March 2024

Effects of Unobservable Bus States on Detection and Localization of False Data Injection Attacks in Smart Grids

Moheb Abdelmalak
University of South Florida

Effects of Unobservable Bus States on Detection and Localization of False Data Injection Attacks in Smart Grids

by

Moheb Abdelmalak

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science
Department of Electrical Engineering
College of Engineering
University of South Florida

Major Professor: Mia Naeini, Ph.D.
Ismail Uysal, Ph.D.
Nasir Ghani, Ph.D.

Date of Approval:
March 12, 2024

Keywords: State Estimation, PMU Placement, Machine Learning, Recurrent Neural Networks, Time Series

Dedication

To my beloved small family—Bebo, Fofo, and Caty—who surround me with love and support…

To my grandfather, Shehata, whose lessons continue to guide me and whose memory I hold dear…

Acknowledgments

First and foremost, my deepest gratitude goes to my thesis advisor, Dr. Mia Naeini, for her unparalleled patience, guidance, and dedication. Her ability to navigate calmly through my research, providing steady support and constructive feedback, has been invaluable. Dr. Naeini's exceptional commitment is evident in the generous amount of time she dedicates to supporting her students, always making herself available to address our concerns and guide us through challenges. This level of dedication, coupled with her patience, has not only facilitated my academic growth but also deeply influenced my approach to problem-solving and learning. Her unwavering support and the importance she places on being there for her students have influenced me tremendously. I am eternally grateful to work under her supervision.

I also wish to express my sincere thanks to Dr. Ismail Uysal, my TA supervisor. His teachings have extended beyond the academic realm, imparting lessons on professionalism, the importance of going the extra mile, and the value of humility and support. It has been an honor both to learn from and work alongside him.

Special thanks go to Dr. Nasir Ghani for his valuable insights and for serving on my thesis committee. His extensive experience in my field of study has greatly enriched this work.

I am also indebted to the faculty of the Department of Electrical Engineering, especially Dr. Yasin Yilmaz, for his generous sharing of knowledge, and Dr. Zhixin Miao, for his advice and support throughout my Master's journey.

Additionally, I would like to extend my gratitude to the members of Dr. Naeini's group: Hamed, for his considerable efforts and support throughout my learning journey; Naeem, Soumav,

and Reza. Despite the brevity of our time together, the knowledge and insights I gained from each of them during our group meetings and discussions have been invaluable.

My heartfelt appreciation extends to my friends in the United States who supported me at the beginning of my journey—Nader, Islam, Faisal, Abdulrahim, Abdulaziz, Verina, Nevine, Mark, Tony, Manal, and Ali, along with many others too numerous to mention—. Your support made navigating life in this new country possible.

Finally, I am profoundly thankful to the U.S. State Department and the Fulbright Student Program for the opportunity and experience they offered me to study at the University of South Florida.

And lastly, I am grateful to God, who has guided every step of my journey.

Table of Contents

List of Tables

List of Figures

Abstract

In an era increasingly marked by sophisticated cyber-attacks, this thesis investigates the critical issue of bus unobservability in smart grids and its impact on the effectiveness of cyber-attack detection and localization models. Given that unobservability is a prevalent challenge in smart grids due to various factors, researchers have developed numerous algorithms for optimal Phasor Measurement Unit (PMU) placement under scenarios of limited observability. However, these models primarily focus on enhancing network observability, often without considering whether this placement optimally facilitates attack detection. This research is driven by the hypothesis that a deeper understanding of the effects of unobservable buses can inform more effective PMU deployment strategies, thereby bolstering the grid's defenses against cyber-attacks.

The research is structured to first provide a comprehensive review of existing state estimation, detection, and localization models, emphasizing data-driven temporal analysis methods. It then delves into an in-depth experimental evaluation to assess how unobservability influences the accuracy and reliability of these models. The insights from these experiments are intended to inform utilities about the potential impacts of network unobservability on cyber-attack detection, contributing to a broader understanding that may support future PMU placement strategies.

The principal finding of this thesis is the identification of a direct correlation between the number of unobservable buses and the efficiency of attack detection and localization performance. As the count of unobservable buses escalates, there is a noticeable decline in the performance of both state estimation and detection and localization models. Accordingly, this study proposes an

estimated threshold for the number of PMUs required to maintain model effectiveness before a critical decline in performance occurs. Moreover, the research delineates that certain buses exert a more significant influence on detection and localization outcomes than others, suggesting that strategic placement of PMUs at these buses can enhance detection capabilities. Additionally, this thesis evaluates the efficacy of detection and localization models under various common PMU placement strategies, concluding that, despite an increase in system observability, these strategies may not optimally support attack detection. The impact of clustered unobservability on detection models is also explored, providing insights into how it affects model performance.

