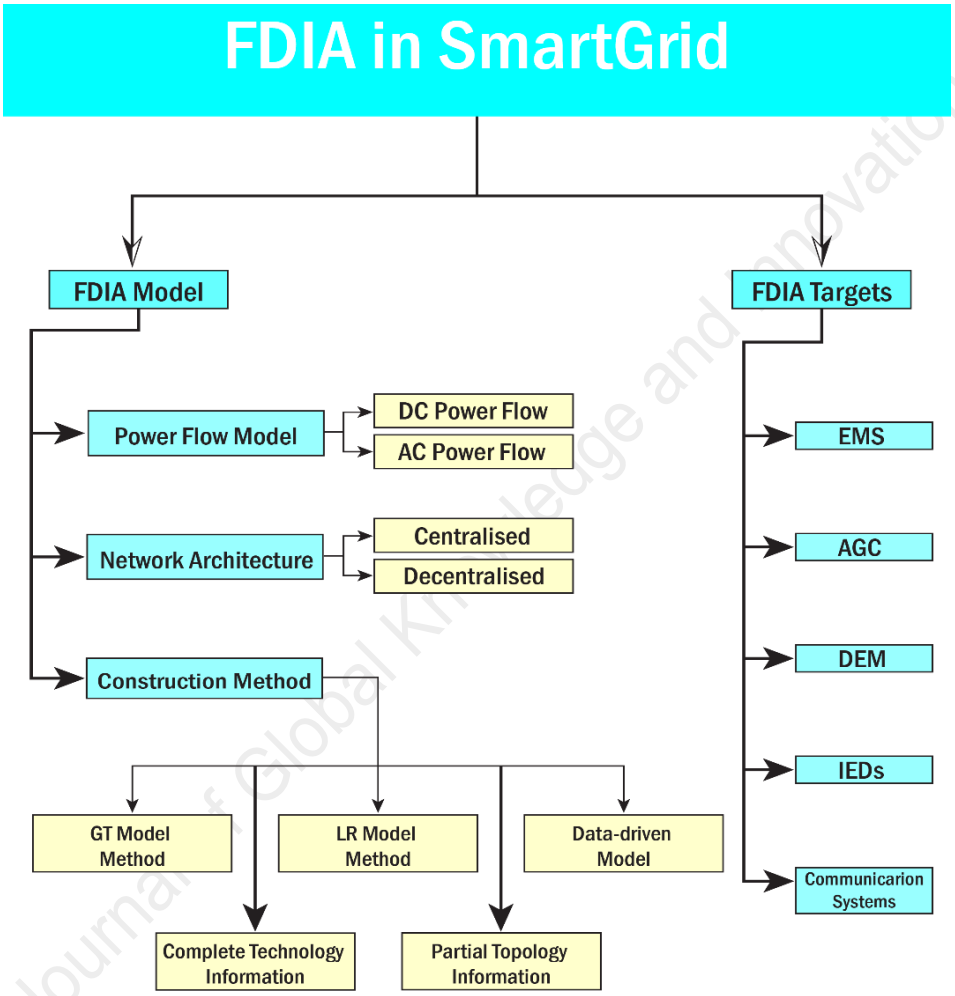


Fig. 3-1 FDIA in SmartGrid

3.1.1 Classification Based on Attack Models

1) Power Flow Model: While industry-standard state estimators depend on nonlinear AC power flow models, most research on FDI attacks is carried out in limited situations and usually uses linear DC- based power flow models. Liu et al. [27] were pioneers in FDI attacks under the DC model, followed by studies such as [31], [34], [35], [36], and [32]. However, these simplified DC models are not suitable for AC-based SEs due to their nonlinear characteristics.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

such as [43] and [44], have explored FDI attacks under both DC and AC models. A detailed comprehension of the structural stuffs of power schemes and the power flow model used is essential for effective vulnerability analysis and countermeasures.

2) Network Architecture:

1. Centralized Attacks: These target the central state estimator by manipulating measurement reports from communication devices, which impacts other functions like optimal power flow and economic dispatch. Notable studies include [27], [48], [49], and [67].
2. Distributed Attacks: These are more challenging in distribution systems due to the requirement for local state knowledge. Attacks can inject bad data at the supply source, target energy control instructions, and affect communication links. Relevant studies include [56], [55], and [69].

3) Construction Methods: Various methods for constructing adversarial FDI attacks are discussed, focusing on techniques used to manipulate data to compromise power system operations.

FDI attacks require detailed information of network topology, transmission parameters, SE algorithms, and BDD methods, assuming significant access to the power system. However, it's unrealistic for adversaries to have extensive measurement access. Liu et al. [27] noted that adversaries often face constraints, limited to certain sensor readings due to physical defenses or budget constraints.

Liu et al. [27] described adversaries injecting random bad data to disrupt SE performance or targeting specific state variables. Research covers both random and targeted FDI attacks impacting SE and additional elements, like in [69], where random data injections disrupted energy supply- demand balance.

Kosut et al. [47] and [48] explored stealthy FDI attacks, proposing a detectability heuristic for BDD vulnerabilities. They developed an algorithm [48] with two attack types: strong, compromising enough meters to make the state unobservable using graph theory, and weak, controlling a particular number of meters.

FDI attacks face challenges as power system topology settings are secure, frequently change, and are only accessible to operators' EMS. Intruders have limited physical access and real-time knowledge of configurations and physical conditions, such as transformer tap adjustments and circuit breakers.

Attacks with Partial Topology Information:

Constructing valid FDI attacks typically assumes that adversaries have full access to topology information. However, it is practical to assume that adversaries have incomplete knowledge of network topology due to limited real-time information about configurations and physical statuses for example transformer tap adjustments, circuit breakers, and switches. Realistic FDI attacks can be initiated with partial information and constrained resources.

Rahman et al. [31] explored FDI attacks using incomplete topology knowledge from both adversary and defense perspectives. Other relevant studies include [35], [36], [39], [58], and [52]. G. Liang et al. [28] reviewed many scenarios where adversaries can obtain partial topology information necessary for FDI attacks, including:

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

1. **Manual or Online Collection**: Adversaries manually collect grid topology information or use online methods with their own meters.
2. **Market Database**: Adversaries extract topology information from location-based price variations.
3. **Power Flow Measurements**: Adversaries gather topology data from power flow

Load Redistribution (LR) Attacks:

LR attacks are a specific type of FDI attack that target load measurements of nodal power injections and power flows to create biased load estimates. These attacks can be executed even with limited access to certain meters.

Yuan et al. [33] initially formulated LR cyberattacks considering various resource constraints. They expanded this framework in [63] to assess two attack objectives: immediate and delayed, utilizing a max-min attacker-defender framework. Xiang et al. [62] introduced a corresponding cyber- physical attack on LR, generators, and transmission lines, formulated as a two-level optimization problem within the attacker-defender model.

Moreover, in [64], leveraging local topology attacks from [66] and concepts from [31], the authors devised a local LR attack strategy using partial network knowledge. Unlike [31], this approach allows the attacker to select any area of interest, not just a specific cut.

Grid Topology Attacks and Line Outages:

Recent research has focused on attacks targeting power grid topology and transmission line outages. Traditionally, adversarial models assumed static grid topology, only allowing false data injection. However, grid topology often changes due to maintenance and failures.

J. Kim and L. Tong [51] developed a stealthy attack model manipulating both network measurements and topology configurations (e.g., transformer taps, circuit breakers) to generate a false topology undetected by the state estimator. Their model includes strong and weak attack regimes based on available information.

Studies like [59] examined coordinated cyber-physical attacks causing unnoticeable transmission line outages. Adversaries could hide grid topology by injecting false data and coordinating cyberattacks to conceal line outages, potentially causing cascading failures.

A heuristic topology attack model in [66] identified attack regions with minimal information. However, [51], [59], and [66] did not account for PMUs, which detect outages via deviations in bus phasors.

Building on [59] and [66], [60] suggested masking line outages by manipulating PMU data. Additionally, [61] examined the impact of security-constrained financial dispatch on transmission line attack strategies.

Data-Driven Attacks:

Known as blind attacks, these FDI attacks are crafted without antecedent knowledge of the power grid. They leverage statistical techniques such as independent component analysis [70], singular value decomposition [71], principal element analysis [72], sparse optimization [73], heuristic approaches, and

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

machine learning algorithms. By analyzing correlations in measurement data and topology parameters, adversaries can launch undetectable attacks.

Esmalifalak et al.[67] pioneered this approach, using independent component analysis to infer system topology and power states from power flow measurements. This method requires statistically independent loads and meter data. Singular value decomposition [71] and principal component analysis [72] have also been utilized to create stealthy FDI attacks, with PCA-based methods transforming measurements into non-correlated components.

These methods are effective only in the existence of additive white Gaussian noise (AWGN). Adnan and Abdun [34], [32] demonstrated that in the presence of gross errors, these blind attacks fail conventional BDD. They proposed a blind attack strategy using matrix recovery to distinguish low- rank measurement matrices from gross errors. Similarly, [68] employed low-rank and sparse matrix factorization for data-driven attacks on matrices with missing values.

In coordinated cyberattacks, false data attacks target different components of the Smart Grid. Power generators, transmission lines, substation networks, renewable energy sources, monitoring and control centers, smart electronic gadgets, and network and communication systems are just a few examples of these components that are susceptible.

3.1.2 Classification Based on Target Attack Models

Cyber-physical components are crucial for observing and controlling the Smart Grid, they also expose it to different kinds of data breaches, though, affecting the availability, security, and integrity of data. FDI (False Data Injection) attacks target components across all Smart Grid domains, such as power generation, transmission, distribution, utilization, market activities, and operations.

1. **EMS (Energy Management System)**: The EMS in the control center is a prime target. The state estimator, which links cyber and physical spaces, is especially vulnerable because it relies on sequential processes. Outputs from SCADA or PMU systems feed into the state estimator, whose results are critical for subsequent EMS modules. An FDI attack on the state estimator can cause significant errors and deceive system operators without detection. The majority of FDI attack methods affect various components, including communication systems, IEDs, AMIs, and power system properties. Transmission lines [61][65], network topology [74][51][59], and system observation [62] are further targets.
2. **Automatic Generation Control (AGC)**: Cyberattacks can target communication systems like PMU and SCADA since they provide data between AGC and generating units or Networked Control Systems (NCSs). Reference [75] shows that adversaries can manipulate the AGC algorithm by altering frequency measurements and control commands. In [76], various data integrity attacks on AGC, such as scaling, ramp, pulse, and random attacks, are studied. These attacks can provide false system load information, altering measurements and generator settings.
3. **Instead of using predefined data integrity models, adversaries often employ intelligent and adaptive strategies.** To address this, Tan et al. [50] were the first to study false data attacks on AGC sensor measurements. They demonstrated that FDI attacks on power flow measurements can cause grid frequency to critical levels quickly, bypassing sensor data integrity checks. Further research on FDI attacks targeting AGC and its communication structures can be found in [77][78].
4. **Contingency Analysis (CA)**: The practicality of FDIs on CA through the SE is examined in [49]. Attackers can insert fake data into the SE, misleading the CA process and causing normal transmission lines to appear as contingencies. This false information is then embedded in the security-constrained economic dispatch (SCED), potentially causing significant impacts (see Section

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

VIII-3). An FDI attack on CA involving security-constrained optimal power flow (SCOPF) and transmission line capacities is also discussed in [79], showing that such attacks can lead to overloading conditions on transmission lines during certain contingencies.