In summary, this thesis provides a focused examination of how bus unobservability impacts the detection and localization of cyber-attacks in smart grids. It highlights the importance of strategic PMU placement as a critical factor in enhancing grid security. This work underscores the necessity for ongoing research in the face of evolving cyber threats, aiming to safeguard critical energy infrastructure effectively.

Chapter 1: Introduction

1.1 The Revolution of Smart Grids

The transition towards smart grids marks a significant paradigm shift in the evolution of power systems, driven by the need to address modern challenges such as energy efficiency, reliability, and the seamless integration of renewable resources. Smart grids epitomize an advanced infrastructure that elevates control and monitoring capabilities through sophisticated digital technology, resulting in substantial improvements over traditional grids. In stark contrast to the latter, which are limited by unidirectional communication and static management, smart grids are characterized by their dynamic bidirectional energy flows and the proactive engagement of consumers in both energy production and consumption. This transformative shift is essential for the effective incorporation of distributed energy resources, including renewables, thus enhancing the grid's resilience to outages and cyber-attacks. The intrinsic value of smart grids is amplified by their flexibility to accommodate diverse power source structures, significantly reducing the likelihood of widespread blackouts and augmenting the overall economic efficiency of power supply by curtailing costs, minimizing energy consumption, and decreasing emissions [1-2].

For instance, the smart grid encompasses a variety of components as illustrated in Figure 1.1. Moving beyond the traditional linear system of generation, transmission, and distribution to the end-user, the smart grid paradigm introduces bidirectional power flow, integrating an array of Distributed Energy Resources (DERs), microgrids, and electric vehicles. It empowers utilities to monitor and manage the system with greater efficiency, thereby reducing energy waste and enhancing economic value through initiatives like demand response programs. This complex

system is underpinned by a robust communication network, essential for coordinating the diverse elements within the smart grid architecture and ensuring optimal performance. Such a sophisticated communication system results in introducing new threats and challenges in smart grids [3].

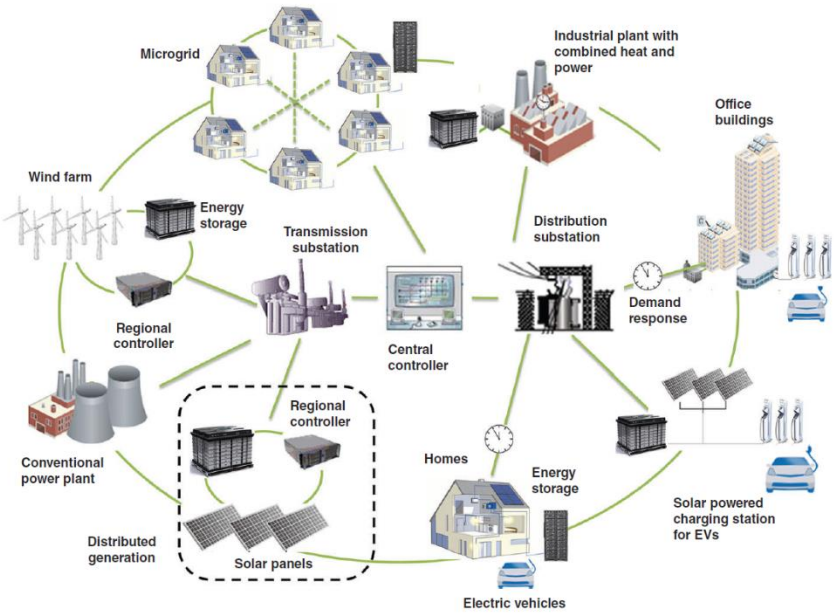

Figure 1.1 Smart grid components. From "Smart grid governance: An international review of evolving policy issues and innovations," by M.A. Brown, S. Zhou, & M. Ahmadi, 2018, WIREs Energy and Environment, e290. Used with permission [3].

1.2 Monitoring and Situational Awareness in Smart Grids

1.2.1 Monitoring the Smart Grid

In smart grids, the convergence of advanced communication technologies, such as wireless networks, fiber optics, and Internet Protocols (IP), with critical infrastructure components like sensors, smart meters, and PMUs forms the backbone for efficient, reliable, and secure electricity management. This integration facilitates two-way communication between the grid's operational components and the control center, enabling real-time data exchange and control actions. Advanced Metering Infrastructure (AMI) and Supervisory Control and Data Acquisition

(SCADA) systems play pivotal roles in collecting and managing data, respectively. AMI offers detailed monitoring of energy usage at the consumer level, while SCADA ensures centralized control over the grid's operational components. This seamless data flow from generation sources to data centers, supported by a robust communication framework, is crucial for optimizing grid performance, integrating distributed energy resources, and enhancing resilience against disruptions, thereby ensuring the grid's overall responsiveness and resilience.

Figure 1.2 illustrates the intricate mesh of communication and physical systems within the smart grid [4]. On the customer end, Smart Meters equipped with AMI enable detailed usage monitoring. The transmission and generation sectors utilize PMUs and Remote Terminal Units (RTUs) to ensure connectivity of transmission devices. Centralized monitoring and control are achieved through systems such as SCADA, ADMS (Advanced Distribution Management System), EMS (Energy Management Systems), and DERMS (Distributed Energy Resources Management Systems) housed within the control center. These systems work in concert to optimize grid

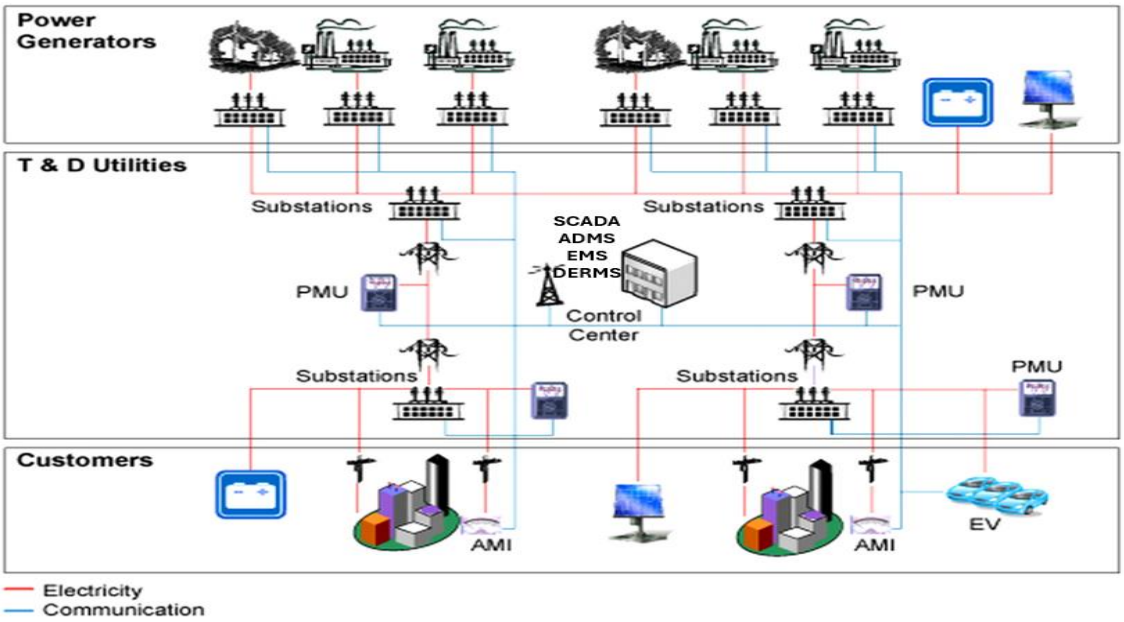

Figure 1.2 Physical and communication layers in smart grids. From “A survey on smart metering and smart grid communication,” by Y. Kabalci, 2016, Energy Reviews, 57, pp. 302–318. Used with permission [4].

performance and reliability, providing a comprehensive overview and real-time management capabilities across the smart grid.