5. **Distribution Energy Management (DEM):** DEM [24] is crucial for managing real-time networks and dynamic decisions-making that traditional EMSs cannot handle. DEMs are used in distributed SEs and DERs/microgrids to improve efficiency, minimize outages, and maintain stable frequency and voltage levels [80]. In spite of their benefits, DEMs are vulnerable to cyberattacks. The impact of FDIs on DEM was studied in [69], revealing that manipulated data can cause imbalanced demand and response, increase transmission and distribution costs, and compromise the stability of energy supplies. Further research on DEM vulnerabilities to false data attacks in dynamic microgrids is presented in [53].

6. **Communication Systems:** Various communication technologies in the Smart Grid are vulnerable to FDI attacks [30]. For example, power system measurements can be compromised via the SCADA system [34], affecting other elements like the SE or AMI. If attackers access the SCADA system, they can falsify customer billing information by damaging AMI. Communication protocols, such as IEC 61850, are also susceptible to FDI attacks [30]. Other vulnerable communication systems include NCS [57], WAMS [29], IEEE C37.118 [30], and wide area network communication infrastructure.

7. **Intelligent Electronic Devices (IEDs):** IEDs connect field devices to communication systems, allowing SCADA and SAS to collect essential grid data. FDI attacks can compromise this critical information by breaching IEDs [54]. For instance, attackers can alter voltage readings and modify IED settings, causing relays to trip. This can lead to abrupt voltage drops below critical levels, resulting in load shedding and potentially causing power outages.

3.1.3 Proposed attack models from the literatures

Jie Lin et al. [3] proposed FDIA attack model in the paper on false data injection attacks against distributed energy routing in the smart grid involves several key mathematical formulations to describe and quantify the impact of such attacks. The model aims to optimize the energy routing process by minimizing the cost of energy transmission, represented as: Minimize {Cost = $\frac{1}{2} \cdot \sum L_{ij} \in$ L($|E_{ij}| \cdot Cost_{ij}$)} Subject to: For each supply-node v ∈ NP, $\sum_{i \in N_v} E_{vi} \leq P_v$, For each demand-node u ∈ ND, $\sum_{j \in N_u} E_{uj} = -D_u$, For all links Lij ∈ L, $E_{ij} = -E_{ji}$. The model further investigates the impact of false data injection attacks by introducing false energy values and link states, represented by D^*_u for forged energy requests, P^*_v for forged energy supplies, and LS^*_{ij} for false link states. The model also considers metrics like supplied energy loss ($\Delta D_n = \sum_{u_i \in N_{D^*}} \Delta D_{u_i}$), increased energy transmission cost ($\Delta Cost_n$=Min($Cost^*$)− Min(Cost))$_m$and the number of outage users, providing a comprehensive quantitative evaluation of the attacks' impact on the distributed energy routing process.

Jinsub Kim et al. [51] addresses undetectable topology attacks on the smart grid by modifying the topology estimate from $G = (V, E)$ to a different target topology $\bar{G} = (V, \bar{E})$. The model assumes that the adversary has global information and can intercept and modify both digital network data $s \in \{0,1\}^d$ and analog meter data z, resulting in modified data $\bar{s} = s + b \pmod 2$ and $\bar{z} = z + a(z)$, where $a(z) \in A \subset \mathbb{R}^m$ and $b \in \{0,1\}^d$. The measurement relationship is modeled by the AC power flow model $z = h(x, G) + e$, with x being the state vector and e the additive noise. For DC models, the relationship simplifies to $z = Hx + e$, where H is the measurement matrix. The key condition for an undetectable attack is $Col(H) \subset Col(\bar{H}, A)$, ensuring the modified measurements $\bar{z} = z + a(z)$ remain in the column space of the target measurement matrix $\bar{H}$. This model offers a framework

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

to evaluate the vulnerability of the grid and devise countermeasures to secure a subset of meters, thus preventing undetectable attacks.

Zong-Han Yu et al. [44] proposed a model in the paper outlines a blind false data injection attack using the Principal Component Analysis (PCA) approximation method to bypass the bad data detection (BDD) system in smart grids. The model leverages PCA to transform the observation vector into a new vector with uncorrelated components, facilitating the construction of a stealthy attack vector $a = H_{PCA}c$. The state estimation problem is represented by $z = Hx + v$. The PCA matrix H_{PCA} is obtained by performing PCA on the dataset z, resulting in the transformed dataset x_{PCA}. The relation between the original state vector x and the PCA-transformed vector x_{PCA} is given by $x \approx P_x x_{PCA}$, in which $P_x = H H_{PCA}^{+}$ and H^{+} represents the pseudoinverse of H. The attack is considered stealthy as it minimally affects the residue vector $r = z - Hx$, maintaining a low probability of detection by the BDD system.

Ying Sun et al. [35] introduces a novel false data injection attack approach called False Data Proportional Attacks (FDPAs). The FDPA model is designed to compromise the state estimation in power systems by leveraging local grid topology rather than the full transmission-line admittance values. To achieve this, the attacker injects false data evenly to all buses and transmission lines linked to a targeted bus. The power system is modeled with N buses and described by the undirected graph $G = (B, E)$, where B represents buses and E represents transmission lines. The state variables are denoted as $x=(x_1, \cdots, x_n)^T$ and measurements as $z = (z_1, \cdots, z_m)^T$, with the relation $z = h(x) + e$, where e represents measurement errors. For DC state estimation, the simplified power flow model is $P_{k,l} = -b_{k,l}\theta_{k,l}$, where $b_{k,l}$ is the susceptance and $\theta_{k,l} = \theta_k - \theta_l$. The attack vector a is constructed as $a = Hc$ for some $c \in R^n$, ensuring the attack remains unobservable. By carefully adjusting the injected false data $\Delta P_{l,i}$and ΔP_i in proportions related to the local topology, the attacker can bypass traditional bad data detection methods. This method was validated through simulations on the IEEE 30-bus test system, demonstrating the FDPA's ability to successfully compromise the system's state estimation.

Jiwei Tian et al. [82] introduce a data-driven and low-sparsity false data injection attack strategy in smart grids, divided into three stages: Eliminate-Infer-Determine (EID). Initially, intercepted meter data containing outliers is preprocessed using the Augmented Lagrange Multiplier (ALM) method to separate the original data matrix $\boldsymbol{Z}$ from the outliers matrix $\boldsymbol{E}$ by solving the optimization problem $\min \|Z\|_* + \lambda \|E\|_1$ subject to $Z_{outlier} = Z + E$. Next, the cleaned data is used to infer the system's incomplete knowledge through parallel factor analysis (PARAFAC), which decomposes a fourth-order tensor Φ as $\Phi = \sum_{k=1}^{ld} \xi k \times nj \circ nj \circ nj \circ nj$. Finally, the inferred system matrix $\hat{N}$ is utilized to design a sparse attack vector $a_i = \hat{N}I$ using convex optimization to solve $\min_l \| a_i \|_0 = \| \hat{N} l \|_0$ subject to $u^T l = 1$. This method constructs effective and undetectable false data injection attacks by leveraging data-driven and low-sparsity approaches, ensuring stealthy attacks even with incomplete system knowledge and the presence of gross errors in measurement data.

Thusitha Dayaratne et al. [22] describe a novel high-impact false data injection attack (FDIA) against real-time pricing (RTP) in smart grids. This attack model focuses on manipulating data to achieve financial benefits without compromising the grid's communication channels or components. The RTP scheme that divided a day into 48 half-hour pricing slots. A demand coordinator sends a price signal for the next 24 hours, consisting of 48 price values, each corresponding to one pricing slot. Household scheduled devices using parameters like start times, demand and running duration. The Home Energy

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

Management System (HEMS) schedules devices, incurring an inconvenience cost if a device doesn't start at the preferred time.

The optimization process involves local optimization for each HEMS and a master optimization by the utility company (UC). Each HEMS schedules devices to minimize the overall cost, including the electricity bill and the inconvenience cost. The aggregated demand profile is sent to the UC, which adjusts the price signal. This process repeats until it converges to the global optimal solution, at which point more cost reduction is impossible.

In the proposed attack model, the attacker focuses on a more realistic and calculated scenario in which compromising devices or communication channels are not required. The attacker manipulates their own data through HEMS or IoT devices. The attack steps include selecting a device and the corresponding pricing slots, *setting the device parameters* to the beginning of the particular pricing slot, setting the latest finish time (ls) as $ls = es + rt - 1$, and increasing the device demand (d_{new}>d_{old}) to a new value (d_{new}). By setting the device as inflexible (with fixed ps and ls), the attacker makes sure that the device's start time is not shifted by the local optimization . The aim is to force the distributed optimization to shift demand to other time slots.

The attacker manipulates their own data through HEMS or IoT devices without compromising communication channels. Possible methods include increasing the demand value of one or many devices, adding fake home devices to HEMS, adding real home devices but disconnecting them once the system converges, or collaborating with other households to spread the false demand.

The experiment setup involves using artificial datasets based on real-world household consumption data, including 10,000 households, each with 5-10 devices. Experiments are conducted with datasets of varying sizes (500, 1000, 2500, 5000, 7500 households). The impact of the attack is assessed by injecting a false demand of 0.1% of the overall demand by increasing the selected device's demand. The other's side cost reduction and the total impact on the community's bill and inconvenience are calculated. The false demand percentage is gradually rises (up to 5%) and the calculations are repeated.

Results show that even a 0.1% false demand injection can significantly reduce the adversary's cost. The adversary can achieve a cost reduction of up to 28.73% for a 0.5% false demand. The attack is effective regardless of the number of participating households, and the false demand percentage is highly correlated to the device usage cost for the opponent.

A small increase in aggregated demand can significantly increase the unit price due to the quadratic nature of the price function. The attack causes HEMS to move devices away from the attacked time slots, leading to a lower actual unit price for the adversary. This type of attack can be executed by any user without compromising the communication channels. The attack demonstrates vulnerabilities in DR systems that rely solely on optimization.

In conclusion, the proposed high-impact FDIA against RTP in smart grids shows how an adversary can manipulate demand data to achieve significant financial benefits. The attack does not require technical skills or compromising the grid's communication channels, making it feasible for any user within the system. The results highlight the need for robust false data detection mechanisms to ensure the reliability and efficiency of DR schemes in smart grids.

Yuancheng Li et al. [58] proposed model introduces a method for constructing false data injection (FDI) attack vectors without requiring complete knowledge of the power system's network topology. Initially, limited topology information is mapped to a high dimension using Kernel Independent

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

Component Analysis (KICA), generating a Jacobian matrix ($H \equiv (\frac{\partial H(x)}{\partial x}|_{x=0})$ based on incomplete topology information. This helps approximate the current state of the power system represented by the state variables vector ($x = [x_1, x_2, \ldots, x_n]^T$. The measurements vector is denoted as $z = [z_1, z_2, \ldots, z_m]^T$, and the attack vector as $a = [a_1, a_2, \ldots, a_m]^T$. Kernel independent components are represented by v_k for $k = 1,2,\ldots,p$. The objective function for the attack vector is formulated as U = $pn^Ta + q \frac{2}{\exp(r^TDr)/\lambda + 1}$, where $r = \frac{a}{L}$ is the proportion of attacked vectors to measurements. The optimization constraints include $\|a - H_pc\| \leq \tau$, $N(a + L) \geq 0$, and $a^T\tilde{N}a = 0$.The Lagrangian function is $L(a, \lambda_1, \lambda_2, \lambda_3) = U(a) + \lambda_1^T h_1(a) + \lambda_2^T h_2(a) + \lambda_3^T h_3(a)$, and the attack vector is updated by maximizing $d_k \nabla U(z = (a_k + \frac{1}{2} d_k^T H_k d_k$ subject to $h_1(a_k) + \nabla h_1(a_k)^T d_k \leq 0, h_2(a_k) + \nabla h_2(a_k)^T d_k$ and $\nabla g(a_k)^T d_k = 0$. The Jacobian matrix approximation is $= Hx + e = H_{px} + e$, and the eigenvalues of kernel independent components are denoted as $\tilde{K} = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_p)$. State estimation follows $z = h(x) + e$. This method is validated through experiments on various IEEE bus systems, demonstrating its effectiveness in constructing attack vectors rapidly and with high success rates, even with limited measurements and incomplete topology information.