1.2.2 Wide Area Situational Awareness and the Issue of Unobservability

As the smart grid becomes more and more equipped with robust communication layers, Wide-Area Situational Awareness (WASA) in smart grids is becoming essential for real-time system monitoring and management. WASA's effectiveness is heavily dependent on the observability of the network, which is challenged by several factors. The cost considerations for the implementation of PMUs in smart grids cannot be overlooked. While PMUs are fundamental to enhancing WASA and achieving network observability, the financial burden they impose is significant. The expenses extend beyond the PMU devices themselves to include the cost of Phasor Data Concentrators (PDCs), the necessary communication infrastructure, the modernization of older substations to ensure compatibility, and the management of the resulting big data. These economic factors make widespread PMU deployment a challenging proposition, despite the potential benefits for smart grid monitoring and management [5]. However, even equipping a system fully with PMUs does not guarantee complete observability. Studies indicate that approximately 10 to 17% of PMUs installed in North America experience quality problems that could lead to conditions of unobservability due to data loss. These quality issues often stem from hardware failures, communication congestion, and delays or losses in data transmission [6]. Moreover, the grid's partial unobservability can also result from cybersecurity threats, such as Denial of Service (DoS) attacks. A DoS attack disrupts service by overwhelming the network with traffic or sending information that triggers a crash, thereby blocking legitimate network traffic and potentially leading to data unavailability from PMUs [7]. These reasons for unobservability present significant hurdles in maintaining the operational security and reliability of smart grids,

emphasizing the need for innovative solutions to enhance WASA capabilities; thus, increasing the reliability and security of the smart grids' operation.

1.2.3 PMU Optimum Placement to Maximize Observability

To address the challenge of observability, the strategic placement of PMUs becomes critical. The optimum placement of these units is a complex problem that seeks to achieve maximum observability with the minimum number of PMUs, considering the constraints of budget, network topology, and the criticality of certain grid sections. Various algorithms and optimization techniques have been developed to identify the key locations where PMUs should be installed to ensure comprehensive monitoring and support the efficient operation of the grid by improving the state estimation of the system [8]. The techniques utilized for optimizing PMU placement have been widely reviewed in the literature [5,9]. This research will further examine some of these techniques in Section 2.4.

1.2.4 Power System State Estimation

State estimation is a vital process in smart grid management, compensating for the inherent issue of unobservability by estimating the grid's state vectors, such as voltages and phase angles, from the available measurements. This mathematical process uses algorithms to provide the most probable snapshot of the grid's status, incorporating measurements from PMUs and other devices. State estimation enables grid operators to make informed decisions, optimize power flow, and enhance system stability by offering insights into the parts of the network that are not directly observable. It plays a crucial role in ensuring the reliability and security of the smart grid, particularly in the detection and localization of cybersecurity threats [10]. State estimation techniques range from traditional approaches to modern, data-driven methods, all of which have been extensively reviewed in the literature [11,12,13,14]. Section 2.2 will explore a range of

established traditional methods alongside some of the data-driven approaches that have been developed to address SE challenges.

1.3 Overview of Cyber-Physical Attacks on Smart Grids

The smart grid's increased connectivity and complexity have exposed it to cyber threats, a vulnerability that has been exploited in various attacks over the years. The first documented cyber-physical attack occurred in 1982, targeting pipeline control software in the Siberian wilderness, resulting in a massive explosion due to manipulated valve controls. In 2003, the Slammer worm disrupted the SCADA systems at the Davis-Besse nuclear power plant. A more sophisticated example was the Stuxnet worm in 2010, which targeted Iranian nuclear facilities, manipulating the SCADA systems to cause physical damage to uranium enrichment centrifuges [15].

The most well-known incident in the context of power systems was the 2015 cyberattack on Ukrainian power distribution companies, where a highly coordinated cyber-attack targeted the Ukrainian power grid, leading to extensive service outages that affected 225,000 customers and exemplifying the vulnerability of smart grids to sophisticated threats. The attackers demonstrated comprehensive capabilities, from initial spear-phishing campaigns to deploying variants of the BlackEnergy 3 malware, to gain entry into the information technology networks of the electricity companies. Once inside, they exhibited a deep understanding of both IT and operational technology environments, including the manipulation of Uninterruptible Power Supplies (UPS) and Human Machine Interfaces (HMI). Their actions culminated in the manual opening of breakers through SCADA systems, resulting in widespread and prolonged blackouts across multiple regions. The attack was further compounded by a simultaneous telephonic denial-of-service that overwhelmed the energy company's call center, preventing customers from reporting the outages and exacerbating the situation. The incident not only disrupted the immediate power supply but

also highlighted the potential long-term implications for smart grid security, emphasizing the need for robust protective strategies against such multi-vector cyber threats [16][17].

Further incidents of varying sophistication have since been documented, such as the Aurora generator attack, where hypothetical attackers desynchronized a generator from the grid by manipulating circuit breakers, potentially causing significant physical damage. Pricing attacks on smart grids have also been reported, where attackers manipulate price signals to create mismatches between generated and consumed power, leading to economic losses and power quality issues [15].

Furthermore, False Data Injection Attacks (FDIA) represent a broad category of cyber threats where attackers manipulate input data to deceive and disrupt system operations. By altering the information processed by systems, FDIA can compromise various functions across different sectors. In the context of power systems, these attacks are particularly concerning as they can mislead operational and control mechanisms. This misguidance may result in unstable system conditions or even precipitate a complete system collapse, especially when critical functions such as state estimation are targeted.

Blind FDI attacks have emerged, where attackers, without explicit knowledge of the power grid's topology, use statistical methods to craft stealthy attack vectors that can go undetected while causing significant harm. Moreover, Load Redistribution (LR) attacks have been designed to manipulate load and line power flow measurements to create conditions for system overload and cascading failures [18].

Additionally, topology attacks - that are examples of FDIA- have been developed by manipulating the estimated topology state, such as switch and breaker states, to cause incorrect system operation. These historical incidents underscore the evolving landscape of cyber threats targeting smart grids and highlight the ongoing challenge of safeguarding critical infrastructure

against such malicious activities. Owing to the diverse nature of these attacks and the significant economic losses they can incur; numerous research initiatives have been undertaken to develop robust models aimed at detecting these threats which will be discussed further in Section 2.2.

1.4 Research Motivation and Questions

As delineated in preceding sections, cyber-attacks pose a significant threat, potentially leading to substantial economic and operational repercussions. Consequently, the development of detection models capable of identifying these threats is of paramount importance for researchers and engineers. Given the inherent nature of power grids, which include unobservable points due to the challenges outlined in Section 1.2, these detection models must be adept at navigating partially unobservable networks. However, while addressing the Optimal PMU Placement (OPP) challenge, the aspect of cyber-attack detection is often overlooked, with the primary focus being on enhancing network observability and state estimation accuracy within constrained budgets.

To our knowledge, scant research has been directed towards optimizing PMU placement in the context of attack mitigation [20-21], with existing studies primarily aimed at preventing the initiation of attacks—a topic that will be explored in detail in the literature review (Chapter 2). Notably, there is a lack of comprehensive analysis on how unobservability impacts the effectiveness of detection and localization mechanisms in the event of an existing attack.

This study seeks to address several pivotal questions, offering in-depth insights that could significantly inform PMU placement strategies. Among these questions are: How does unobservability influence the detection and localization of attacks? How many PMUs can remain unobservable before detection models become ineffective? How do the intensity of the attack and the number of targeted buses impact detection in a not fully observable network? Are there specific grid locations where unobservability detrimentally affects detection mechanisms? Do current

literature-proposed PMU placement strategies also optimize protection and enhance attack detection? Moreover, how do detection models behave when unobservable buses are either dispersed throughout the network or clustered in specific areas?

This research aims to elucidate these inquiries through data-driven models, initially applying state estimation to discern the status of unobservable buses; thereafter, presenting a fully observable network to the detection model for attack identification and localization, or directly using the results from the State Estimation to identify the attacks. Subsequent chapters will delve into the mechanisms in greater detail. It is important to mention that while this thesis does not directly devise a PMU placement strategy, our findings are anticipated to offer valuable insights, aiding utilities in PMU deployment and refining their strategies to ensure comprehensive observability alongside cyber-attack detection and localization capabilities.

1.5 Contributions and Thesis Organization

This thesis contributes to the field of smart grid cybersecurity, with a particular focus on state estimation, detection, and localization of cyber-attacks in the context of PMU placement and grid observability. The contributions of this thesis are summarized as follows:

- Comprehensive review and implementation of State Estimation model: This work provides a thorough review and implementation of various data-driven models for state estimation based on temporal analysis. For all the models, their performance will be assessed using various evaluation metrics along with determining the computational efficiency of each model.
- Comprehensive review and analysis of data-driven attack detection and localization models: A detailed review and analysis of several detection and localization models are presented, focusing on data-driven temporal approaches in both supervised and

unsupervised frameworks. This analysis contributes to a deeper understanding of how these models can be effectively applied to identify and localize cyber-attacks within the smart grid infrastructure.