3.2 Impact of FDIA on Smart Grids

False Data Injection Attacks (FDIA) represent a major cybersecurity threat to smart grids, which are modern electricity networks that utilize digital communications technology to monitor and control electricity flow. The impact of FDIA on smart grids can be profound and multifaceted, affecting various aspects of grid operations, economic stability, and security.

Operational Disruption

FDIA can severely disrupt the usual operation of smart grids by adding erroneous data into the grid's operational data streams. This manipulation can lead to several operational inefficiencies:

- **Energy Routing Inefficiencies**: Manipulated data about energy demand and supply can cause suboptimal routing decisions. Energy may be directed along inefficient or even non-existent paths, increasing transmission costs and reducing overall system reliability. This inefficiency not only raises operational costs but can also cause energy shortages in areas with falsely reported high demand.
- **Grid Imbalance**: By misrepresenting the actual state of the grid, FDIA can create artificial imbalances. For instance, false demand-side data might show an increased energy need, prompting the grid to reroute energy unnecessarily, leading to potential overloads or shortages. Similarly, supply-side attacks that misrepresent available capacity can cause incorrect energy allocation, resulting in either excess or insufficient energy distribution.
-

Economic Consequences

The economic impacts of FDIA are substantial, affecting both individual users and the overall market.

- **Manipulation of Real-Time Pricing**: FDIA can be used to manipulate real-time pricing (RTP)

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

mechanisms, allowing attackers to gain financial benefits. For example, by falsifying their energy demand data, an attacker can influence the distributed optimization process used in RTP, thereby reducing their electricity costs while increasing costs for other consumers. This not only undermines the fairness of the energy market but also leads to economic losses for other users and the utility company.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

- **Increased Operational Costs**: The inefficiencies caused by FDIA, such as energy being routed through suboptimal paths, can significantly increase operational costs. Utility companies may have to invest more in managing these inefficiencies, which can translate to higher costs for consumers.

Security and Reliability

FDIA creates major concerns to the security and reliability of smart grids.

- **Compromised State Estimation**: Smart grids rely on accurate state estimation to function effectively. FDIA can manipulate the data used in state estimation, leading to incorrect assessments of the grid's state. This can prevent grid operators from making informed decisions, potentially leading to incorrect operational responses and further destabilizing the grid.
- **Bypassing Detection Mechanisms**: Advanced FDIA can be designed to bypass traditional detection mechanisms. For example, attacks that align injected errors with the grid's operational data can avoid detection by standard residual-based bad data detection systems. This makes it challenging to identify and mitigate such attacks promptly.

Increased Vulnerability

Smart grids are particularly vulnerable to FDIA due to their reliance on digital communications and data.

- **Exploitation of Data Collection and Transmission**: FDIA can exploit vulnerabilities in the data collection and transmission processes of smart grids. By injecting false data at various points in the data flow, attackers can cause widespread disruptions and inefficiencies. This exploitation can lead to a breakdown in the grid's ability to respond to real-time conditions accurately.
- **Sophisticated Attack Techniques**: Attackers can employ sophisticated methods, such as Principal Component Analysis (PCA) or Kernel Independent Component Analysis (KICA), to craft undetectable FDIA even with limited information about the grid's topology [100]. These sophisticated methods further complicate the detection and mitigation of such attacks.

Impact on Dynamic Partitioning

Dynamic microgrid partitioning is essential for optimizing energy distribution within smart grids. FDIA can significantly disrupt this process.

- **Misreported Supply and Demand**: FDIA can manipulate the data used in dynamic partitioning by under-reporting energy supply or over-reporting energy demand. This can lead to inefficient microgrid segmentation, affecting the dependability and effectiveness of energy distribution within the grid. As a result, operational failures and increased energy losses can occur.
- **Operational Failures:** Disrupted partitioning can cause certain areas within the grid to experience energy shortages or surpluses, leading to operational failures. This imbalance can be particularly problematic during peak demand periods, potentially leading to widespread blackouts or brownouts.

Systemic Risks

The interconnected nature of smart grids means that a localized FDIA can have widespread effects:

- **Cascading Failures**: Disruptions in one part of the grid can quickly cascade to other parts, affecting broader grid stability and performance. This interconnectivity can amplify the impact of FDIA, turning what might have been a localized issue into a major grid-wide problem.
- **Grid Stability**: FDIA can undermine the overall stability of the grid by causing unpredictable fluctuations in energy supply and demand. This can make it challenging for grid operators to make

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

sure a stable and dependable energy supply, leading to frequent adjustments and potential overreactions that can further destabilize the grid.

The impact of FDIA on smart grids underscores the critical need for robust cybersecurity measures. These attacks can disrupt operations, misallocate resources, cause economic losses, compromise security, increase system vulnerabilities, affect dynamic partitioning processes, and introduce systemic risks. Ensuring the reliability and efficiency of smart grids requires comprehensive security strategies to detect and mitigate FDIA, safeguarding the grid's operational integrity and economic stability.

3.3 Summary

False data injection attacks (FDIAs), which target smart grids' digital communication and data processes, are a severe concern. . These attacks can disrupt operations, mislead decision-making, and compromise the security and reliability of the grid. FDIAs can cause operational inefficiencies, economic losses, and systemic risks, impacting various aspects of grid operations, economic stability, and security.

Understanding the foundations of FDIAs, including their concept, mechanism, and impact, it's important to reducing these risks. FDIAs exploit vulnerabilities in data acquisition and communication processes, manipulating data to distort the system's perceived state. Attackers use reconnaissance to gather information, identify vulnerabilities, manipulate data, assess impact, and evade detection. Various attack models exist based on power flow models, network architecture, construction methods, and data-driven approaches.

The impact of FDIAs on smart grids is multifaceted. They can disrupt operational efficiency, manipulate real-time pricing, increase operational costs, compromise state estimation, bypass detection mechanisms, and exploit vulnerabilities in data collection and transmission. FDIAs also affect dynamic microgrid partitioning, leading to operational failures and systemic risks like cascading failures and grid instability.

In conclusion, protecting smart grids from FDIAs requires comprehensive cybersecurity measures. Understanding the attack models, vulnerabilities, and potential impacts is crucial for developing effective security strategies. By implementing robust security measures, smart grid operators can safeguard the grid's operational integrity, economic stability, and overall reliability.

Chapter 4 Neural Network Based Suppression Method

4.1 Overview of Neural Networks

Machine learning algorithms have a subclass called neural networks that are designed to identify patterns. They harness a sort of machine insight, labeling, and grouping of raw input to know sensory data. They are made up of layers upon layers of networked nodes, or neurons, with the capacity for each layer to acquire increasingly intricate data representations. In applications like picture and speech recognition, language translation, and gaming, where the connection between inputs and outputs is extremely nonlinear and complicated, neural networks perform very well [84]. Neural networks are depending on the knowledge of false neurons, which are modeled after biological neurons present in the human head. Based on applied weights and activation goals, these artificial neurons process input data and generate output signals.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

Neural networks are characterized by their architecture, which incorporates the input layer, unseen layers, and the yield layer or output layer. The input layer takes the raw data, the hidden layers examine the data through several transformations, and the output layer offers the ultimate forecast or classification result. The learning method in neural networks encompasses modifying the weights of the linking between neurons to decrease the error between the expected output and the actual output. This operation is often done by a method called back propagation, which propagates the error backward through the network to bring up-to-date the weights [85].

4.1.1 The Convolutional Neural Networks

CNNs (Convolutional Neural Networks), a system of neural networks, typically used for processing structured grid data like photographs. CNNs are planned to adaptively and automatically acquire three-dimensional hierarchies of information as of input photos. They apply a mathematical procedure called convolution, which captures the local relationships in the input data [86]. The prime components of CNNs contain three layers. They are convolutional layers, fully linked layers.and pooling layers.

Convolutional Layers: These layers use a set of filters in the input, each making a feature map that shows specific features of the input, for instance, colors, textures, or edges. The filters slide over the input data, creating a map of activations recognized as feature maps Each filter is designed to detect a precise pattern in the data, enabling the network to learn compound features at multiple levels of abstraction.

- **Fully Connected/Linked Layers:** These layers are harnessed at the end of the network to combine the features extracted by prior layers to produce predictions. Allowing the model to integrate all the learned features for the last output, every neuron in an entirely connected layer is linked to all neurons in the preceding layer. The fully linked or connected layers translate the high-level feature representations into the final classification or regression outcomes.
- **Pooling Layers:** These layers decrease the dimensionality of each feature map while retaining the most significant information. Pooling is typically performed using operations like max pooling or else average pooling, which aid in reducing the computational complexity and controlling over-fitting. By down-sampling the feature maps, pooling layers confirm that the network is further strong to dissimilarities in the input data, such as translation and rotation.

CNNs have been extremely fruitful in tasks for example object detection, image sorting, and segmentation, largely because of their capability to capture spatial hierarchies in images. The hierarchical structure of CNNs enables them to study low-level properties like ends and textures in the primary layers and high-level features like shapes and substances in the deeper layers [87]. Notable applications of CNNs include facial recognition schemes, autonomous vehicles, medical image analysis, and more.

4.1.2 Recurrent Neural Networks

One kind of neural network entitled recurrent neural networks (RNNs) is designed on the way to identify patterns in data sequences, including time series text, financial data, speech, and video. RNNs have an inner memory that permits them to maintain info about aforementioned inputs and use this information to influence the current output. This memory is built harnessing loops within the network, enabling the retention of sequential data [88].