- Experimental evaluation of bus unobservability impact: Through a series of comprehensive experiments, this thesis investigates the impact of bus unobservability on the performance of detection and localization models. It examines how the number of unobservable buses affects detection accuracy, identifies critical points in the grid where PMUs are essential for enhancing detection capabilities, and provides insights into optimal PMU placement strategies. These experiments yield valuable recommendations for PMU placement, aiming to improve smart grid security.

This thesis is organized as follows:

Chapter 2 (Literature Review) delves into the core concepts underpinning this thesis, including state estimation, the detection and localization of FDIA, and strategies for PMU placement. It aims to provide a foundational understanding and contextual background for the study.

Chapter 3 (Methodology, Dataset, and Attack Model) shows the approach utilized in this research, detailing the dataset employed, the mechanisms for generating FDIA cyber-attacks, and the metrics used to evaluate model performance.

Chapter 4 (State Estimation Models) focuses on examining and evaluating various data-driven models for state estimation based on temporal analysis. The goal is to identify the most effective model(s) for the dataset.

Chapter 5 (Detection and Localization Models) presents an analysis of detection and localization models based on temporal data-driven approaches. Both supervised and unsupervised

frameworks are explored to ascertain the optimal models tailored to the dataset in use throughout utilizing various performance metrics.

In Chapter 6 (Experimental Evaluation of Effects of Unobservability) extensive experiments are conducted to assess the impact of bus unobservability on the efficacy of state estimation and detection models. The findings from these experiments are expected to yield actionable insights regarding the optimal number and placement of PMUs to enhance detection capabilities.

Finally, Chapter 7 (Conclusions and Future Work) summarizes the key findings of the thesis and proposes directions for future research to build upon the work presented.

Chapter 2: Literature and Review of Key Concepts

This chapter embarks on a comprehensive exploration of the pivotal concepts underpinning this thesis, focusing on time-series analysis, state estimation, detection and localization of cyber threats, and placement strategies within smart grids. Each of these areas plays a crucial role in enhancing the security, reliability, and efficiency of smart grid operations, particularly in the context of defending against and mitigating the impacts of cyber-attacks.

2.1 Time Series Analysis Using Deep Neural Network

Anomaly and attack detection within infrastructures like smart grids inherently relies on time-series analysis due to the temporal relationships among measurements over time. This means that understanding the temporal patterns among various measurements is pivotal for enriching the learning process of Machine Learning (ML) models. By grasping these underlying connections, it becomes possible to enhance grid status forecasting, identify anomalies when typical time patterns are disrupted, and explore further applications. Therefore, the integration of Recurrent Neural Networks (RNNs) is indispensable for capturing these dependencies, as they are specifically designed to process sequential data, making them an essential tool for effectively analyzing and predicting based on the dynamic, time-sensitive nature of smart grid data.

RNN networks were first introduced in [22-23]. The need for RNNs arises from the limitations of traditional Neural Networks (NNs) in processing sequential data. Unlike NNs, which assume data samples are independent, RNNs can handle sequences where there is a dependency between elements, such as speech, language, and time series. NNs struggle with capturing long-range dependencies and cannot manage variable-length sequences effectively. Techniques, such

as fixed-size sliding windows, have limitations in capturing longer dependencies and adding noise. RNNs, by maintaining a state vector, can remember past information, allowing them to capture dependencies across time steps and handle variable-length sequences efficiently, overcoming the constraints of NNs [24].

However, RNNs often struggle with long-term dependencies because of the vanishing gradient problem when applying back propagation, which makes them less effective for sequences where past information is crucial for understanding future states [25].

To overcome the issue of vanishing gradient difficulty with learning long-term dependencies in RNNs, Long Short-Term Memory (LSTM) was first introduced in 1997 [26]. Unlike RNNs, which struggle with retaining past information due to weight changes during learning, LSTM introduces a gating mechanism. This mechanism manages information flow within neurons, allowing for controlled memory behavior that captures both short-term and long-term dependencies. The architecture includes forget and add gates, inversely linked to regulating memory capacity, mimicking the limited nature of human memory [27].

The LSTM architecture features six key components -shown in Figure 2.1 and represented by a set of equations 2.1 each with a specific function in processing sequential data:

- Input: Integrates current input $\boldsymbol{x}^t$ and previous output $\boldsymbol{h}^{(t-1)}$, processed through a tanh function to generate $\boldsymbol{C}$
- Input Gate: Determines the relevance of new information to be added to the memory cell by processing $\boldsymbol{x}^t$and $\boldsymbol{h}^{(t-1)}$ and applying a sigmoid Function.
- Forget Gate: Decides which information to discard from the cell state, aiding in managing the memory's relevance across different sequences.