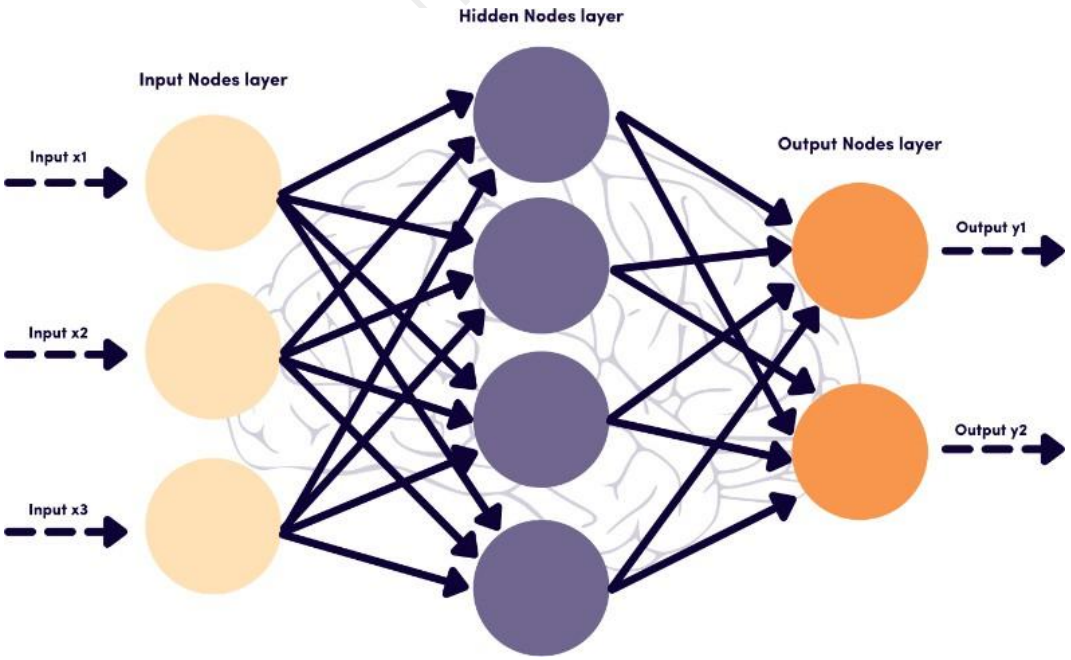
- Hidden State: The hidden state, which stores details on the order of inputs that have been processed thus far, is the fundamental building block of RNNs. In each time step, the hidden state is updated according to the prior hidden state and the present input. This makes the system suitable for sequence modeling by allowing it to maintain a dynamic state that changes over time.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

- Recurrent Layer: This layer applies the same set of weights to the input at each time step, which allows the network to handle orders of fluctuating lengths and maintain temporal information. The shared weights ensure that the network can generalize across different parts of the sequence, capturing temporal dependencies and patterns.
- Long Short-Term Memory (LSTM) & Gated Recurrent Units (GRU)[101]: These are distinct types of RNNs intended to process the problem to remove gradients that can occur in regular RNNs. LSTM networks use gates to control the flow of data, allowing them to maintain and bring up-to-date long-term dependencies in the information. GRUs make simpler the LSTM construction by merging the forget and input gates into a solo bring up-to-date gate. Both LSTM and GRU units are capable of learning long-range dependencies, making them effective for tasks involving long orders.

RNNs are widely harnesses in applications for instance language modeling, speech understanding, and machine translation, where understanding the context and sequence of information is crucial. They excel in tasks where the temporal dynamics of the data are important, allowing the model to learn and predict based on sequential patterns. Advanced applications of RNNs include natural language processing, music composition, and video analysis [88].

In summary, neural networks, particularly CNNs and RNNs, have transformed the direction of machine learning by enabling models to automatically learn and extract meaningful patterns from complex data. Their architectures, designed to handle spatial and temporal dependencies, respectively, make them powerful tools for a broad range of applications. Fig. 4-1 showing Neural Network [83].



Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

Fig. 4-1 Neural Network

4.1 FDIA detection and positioning solution based on SA-DCNN

4.1.1 SA mechanism

The idea of attention was initially proposed in biology and has gradually developed into an important research field in cognitive science. It refers to a complex cognitive ability that humans have, that is, selectively focusing on certain aspects or characteristics of information in a specific time and space, and ignoring other perceptible information [90][91] . Under the SA mechanism, autonomous prompts are called queries. Given any query, attention weights can be calculated to guide the selection of optimal sensory inputs. These sensory inputs are called values, and each value

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

associated with a key. Based on this, we can assume that the input sequence is $X = [x_1, ..., x_N] \in R^{Dx \times N}$ and the output is $H = [h_1, ..., h_N] \in R^{Dv \times N}$, the specific calculation process of the SA mechanism is shown in Fig. 4-2 [89]:

(1) Suppose the input sequence is x_i, primary linearly plot/map the input sequence into three vector units, namely key vector $k_i \in R^{Dk}$, query vector $q_i \in R^{Dk}$, and value vector $v_i \in R^{Dv}$, and for the whole input sequence X, the linear mapping procedure can be obtained by the following formula:

$$Q = W_q X \in R^{Dk \times N} \tag{4-1}$$

$$K = W_k X \in R^{Dk \times N} \tag{4-2}$$

$$V = W_V X \in R^{Dv \times N} \tag{4-3}$$

Where, $W_q \in R^{Dk \times Dx}$, $W_k \in R^{Dk \times Dx}$, $W_V \in R^{Dv \times Dx}$ are respectively the parameter matrices used for learning and training in the linear mapping process [96], and $Q = [q_1, ..., q_N]$, $K = [k_1, ..., k_N]$, $V = [v_1, ..., v_N]$,are matrices composed of query vectors, key vectors and value vectors correspondingly.

(2) For the query vector $q_n \in Q$, after passing the SA mechanism, the output vector h_n is expressed as:

$$\begin{aligned} h_n &= attention(q_n, (K, V)) \\ &= \sum_{j=1}^{N} \alpha_{nj} v_j = \sum_{j=1}^{N} \frac{\exp(s(k_j, q_n))}{\sum_{i=1}^{N} \exp(s(k_i, q_n))} v_j \\ &= \sum_{j=1}^{N} soft\max(s(k_j, q_n)) v_j \end{aligned} \tag{4-4}$$

Here, $n, j \in [1, N]$ represents the location of the output vector sequence and the input vector sequence, α_{nj} denotes the weight of the nth output vector focusing on the jth input vector, $soft\max(\cdot)$ represents the normalization function, and $s(k_j, q_n) = k_j^T q_n$ represents the scoring function. In order to reduce the normalization error, the attention marking function is scaled and

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

simplified, so the output is $\boldsymbol{H}$ denotes as:

$$\boldsymbol{H} = soft\max\left(\frac{\boldsymbol{K^T Q}}{\sqrt{D_k}}\right)\boldsymbol{V} \tag{4-5}$$

Among them, D_k represents the input vector dimension.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

The SA mechanism effectively converts the input sequence into a vector representation containing a large quantity of attention data, reducing the learning of useless data. It can also "dynamically" generate different connection weights when processing variable-length sequences, improving the training model's performance. Since it is problematic for CNN to learn the long- distance dependencies of sequences, embedding the SA mechanism into DCNN as a layer of the neural network (NN) can improve the effectiveness of covert FDIA detection and positioning.

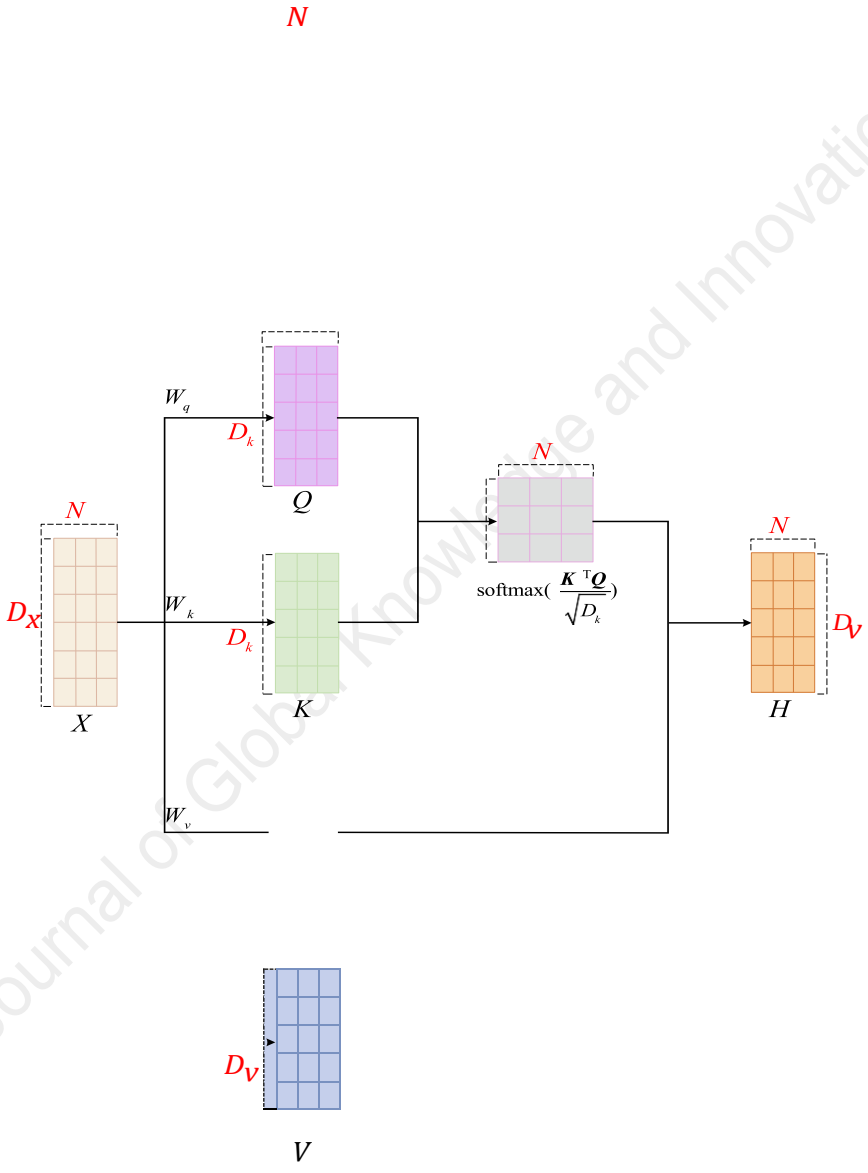


Fig. 4-2 SA-The calculation process of the mechanism

4.1.2 SA-DCNN framework and FDIA detection and positioning process

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

4.1.2.1 Multi-label classification

From a mathematical point of view, detecting the existence of FDIA in the power system can be seen dividing the entire measurement vector hooked on two categories: presence and absence. Therefore, FDIA detection for single-label classification based on machine learning algorithms is a very simple problem. However, identifying the location of the attack requires multi-label classification, which is a relatively SA-DCNN training process

The SA-DCNN structure is exposed in Fig. 4-3 and whereas contains an input layer, three convolutional layers, a flat layer, an SA layer, a fully connected layer and finally ends with an output layer. The input layer $\boldsymbol{z^t} \in [z^t_1, z^t_2, ..., z^t_n]$ represents the input data with time measurement of n at the time of t, and $\boldsymbol{y^t} \in [y^t_1, ..., y^t_n]$ represents the determined input data label.

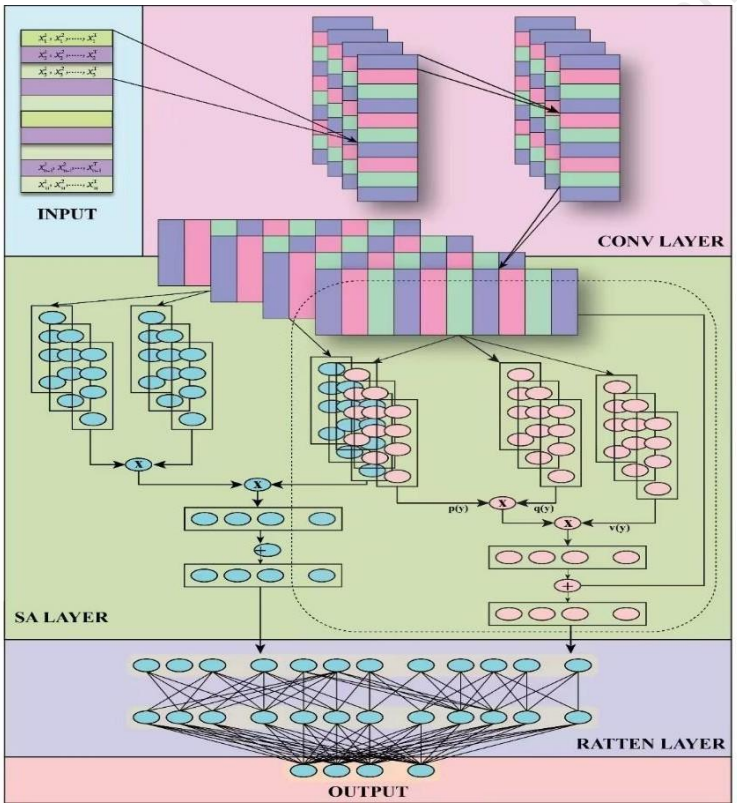


Fig. 4-3 SA-DCNN framework

Inatially, after inputting $\boldsymbol{z^t}$ into the primary convolutional layer, information features are excavated through nonlinear transformations such as convolution operations, batch normalization, and the use of ReLU activation functions. The $c_{1,j}$th feature map of the first convolutional layer j generated by $\boldsymbol{z^t}$ can be expressed as:

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

$$c_{1,j} = \mathrm{Re}LU(\boldsymbol{z}^{t} * \boldsymbol{h}_{\boldsymbol{1,j}} + b_{1,j}) \quad (4\text{-}6)$$

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

$$z^{t} * h_{1,j} = \sum_{k=1}^{l_{1,j}} (h_{1,j})[i] \cdot (z)[i-k-\frac{l_{1,j}}{2}] \quad (4\text{-}7)$$

Here, $h_{1,j}$ denotes the jth convolution kernel of the initial convolution layer, $b_{1,j}$ presents the length of convolution kernel, and denotes the relevant bias of the first convolution layer.

After that all convolutional layers execute the same convolution action, and the output of the earlier convolutional layer is used as the input of the next convolutional layer. Based on this, the output of $q-1$ the previous convolutional layer is input to the c_{q-1}th convolutional layer, and that can be stated as follows:

$$c_{q,j} = \mathrm{Re}LU(c_{q-1} * h_{q,j} + b_{q,j}) \quad (4\text{-}8)$$

In this equation, $c_{q,j}$ denotes the jth feature map in the qth convolutional layer. In order to expand the efficiency of sensing long sequence data, the output of the last convolutional layer, i.e., the features learned by the q_{max} layer, is input to the SA layer. The production of this layer can be attained by formula (4-5). Then the feature output of the SA layer is overextended, input into a fully connected layer, and triggered by means of the activation function ReLU, that can be unambiguously stated as the subsequent formula:

$$c_F = \mathrm{Re}LU(w_F \cdot c_S + b_F) \quad (4\text{-}9)$$

Here, c_S、c_F、w_F、b_F denote the input, output, weight and bias relations of the fully connected layer respectively.

Thereafter, the sigmoid function is harnessed to classify the output of the output layer, and the results are as follows:

$$\hat{y}^{t} = sigmoid(w_D \cdot c_F + b_D) \quad (4\text{-}10)$$

Here, $\hat{y}^{t} = [\hat{y}_1^{t}, \ldots, \hat{y}_n^{t}]$ represents the last result of multi-label classification; w_D、b_D represents the weight and bias of the output layer. It should be noted that in order to expand the sensitivity of the convolution action to positional features, the entire network does not use the pooling layer, so that the algorithm can achieve better detection and positioning performance.

Finally, SA-DCNN model classification results, $\hat{y}^{t}, i = 1, \ldots, n$ are associated with the detection threshold , to regulate the false data existing in the measurement data, which can be expressed as follows:

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

$$if\ \begin{cases} \hat{y}_i^t \geq \square \rightarrow \hat{y}_i^t = 1 \quad (\boldsymbol{false\ data}) \\ \hat{y}_i^t < \square \rightarrow \hat{y}_i^t = 0 (\boldsymbol{normal\ data}) \end{cases} \tag{4-11}$$

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

When $\hat{y}_i^t$ is greater than θ, assign it 1 directly and classify it as false data, otherwise assign it 0 and classify it as ordinary data. After detecting false data, the attack area of the false information can be located based on multiple labels [96].

The overall process of realizing FDIA recognition and positioning by dint of SA-DCNN is shown in Fig. 4-4.

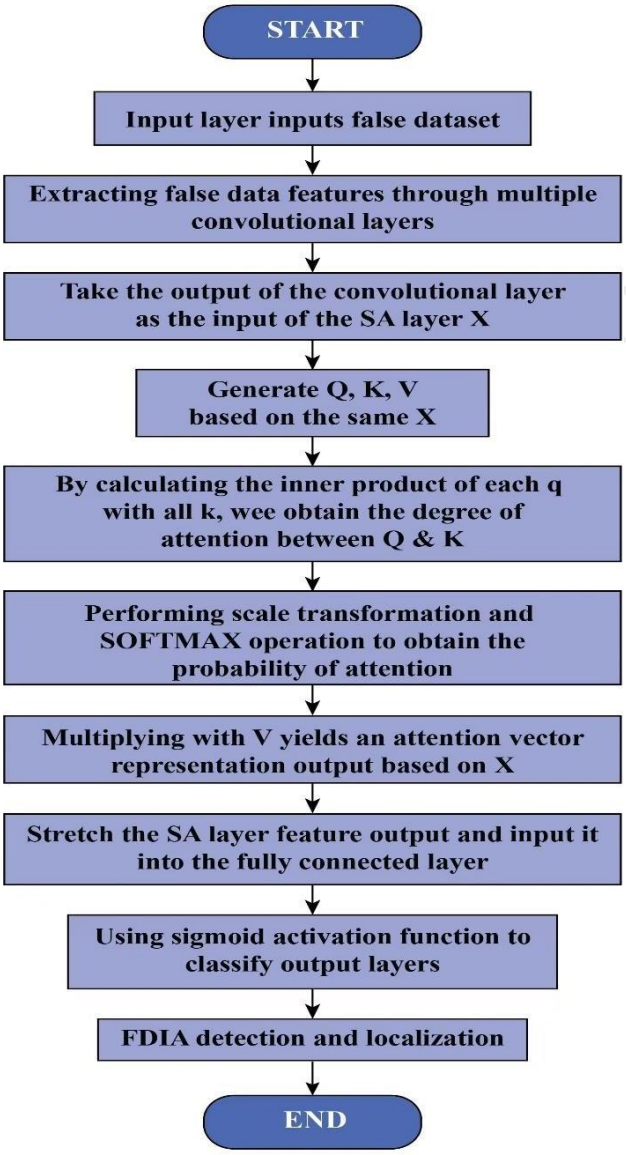


Fig. 4-4 Detection and positioning flow chart

4.2 FDIA data recovery solution based on AE-LSTM

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

4.2.1 Auto-encoder model

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

the input, the decoder excerpts feature from the feature encoding part. At present, many papers detect FDIA in power systems by comparing the errors between generated data and input data [94][94][95], and achieve very good results. In this paper, AE is mainly used to detect false data. To restore normal data instead of detecting FDIA, with the help of the AE model, corrected data with the same distribution pattern as the input can be generated, and the corrected data can be used to replace the detected false attack data, thereby achieving the recovery of the original data. The effect of data recovery can be verified with the help of the aforementioned SA-DCNN.

Suppose a time-specific multivariate sequence data set is $\boldsymbol{X} = [x^t_1, x^t_2, ..., x^t_m]$, where m represents the input feature dimension, and the AE model can be expressed as [97]:

$$\begin{cases} \varphi : \boldsymbol{x} \to \boldsymbol{H} : f_e(x, \theta_e) \\ \psi : \boldsymbol{H} \to \boldsymbol{x}' : f_d(x, \theta_d) \end{cases} \tag{4-13}$$

φ, ψ represent the encoding and decoding change method respectively. Among them, $\boldsymbol{H}$ presents the minimum feature space, f_e, f_d presents the nonlinear system in the encoding and decoding process respectively, $\theta_e = \{\boldsymbol{W_e}, \boldsymbol{b_e}\}$ and $\theta_d = \{\boldsymbol{W_d}, \boldsymbol{b_d}\}$, denotes the AE model training weight and bias respectively, $\boldsymbol{x}$ and $\boldsymbol{x}'$ denotes the input and produced data respectively. In general, $\boldsymbol{H} = f_e(\boldsymbol{W_e}\boldsymbol{x} + \boldsymbol{b_e})$ and $\boldsymbol{x}' = f_d(\boldsymbol{W_d}\boldsymbol{H} + \boldsymbol{b_d})$ are occupied as normal operation. The optimal $\boldsymbol{\theta_e}, \tilde{\boldsymbol{\theta_d}}$ can be found by minimalizing the residual difference between the input data and the generated data as:

$$\{\tilde{\boldsymbol{\theta_e}}, \tilde{\boldsymbol{\theta_d}}\} = \arg\min_{\boldsymbol{\theta_e}, \boldsymbol{\theta_d}} \| \boldsymbol{x} - \tilde{\boldsymbol{x}} \|_2 \tag{4-14}$$

In order to further improve the adaptability of the AE model, reduce the dependence on time characteristics, and reduce the over-fitting of the model, they use the recurrent neural network to learn the characteristics of sequence data and replaces the hidden layer in AE with LSTM to form AE-LSTM. Improve the effectiveness of data-driven algorithms in restoring false data to normal data.

4.2.2 Data recovery process based on AE-LSTM

The LSTM is the further development of RNN and can often be used to solve problems such as gradient disappearance that happen during long sequence data training. Due to the introduction of gates and memory neurons, the LSTM network can not only control the transmission of input, output and hidden states, but also reduce over-fitting problems during the exercise process. The LSTM network model is exposed in Fig. 4-5.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

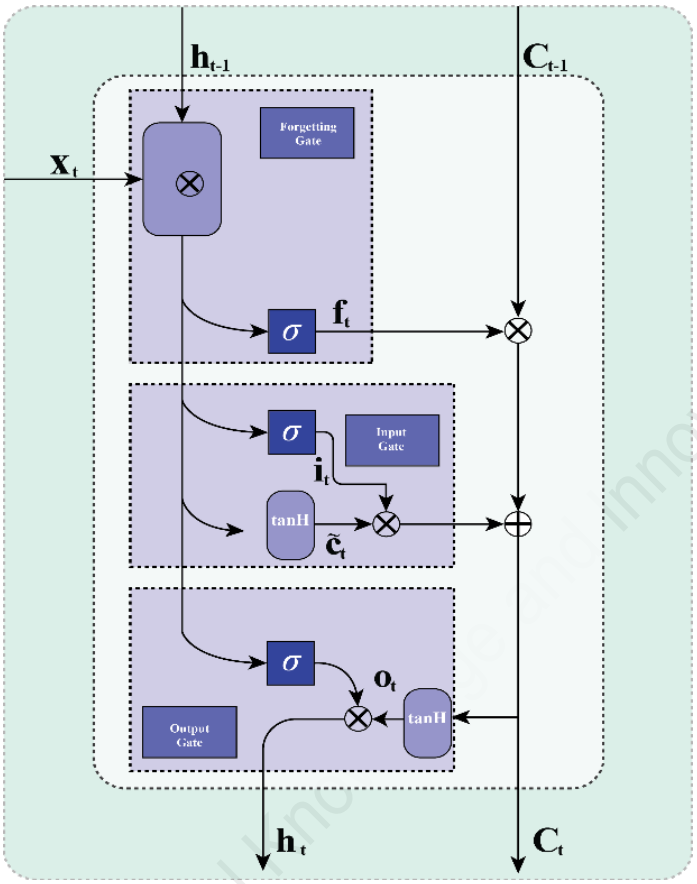


Fig. 4-5 LSTM network model

For example there are h hidden sections, the input is $\boldsymbol{X_t}$, the present time step state is $\boldsymbol{H_t}$, the memory neuron is $\boldsymbol{C_t}$, the previous time step hidden state is $\boldsymbol{H_{t\text{-}1}}$, and the memory neuron is $\boldsymbol{C_{t\text{-}1}}$. The candidate neuron is $\tilde{\boldsymbol{C_t}}$. At the corresponding moment, the input gate is $\boldsymbol{I_t}$, the forget gate is $\boldsymbol{F_t}$, and the output gate is $\boldsymbol{O_t}$. The calculation process of LSTM is as follows [97]:

$$\boldsymbol{I_t} = \sigma(\boldsymbol{X_t W_{xi}} + \boldsymbol{H_{t\text{-}1} W_{hi}} + \boldsymbol{b_i}) \tag{4-15}$$

$$\boldsymbol{F_t} = \sigma(\boldsymbol{X_t W_{xf}} + \boldsymbol{H_{t\text{-}1} W_{hf}} + \boldsymbol{b_f}) \tag{4-16}$$

$$\boldsymbol{O_t} = \sigma(\boldsymbol{X_t W_{xo}} + \boldsymbol{H_{t\text{-}1} W_{ho}} + \boldsymbol{b_o}) \tag{4-18}$$

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

$$\tilde{C_t} = \tanh(X_t W_{xc} + H_{t-1} W_{hc} + b_c) \quad (4\text{-}19)$$

$$C_t = F_t \odot C_{t-1} + I_T \odot C_t \quad (4\text{-}20)$$

$$H_t = O_t \odot \tanh(C)_t \quad (4\text{-}21)$$

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

Where, W_{xi}、W_{xc}、W_{hi}、W_{hf}、W_{ho}、W_{hc},W_{xf}、W_{xo}、represent the relevant weight matrix of the input data X_t respectively, b_i、b_f、b_o、b_c are the connection bias terms respectively, and is the activation functions, ⊙ represent the multiplication of each element.