- Memory Cell: Holds the LSTM's internal state, updating with relevant inputs while discarding outdated information.
- Output Gate: Controls the information to be output from the LSTM unit by filtering the cell state.
- Output: Produces the LSTM unit's final output, blending the cell state with the output gate's decision

$$
\begin{aligned}
\boldsymbol{i}^t &= \sigma(\boldsymbol{W}_{ix}\boldsymbol{x}^t + \boldsymbol{W}_{ih}\boldsymbol{h}^{t-1} + \boldsymbol{b}_i) \\
\boldsymbol{f}^t &= \sigma\left(\boldsymbol{W}_{fx}\boldsymbol{x}^t + \boldsymbol{W}_{fh}\boldsymbol{h}^{t-1} + \boldsymbol{b}_f\right) \\
\boldsymbol{o}^t &= \sigma(\boldsymbol{W}_{ox}\boldsymbol{x}^t + \boldsymbol{W}_{\text{oh}}\,\boldsymbol{h}^{t-1} + \boldsymbol{b}_o) \\
\widetilde{\boldsymbol{C}} &= \tanh\,(\boldsymbol{W}_{\widetilde{C}x}\boldsymbol{x}^t + \boldsymbol{W}_{\widetilde{C}h}\boldsymbol{h}^{t-1} + \boldsymbol{b}_{\widetilde{C}}) \\
\boldsymbol{C}^t &= \boldsymbol{i}^t \odot \widetilde{\boldsymbol{C}}^t + \boldsymbol{f}^t \odot \boldsymbol{C}^{t-1} \\
\boldsymbol{h}^t &= \tanh\,(\boldsymbol{C}^t) \odot \boldsymbol{o}^t
\end{aligned}
\tag{2.1}
$$

where $W_{ix}, W_{ih}, W_{fx}, W_{fh}, W_{ox}, W_{oh}, W_{\widetilde{C}x}, W_{\widetilde{C}h}$ represent the weights; and $b_i, b_f, b_o, b_{\tilde{C}}$ represent the bias vector [28].

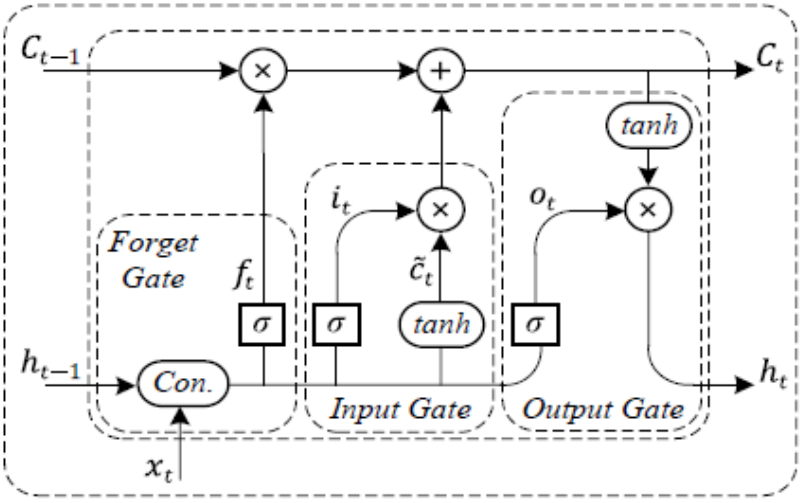

Figure 2.1 LSTM cell. From "Spatio-temporal data-driven detection of false data injection attacks in power distribution systems," by A.S. Musleh, G. Chen, Z.Y. Dong, C. Wang, & S. Chen, 2023, Electrical Power and Energy Systems, 145(108612). Used with permission [28].

The LSTM architecture, as explained, has proven to be very effective when dealing with prediction in time series. Thus, it is a basic building block of all the models that are discussed in this study.