The inflow and outflow of information controlled by the forget gate and input gate of LSTM, thereby achieving more precise control of past memory information and current new data, thereby improving the effect of prediction tasks [102]. Specifically, when the output gate is near to 1, all memory info can be transferred to the prediction part, and when the output gate is close to 0, only the data in the memory cell is retained without updating the hidden state. This mechanism can effectively regulate the model's training process and improve its efficacy.

As mentioned before, in addition to detecting and locating attacked power grid data, accurate recovery of operating data is also crucial. The AE system can effectively decrease the dimensionality of data features, and the LSTM model can well mine the historical characteristics of time series data. Combining AE and LSTM models can deeply capture the spatiotemporal correlation of power grid operating data, thereby generating corrected data with the same distribution as the measured data, and using it to replace the detected false attack data, thereby achieving accurate recovery of the original data. The LSTM layer represented by formulas (4-15)-(4-21) is an alternative implementation of the traditional AE hidden layer encoding and decoding formula [95]. The designed AE-LSTM overall network model is shown in Fig. 4-6. The process for the defender to generate correction data based on this model is shown in Fig. 4-7, in which the residual detection is calculated as follows:

$$r(x^t)_i = \left\| x_i^t - f_d^{LSTM}\left(f_e^{LSTM}(x^t,\boldsymbol{\theta})_i,\tilde{\boldsymbol{\theta}}\right)_{\boldsymbol{d}} \right\|_2 \tag{4-22}$$

Where, f_d^{LSTM}, f_e^{LSTM} represents the encoding and decoding nonlinear functions of AE-LSTM respectively [94][95]. If the residual error generated by the corrected data is lesser comparing the set threshold, the data correction that is considered successful. Thereafter, recovery data can be generated by replacing the false attack data at the conforming spatiotemporal location along with the generated correction data.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

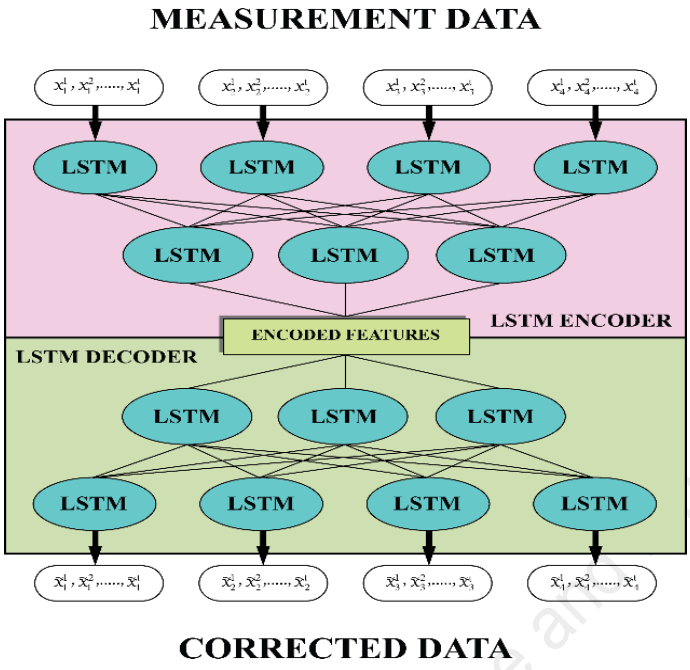
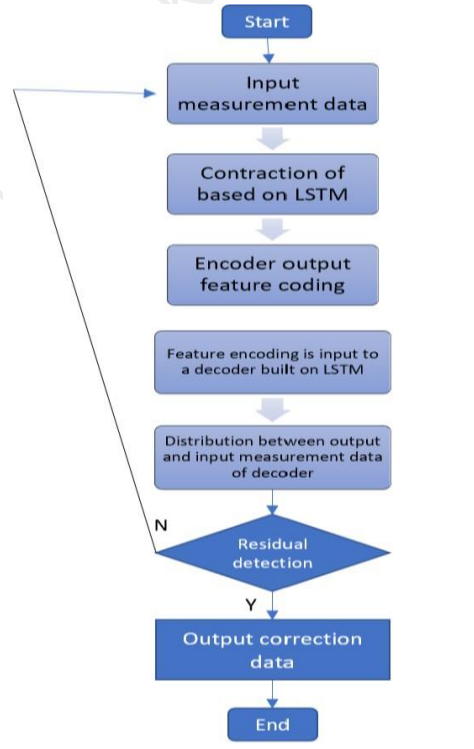


Fig. 4-6 AE-LSTM network model



Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

Fig. 4-7 AE-LSTM Generate revised data flow diagram

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

4.3 Summary

This chapter explores the complexities of neural networks, with particular attention to the two models that have transformed machine learning: recurrent neural networks (RNNs) and convolutional neural networks (CNNs). RNNs are decent at processing sequential input like voice and language, while CNNs are decent at jobs like object detection and image categorization. After examining their designs and essential elements that allow them to recognize intricate patterns in data, such as hidden states in RNNs and convolutional layers in CNNs.

We also present the integration of the self-attention (SA) mechanism into deep convolutional neural networks (DCNNs), which is a cognitive skill that resembles human attention. With SA, the network performs better at tasks like fake data injection attack (FDIA) detection and power system location by capturing long-distance relationships in sequences.

Here, also touch on the application of LSTM networks and auto-encoders (AE) to FDIA data recovery. While AE-LSTM assists in retrieving the original data by producing corrected data with the same distribution pattern as the input, AE assists in identifying fraudulent data. To reduce the remaining discrepancy between the input data and output data and essentially restore normal data, this method entails encoding and decoding the input data.

Overall, this chapter shows how neural networks may be harnessed to learn intricate forms from data and to solve practical issues like data recovery in power systems and FDIA detection. These networks' capabilities are further enhanced by the combination of SA and LSTM, which makes them useful instruments for guaranteeing the dependability and security of power systems.

Operational Implications:

FDIA can severely disrupt the normal operations of smart grids. By manipulating energy demand and supply data, attackers can cause inefficient energy routing and imbalances within the grid. For instance, erroneous demand-side information may force the grid to reroute energy unnecessarily, overloading certain areas. Conversely, supply-side attacks might misrepresent available capacity, leading to improper energy distribution. These operational inefficiencies not only increase transmission costs but also compromise overall system reliability. Furthermore, these disruptions can lead to increased wear and tear on infrastructure, requiring more frequent maintenance and potentially shortening the lifespan of critical components.

The necessity for robust systems to identify and mitigate FDIAs is crucial to maintain seamless smart grid operations. Real-time monitoring and advanced analytics can help in early detection and response to such anomalies. It is also vital to implement automated control systems that can dynamically respond to perceived risks. By integrating machine learning and artificial intelligence, smart grids can adapt to become more resilient against such sophisticated threats. This proactive strategy not only supports in preserving operational integrity but also increases the grid's capacity to recover fast from any interruptions produced by FDIA.

Economic Consequences:

The economic impact of FDIA extends to both individual consumers and the broader market. Attackers can exploit real-time pricing mechanisms to gain financial benefits at the expense of utility companies and other consumers. For example, manipulating energy demand statistics can reduce the attacker’s electricity bill while increasing costs for others, thus undermining market stability and fairness. The resultant financial losses and increased operational costs necessitate higher investments from utility providers to manage these

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

inefficiencies. This can lead to higher consumer expenses as utility providers pass on these costs.

Moreover, the uncertainty introduced by FDIA can deter investment in smart grid technologies. Potential investors may view the smart grid as a high-risk venture, slowing down the deployment of advanced technologies that could otherwise improve grid efficiency and sustainability. The economic repercussions also extend to the macroeconomic level, where the stability and reliability of the energy supply are crucial for industrial productivity and economic growth. A compromised smart grid can lead to increased operational costs, which, in turn, can drive up energy prices, affecting the competitiveness of industries relying on stable and affordable energy.

Security and Reliability Threats:

FDIA postures critical threats to the security and reliability of all kind of smart grids. These attacks can compromise state estimation processes, leading to inaccurate assessments of the grid's condition. As a result, grid operators may struggle to make informed decisions, potentially causing inappropriate operational responses and further destabilizing the grid. Advanced FDIAs can bypass traditional detection mechanisms, aligning injected errors with operational data to avoid detection. This underscores the necessity for effective detection and extenuation methods to ensure the security of the grids.

The growing complexity of smart-grid infrastructure, along with its integration for distributing energy resources, IoT devices, and advanced metering infrastructure, expands the attack surface for cyber threats. Ensuring robust cybersecurity measures involves not only the deployment of advanced detection algorithms but also the implementation of stringent access controls, continuous monitoring, and regular security audits. Additionally, building a culture of cybersecurity awareness among all stakeholders, including utility personnel and consumers, is crucial. Education and training programs can help in recognizing potential threats and responding effectively.

Vulnerability of Smart Grids:

Smart grids are particularly susceptible to FDIAs because of their reliance on digital communication and data collection processes. Attackers can exploit vulnerabilities in these processes, causing widespread disruptions and inefficiencies. Sophisticated attack systems, for example Principal Component Analysis (PCA) and Kernel Independent Component Analysis (KICA), enable attackers to create undetectable FDIAs even with limited knowledge of the grid's topology. The complexity of these threats makes detection and mitigation more challenging.

Furthermore, the decentralized nature of smart grids, with multiple entry points for data collection and transmission, increases the potential for security breaches. Ensuring end-to-end security across all components of the grid is paramount. This includes securing communication channels, protecting data integrity, and ensuring the reliability of sensor data. Adopting a multi-layered security approach, which combines physical security measures with advanced cybersecurity protocols, can help in mitigating these vulnerabilities. Frequent penetration tests and vulnerability assessments are also necessary to find possible vulnerabilities and fix them before attackers can exploit them.

Impact on Dynamic Microgrid Partitioning:

FDIA can significantly disrupt dynamic microgrid partitioning, essential for optimizing energy distribution within smart grids. Manipulated data can lead to inefficient microgrid segmentation, affecting the reliability and efficiency of energy distribution. This can result in operational failures, particularly during peak demand periods, leading to widespread blackouts or brownouts. Ensuring accurate data for dynamic partitioning is crucial for maintaining grid stability and efficiency.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

The ability to dynamically partition the grid into microgrids allows for localized management of energy sources, improving resilience and dropping the influence of large-scale disruptions. However, FDIAs targeting this capability can severely undermine its effectiveness. By injecting false data, attackers can cause misallocation of resources, leading to either underutilization or overloading of certain segments of the grid. This not only distresses the immediate operation of the smart grid but can also have long-term implications for infrastructure planning and investment. Ensuring robust validation and verification processes for data used in dynamic partitioning is essential to safeguard against such attacks.

Systemic Risks:

The interconnected nature of smart grids means that a localized FDIA can have widespread effects. Disruptions in one part of the grid can cascade to other parts, affecting overall grid stability and performance. This interconnectedness can amplify the impact of FDIA, turning localized issues into major grid-wide problems. Ensuring the reliability and efficiency of smart grids requires comprehensive security strategies to detect and mitigate FDIA, safeguarding the grid's operational integrity and economic stability.

The systemic risks posed by FDIA are further exacerbated by the growing complexity of the energy ecosystem, which includes not only traditional power generation and distribution but also renewable sources, electric automobiles, and smart appliances. The incorporation of these diverse elements increases the potential for cascading failures and complicates the task of maintaining grid stability. To address these challenges, a holistic strategy for grid management is required, one that encompasses both preventive measures and rapid response strategies. This includes developing advanced analytics for real-time monitoring, deploying automated response systems, and fostering collaboration among different stakeholders to ensure a coordinated and effective response to any incidents.

Chapter 6 Conclusion & Future Outlook

6.1 Conclusion

With widely investigation, this study has thoroughly examined the critical issue of False Data Injection Attacks (FDIA) on smart grids, analyzing various attack models and their impacts. The research has demonstrated the vulnerabilities of smart grids to FDIAs and highlighted the importance of enhancing their security. By developing an advanced neural network-based framework for detecting, localizing, and recovering tampered data, the study delivers a robust solution to alleviate the effects of these attacks.

The proposed model utilizes deep convolutional neural networks with self-attention mechanisms and autoencoders equipped with long- and short-term memory networks. This approach has shown significant improvements in identifying and countering FDIA, ensuring the resilience of smart grid operations. The findings emphasize that FDIAs can disrupt grid functionality, leading to operational inefficiencies, economic losses, and compromised reliability. The study's contributions offer a promising direction for enhancing smart grid security against such sophisticated cyber threats.

6.2 Future Outlook

As smart grid technology evolves, driven by advancements in information and communication technologies, securing these grids will become increasingly vital. Future research and development in this area should focus on several key directions:

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

1. **Enhanced Detection Mechanisms**:

Improving the accuracy and speed of FDIA detection systems using progressive machine learning algorithms like federated learning and sophisticated neural network architectures.

2. **Integration of Emerging Technologies**:

Leveraging technologies such as block-chain for secure data transactions and quantum computing for advanced encryption to add additional layers of security.

3. **Adaptive Security Strategies**:

Developing real-time monitoring systems capable of dynamically adjusting defense mechanisms based on detected threats to maintain grid security.

4. **Interdisciplinary Research**:

Encouraging interdisciplinary research combining expertise from electrical engineering, computer science, and cybersecurity to develop innovative solutions for smart grid security.

5. **Global Collaboration**:

Fostering international collaboration to share knowledge, best practices, and threat intelligence, building a more resilient global smart grid infrastructure.

By pursuing these directions, future research can significantly increase the safety and resilience of smart grids, ensuring their reliability as a component of this contemporary energy structure. The ongoing development of smart grids presents both opportunities and challenges, and addressing these challenges through innovative security solutions will be key to their successful implementation and operation.

Acknowledgement

Words cannot explain within these few words that my thankfulness to my mentor S M SOJIB AHAMED sir for his invaluable guidance, support, patience and feedback. Since the start of my academic journey at this university, I would like to extend my cordial thanks to the instructors who have imparted knowledge to me. Their guidance will enable me to grow up more in the future. Lastly, I'd like to mention my parents and partner who never give up on me and belief in me.
And always give me emotional support.

References

[1] Liu, Y., Ning, P., & Kundur, P. (2009). False data injection attacks in power systems. In 2009 IEEE Power & Energy Society General Meeting (pp. 1-8). IEEE.
[2] He, Youbiao, Gihan J. Mendis, and Jin Wei. "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism." IEEE Transactions on Smart Grid 8.5 (2017): 2505-2516.
[3] Lin, Jie, et al. "On false data injection attacks against distributed energy routing in smart grid." 2012

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

IEEE/ACM Third International Conference on Cyber-Physical Systems. IEEE, 2012.
[4] Tufail, Shahid, Shanzeh Batool, and Arif I. Sarwat. "False data injection impact analysis in ai- based smart grid." SoutheastCon 2021. IEEE, 2021.
[5] Zhang, Ying, Jianhui Wang, and Bo Chen. "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach." IEEE Transactions on Smart Grid 12.1 (2020): 623-634.
[6] Yu, Wei, et al. "An integrated detection system against false data injection attacks in the smart grid." Security and Communication Networks 8.2 (2015): 91-109.
[7] Xu, Ruzhi, et al. "Achieving efficient detection against false data injection attacks in smart grid." IEEE Access 5 (2017): 13787-13798.
[8] Chen, Po-Yu, et al. "Detection of false data injection attacks in smart-grid systems." IEEE Communications Magazine 53.2 (2015): 206-213.
[9] Niu, Xiangyu, et al. "Dynamic detection of false data injection attack in smart grid using deep learning." 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). IEEE, 2019.
[10] Tran, Nam N., et al. "Designing constraint-based false data-injection attacks against the unbalanced distribution smart grids." IEEE Internet of Things Journal 8.11 (2021): 9422-9435.
[11] Habib, AKM Ahasan, et al. "False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction." Computers and Electrical Engineering 107 (2023): 108638.
[12] Pei, Chao, et al. "A deviation-based detection method against false data injection attacks in smart grid." IEEE access 9 (2021): 15499-15509.
[13] Ayad, Abdelrahman, et al. "Detection of false data injection attacks in smart grids using recurrent neural networks." 2018 IEEE power & energy society innovative smart grid technologies conference (ISGT). IEEE, 2018.
[14] Drayer, Elisabeth, and Tirza Routtenberg. "Detection of false data injection attacks in smart grids based on graph signal processing." IEEE Systems Journal 14.2 (2019): 1886-1896.
[15] Dehghani, Moslem, et al. "Fourier singular values-based false data injection attack detection in AC smart-grids." Applied Sciences 11.12 (2021): 5706.
[16] Youssef, El-Nasser S., and Fabrice Labeau. "False data injection attacks against state estimation in smart grids: Challenges and opportunities." 2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE). IEEE, 2018.
[17] Anwar, Adnan, and Abdun Naser Mahmood. "Vulnerabilities of smart grid state estimation against false data injection attack." Renewable energy integration: challenges and solutions (2014): 411-428.
[18] Wang, Yi, et al. "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids." IEEE Access 5 (2017): 26022-26033.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

[19] Nath, Samrat, et al. "Quickest detection of false data injection attacks in smart grid with dynamic models." IEEE Journal of Emerging and Selected Topics in Power Electronics 10.1 (2019): 1292-1302.
[20] Li, Yang, et al. "Detection of false data injection attacks in smart grid: A secure federated deep learning approach." IEEE Transactions on Smart Grid 13.6 (2022): 4862-4872
[21] Rahman, Moshfeka, Yuanliang Li, and Jun Yan. "Multi-objective evolutionary optimization for worst-case analysis of false data injection attacks in the smart grid." 2020 IEEE Congress on Evolutionary Computation (CEC). IEEE, 2020.
[22] Dayaratne, Thusitha, et al. "High impact false data injection attack against real-time pricing in smart grids." 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe). IEEE, 2019.
[23] Musleh, Ahmed S., et al. "Detection of false data injection attacks in smart grids: A real-time principle component analysis." IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society. Vol. 1. IEEE, 2019.
[24] Li, Beibei, et al. "Detection of false data injection attacks on smart grids: A resilience-enhanced scheme." IEEE Transactions on Power Systems 37.4 (2021): 2679-2692.
[25] Iqbal, Maryam, and Mohammad Ayman Iqbal. "Attacks due to false data injection in smart grids: Detection & protection." 2019 1st Global Power, Energy and Communication Conference (GPECOM). IEEE, 2019.
[26] Smart Grid Simulation Optimizes Conventional, Renewable Energy Usage. (n.d.). MOSIMTEC. https://mosimtec.com/smart-grid-simulation/
[27] Liu, Yao, Peng Ning, and Michael K. Reiter. "False data injection attacks against state estimation in electric power grids." *ACM Transactions on Information and System Security (TISSEC)* 14.1 (2011): 1-33.
[28] Liang, Gaoqi, et al. "A review of false data injection attacks against modern power systems." *IEEE Transactions on Smart Grid* 8.4 (2016): 1630-1638.
[29] Wang, Qi, et al. "A two-layer game theoretical attack-defense model for a false data injection attack against power systems." *International Journal of Electrical Power & Energy Systems* 104 (2019): 169-177.
[30] Gungor, V. Cagri, et al. "A survey on smart grid potential applications and communication requirements." *IEEE Transactions on industrial informatics* 9.1 (2012): 28-42.
[31] Rahman, Md Ashfaqur, and Hamed Mohsenian-Rad. "False data injection attacks with incomplete information against smart power grids." *2012 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2012.
[32] Anwar, Adnan, Abdun Naser Mahmood, and Mark Pickering. "Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements." *Journal of Computer and System Sciences* 83.1 (2017): 58-72.
[33] Yuan, Yanling, Zuyi Li, and Kui Ren. "Modeling load redistribution attacks in power systems." *IEEE Transactions on Smart Grid* 2.2 (2011): 382-390.
[34] Anwar, Adnan, and Abdun Naser Mahmood. "Stealthy and blind false injection attacks on SCADA EMS in the presence of gross errors." *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 2016.
[35] Sun, Ying, et al. "False data injection attacks with local topology information against linear state estimation." *2015 IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA)*. IEEE, 2015.
[36] Liu, Xuan, et al. "Modeling of local false data injection attacks with reduced network information." *IEEE Transactions on Smart Grid* 6.4 (2015): 1686-1696.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

[37] Hug, Gabriela, and Joseph Andrew Giampapa. "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks." *IEEE Transactions on smart grid* 3.3 (2012): 1362-1370.
[38] Rahman, Md Ashfaqur, and Hamed Mohsenian-Rad. "False data injection attacks against nonlinear state estimation in smart power grids." *2013 IEEE Power & Energy Society General Meeting*. IEEE, 2013.
[39] Liu, Xuan, and Zuyi Li. "False data attacks against AC state estimation with incomplete network information." *IEEE Transactions on smart grid* 8.5 (2016): 2239-2248.
[40] Liang, Jingwen, Oliver Kosut, and Lalitha Sankar. "Cyber attacks on AC state estimation: Unobservability and physical consequences." *2014 IEEE PES General Meeting| Conference & Exposition*. IEEE, 2014.
[41] Liang, Jingwen, Lalitha Sankar, and Oliver Kosut. "Vulnerability analysis and consequences of false data injection attack on power system state estimation." *IEEE Transactions on Power Systems* 31.5 (2015): 3864-3872.
[42] Tran, Nam N., et al. "Designing false data injection attacks penetrating AC-based bad data detection system and FDI dataset generation." *Concurrency and Computation: Practice and Experience* 34.7 (2022): e5956.
[43] Song, Yufei, et al. "Intelligent data attacks against power systems using incomplete network information: a review." *Journal of Modern Power Systems and Clean Energy* 6.4 (2018): 630- 641.
[44] Yu, Zong-Han, and Wen-Long Chin. "Blind false data injection attack using PCA approximation method in smart grid." *IEEE Transactions on Smart Grid* 6.3 (2015): 1219- 1226.
[45] Kang, Jeong-Won, Il-Young Joo, and Dae-Hyun Choi. "False data injection attacks on contingency analysis: Attack strategies and impact assessment." *IEEE Access* 6 (2018): 8841- 8851.
[46] Chen, Jiongcong, et al. "Impact analysis of false data injection attacks on power system static security assessment." *Journal of Modern Power Systems and Clean Energy* 4.3 (2016): 496- 505.
[47] Kosut, Oliver, et al. "Limiting false data attacks on power system state estimation." *2010 44th Annual Conference on Information Sciences and Systems (CISS)*. IEEE, 2010.
[48] Kosut, Oliver, et al. "Malicious data attacks on the smart grid." *IEEE Transactions on Smart Grid* 2.4 (2011): 645-658.
[49] Kim, Tung T., and H. Vincent Poor. "Strategic protection against data injection attacks on power grids." *IEEE Transactions on Smart Grid* 2.2 (2011): 326-333.
[50] Tan, Rui, et al. "Modeling and mitigating impact of false data injection attacks on automatic generation control." *IEEE Transactions on Information Forensics and Security* 12.7 (2017): 1609-1624.
[51] Kim, Jinsub, and Lang Tong. "On topology attack of a smart grid: Undetectable attacks and countermeasures." *IEEE Journal on Selected Areas in Communications* 31.7 (2013): 1294- 1305.
[52] Deng, Ruilong, and Hao Liang. "False data injection attacks with limited susceptance information and new countermeasures in smart grid." *IEEE Transactions on Industrial Informatics* 15.3 (2018): 1619-1628.
[53] Zhang, Xialei, et al. "On false data injection attacks against the dynamic microgrid partition in the smart grid." *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

[54] Hao, Jianye, et al. "An adaptive Markov strategy for defending smart grid false data injection from malicious attackers." *IEEE Transactions on Smart Grid* 9.4 (2016): 2398-2408.
[55] Ozay, Mete, et al. "Distributed models for sparse attack construction and state vector estimation in the smart grid." *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2012.
[56] Tajer, Ali, et al. "Distributed joint cyber attack detection and state recovery in smart grids." *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2011.
[57] Li, Yuzhe, Dawei Shi, and Tongwen Chen. "False data injection attacks on networked control systems: A Stackelberg game analysis." *IEEE Transactions on Automatic Control* 63.10 (2018): 3503-3509.
[58] Li, Yuancheng, and Yuanyuan Wang. "False data injection attacks with incomplete network topology information in smart grid." *IEEE Access* 7 (2018): 3656-3664.
[59] Li, Zhiyi, et al. "Bilevel model for analyzing coordinated cyber-physical attacks on power systems." *IEEE Transactions on Smart Grid* 7.5 (2015): 2260-2272.
[60] Liu, Xuan, et al. "Masking transmission line outages via false data injection attacks." *IEEE Transactions on Information Forensics and Security* 11.7 (2016): 1592-1602.
[61] Liu, Xuan, and Zuyi Li. "Trilevel modeling of cyber attacks on transmission lines." *IEEE Transactions on Smart Grid* 8.2 (2015): 720-729.
[62] Xiang, Yingmeng, et al. "Coordinated attacks against power grids: Load redistribution attack coordinating with generator and line attacks." *2015 IEEE Power & Energy Society General Meeting*. IEEE, 2015.
[63] Yuan, Yanling, Zuyi Li, and Kui Ren. "Quantitative analysis of load redistribution attacks in power systems." *IEEE Transactions on Parallel and Distributed Systems* 23.9 (2012): 1731- 1738.
[64] Liu, Xuan, and Zuyi Li. "Local load redistribution attacks in power systems with incomplete network information." *IEEE Transactions on Smart Grid* 5.4 (2014): 1665-1676.
[65] Che, Liang, et al. "Cyber cascades screening considering the impacts of false data injection attacks." *IEEE Transactions on Power Systems* 33.6 (2018): 6545-6556.
[66] Liu, Xuan, and Zuyi Li. "Local topology attacks in smart grids." *IEEE Transactions on Smart Grid* 8.6 (2016): 2617-2626.
[67] Esmalifalak, Mohammad, et al. "A stealthy attack against electricity market using independent component analysis." *IEEE Systems Journal* 12.1 (2015): 297-307.
[68] Anwar, Adnan, Abdun Naser Mahmood, and Mark Pickering. "Data-driven stealthy injection attacks on smart grid with incomplete measurements." *Intelligence and Security Informatics: 11th Pacific Asia Workshop. PAISI 2016, Auckland, New Zealand, April 19, 2016, Proceedings 11*. Springer International Publishing, 2016.
[69] Lin, Jie, et al. "On false data injection attacks against distributed energy routing in smart grid." *2012 IEEE/ACM Third International Conference on Cyber-Physical Systems*. IEEE, 2012.
[70] Oja, Erkki, et al. "Independent component analysis and blind source separation." *Helsinki Univ. Technol., Espoo, Finland, Tech. Rep* (2003).
[71] Viberg, Mats, and Bjorn Ottersten. "Sensor array processing based on subspace fitting." *IEEE Transactions on signal processing* 39.5 (1991): 1110-1121.
[72] Abdi, Hervé, and Lynne J. Williams. "Principal component analysis." *Wiley interdisciplinary reviews: computational statistics* 2.4 (2010): 433-459.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

[73] Liu, Lanchao, et al. "Detecting false data injection attacks on power grid by sparse optimization." *IEEE Transactions on Smart Grid* 5.2 (2014): 612-621.
[74] Liang, Gaoqi, et al. "Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism." *IEEE Transactions on Smart Grid* 9.4 (2017): 3820-3829.
[75] Ashok, Aditya, et al. "Experimental evaluation of cyber attacks on automatic generation control using a CPS security testbed." *2015 IEEE Power & Energy Society General Meeting*. IEEE, 2015.
[76] Sridhar, Siddharth, and Manimaran Govindarasu. "Model-based attack detection and mitigation for automatic generation control." *IEEE Transactions on Smart Grid* 5.2 (2014): 580-591.
[77] Khalaf, Mohsen, Amr Youssef, and Ehab El-Saadany. "Joint detection and mitigation of false data injection attacks in AGC systems." *IEEE Transactions on Smart Grid* 10.5 (2018): 4985- 4995.
[78] Biswas, Saroj, and Arif Sarwat. "Vulnerabilities in two-area automatic generation control systems under cyberattack." *2016 Resilience Week (RWS)*. IEEE, 2016.
[79] Rahman, Mohammad Ashiqur, et al. "Novel attacks against contingency analysis in power grids." *arXiv preprint arXiv:1911.00928* (2019).
[80] Sun, H. B., and B. M. Zhang. "Global state estimation for whole transmission and distribution networks." *Electric Power Systems Research* 74.2 (2005): 187-195.)
[81] Chin, Wen-Long, Chun-Hung Lee, and Tao Jiang. "Blind false data attacks against AC state estimation based on geometric approach in smart grid communications." *IEEE Transactions on Smart Grid* 9.6 (2017): 6298-6306.
[82] Tian, Jiwei, Buhong Wang, and Xia Li. "Data-driven and low-sparsity false data injection attacks in smart grid." *Security and Communication Networks* 2018 (2018).
[83] Memon, M. (2022, November 16). ANN vs CNN vs RNN: Neural Networks Guide. Levity. https://levity.ai/blog/neural-networks-cnn-ann-rnn
[84] LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. "Deep learning." *nature* 521.7553 (2015): 436-444.
[85] Goodfellow, Ian, Yoshua Bengio, and Aaron Courville. *Deep learning*. MIT press, 2016.
[86] Krizhevsky, Alex, Ilya Sutskever, and Geoffrey E. Hinton. "ImageNet classification with deep convolutional neural networks." *Communications of the ACM* 60.6 (2017): 84-90.
[87] Simonyan, Karen, and Andrew Zisserman. "Very deep convolutional networks for large-scale image recognition." *arXiv preprint arXiv:1409.1556* (2014).
[88] Hochreiter, Sepp, and Jürgen Schmidhuber. "Long short-term memory." *Neural computation* 9.8 (1997): 1735-1780.
[89] 邱锡鹏. 神经网络与深度学习. 机械工业🎧版社, 2020.
[90] Corbetta, Maurizio, and Gordon L. Shulman. "Control of goal-directed and stimulus-driven attention in the brain." *Nature reviews neuroscience* 3.3 (2002): 201-215.
[91] Niu, Zhaoyang, Guoqiang Zhong, and Hui Yu. "A review on the attention mechanism of deep learning." *Neurocomputing* 452 (2021): 48-62.
[92] Cordonnier, Jean-Baptiste, Andreas Loukas, and Martin Jaggi. "On the relationship between self-attention and convolutional layers." *arXiv preprint arXiv:1911.03584* (2019).
[93] Musleh, Ahmed S., et al. "Attack detection in automatic generation control systems using LSTM-based stacked autoencoders." *IEEE Transactions on Industrial Informatics* 19.1 (2022): 153-165.
[94] Chen, Liang, et al. "Stacked autoencoder framework of false data injection attack detection in smart grid." *Mathematical Problems in Engineering* 2021 (2021): 1-8.

Journal of Global Knowledge and Innovation (JGKI), Volume 3, Issue 2, February-2025
ISSN 3079-1995
www.jgkijournal.com
DOI: https://doi.org/10.7910/DVN/D5XIZW

[95] Majidi, Seyed Hossein, Shahrzad Hadayeghparast, and Hadis Karimipour. "FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid." *International Journal of Critical Infrastructure Protection* 37 (2022): 100508.

[96] Wang, Shuoyao, Suzhi Bi, and Ying-Jun Angela Zhang. "Locational detection of the false data injection attack in a smart grid: A multilabel classification approach." *IEEE Internet of Things Journal* 7.9 (2020): 8218-8227.

[97] 陆继翔, et al. "基于 CNN-LSTM 混合神经网络模型的短期负荷预测方法." 电力系统自动化 43.8 (2019): 131-137.

[98] Bántay, László, and János Abonyi. "Machine Learning-Supported Designing of Human– Machine Interfaces." Applied Sciences, vol. 14, no. 4, 2024, p. 1564.

[99] IDC and CGI explore digital strategies helping utilities navigate the energy transition | CGI.com. https://www.cgi.com/en/article/energy-utilities/idc-cgi-explores-digital-strategies-for- navigating-the-energy-transition

[100] Du, Shiqiao, and Minoru Sakurai. "Multivariate Analysis of Properties of Amino Acid Residues in Proteins from a Viewpoint of Functional Site Prediction." Chemical Physics Letters, 2010, https://doi.org/10.1016/j.cplett.2010.02.006.

[101] Memiș, Erkut, et al. "Comparative Study for Sentiment Analysis of Financial Tweets with Deep Learning Methods." Applied Sciences, vol. 14, no. 2, 2024, p. 588.

[102] Yoon-Soo, Shin, and Junhee Kim. "Sensor Data Reconstruction for Dynamic Responses of Structures Using External Feedback of Recurrent Neural Network." Sensors, vol. 23, no. 5, 2023, p. 2737.

[103] Load Prediction of HVAC Systems using Deep Learning, DOI: 10.5281/zenodo.13134333

Received: 1 January 2025 **Published: 22 February 2025**