A simpler version of the LSTM cell - The Gated Recurrent Unit (GRU) cell – was introduced later. GRU is an evolution of the LSTM designed to adaptively capture dependencies of different time scales. GRUs simplify the LSTM architecture by using fewer parameters with just two gates: update and reset. The update gate helps the GRU determine how much of the past information needs to be passed along to the future, and the reset gate defines how much of the past information to forget. These mechanisms allow GRUs to efficiently manage information flow throughout the network, balancing between memory retention and forgetting. This streamlined structure enables GRUs to achieve performance on par with LSTMs, often with faster training times due to their reduced complexity [29]. GRU is also frequently used in the models adopted in this thesis.

2.2 State Estimation

State estimation is a key aspect of smart grids, vital for wide-area monitoring. It directly impacts crucial functions within the grid. Traditional methods of state estimation, reliant on accurate system models, can falter due to model inaccuracies. Thus, data-driven state estimation has emerged, leveraging the abundance of data in energy systems. Despite its advantages, it confronts challenges like data handling and sensor inaccuracies. Addressing these issues is essential to enhance power system reliability and security. This section will review classical and contemporary data-driven state estimation techniques. Incorporating such machine learning and advanced algorithms, these contemporary techniques offer potential solutions to overcome traditional limitations that don’t depend on the physical dynamic network topology.

2.2.1 Classical State Estimation

Conventional State Estimation (SE) in power systems is a pivotal process that provides operators with the best estimate of the system's state variables, typically voltages and phase angles, based on redundant and noisy measurements. It employs mathematical models to represent the physical behavior of the power grid, allowing for the optimization of power flow and ensuring grid stability. Traditional SE methods are model-based, relying heavily on the accuracy of the network model and the measurements from various sensors across the system [11].

Traditional SE tackles this by formulating an over-determined system of nonlinear equations, usually approached as an optimization problem. The fundamental equation for SE is $z = h(y) + e$ where z represents the measurement vector, y is is the state vector, $h(y)$ is the nonlinear function mapping system states to measurements, and e encapsulates measurement errors [20].

A very common example is the DC state estimation, where only real power flows are considered, ignoring reactive power and losses. The real power flow between buses i and j is described by equation 2.2:

$$P_{ij} = \frac{X_{ij}}{(\theta i - \theta j)} \tag{2.2}$$

and the power injection at bus i is $P_i = \sum(j \in N_i)\, P_{ij}$ where N_i is the set of buses connected to bus i and X is the line admittance. Then the fundamental SE equation $z = h(y) + e$, to solve for the state vector using methods such as *Weighted Least Squares (WLS),* which minimizes the following objective function in equation 2.3.

$$J(y) = (z - H\hat{y})^T R^{-1} (z - H\hat{y}) \tag{2.3}$$

Now, if the attacker was able to launch an attack vector “a”, a manipulated measurement vector will be received at the estimator end*:* $Z_a = Z + a$; now the estimator will estimate a new

malicious vector: $\hat{y}_{mal} = \hat{y} + c$ Where c is the error associated with the given malicious vector. The estimator then can detect an attack if $\| z - H\hat{y} \|^2 < \tau$; where τ is a predetermined threshold [30].

Further, the work presented in [31] provides a comprehensive examination of various SE methodologies tailored for distribution systems. The work explores three SE algorithms: the WLS explained above, the Weighted Least Absolute Value (WLAV), and the Schweppe Huber Generalized M-estimator (SHGM). The difference between the three methods can be summarized as follows:

- WLS is the most common approach, where the objective is to minimize the squared differences between measured and estimated values, adjusted by the measurement's error variances. This method assumes measurement errors are Gaussian and statistically independent.
- WLAV aims to minimize the absolute differences between measured and estimated values. This method is less sensitive to outliers compared to WLS, providing a robust alternative by not squaring the residuals, thus not amplifying the effect of large errors.
- SHGM further enhances robustness against outliers by applying a weighting function to the residuals, which can adapt based on the residual size, reducing the influence of significant outliers.

2.2.2 Data-Driven State Estimation

Data-driven state estimation represents a significant shift from traditional model-based approaches, leveraging the wealth of data generated by modern power systems to enhance grid monitoring and operational efficiency. Unlike classical methods that rely on predefined system models, data-driven techniques employ advanced algorithms and machine learning to infer the

grid's state directly from data. This approach offers the potential to overcome limitations related to inaccurate or incomplete models, providing a more flexible and adaptive framework for managing the complexities of contemporary and future energy systems [10].

While there are ML and statistical-based models that tackle the state estimation problem such as ARMA method, Kalman filter, and Bayesian approach [7,32,33], Artificial Neural Networks models [34] become more popular due to the large volume of available data as more PMUs and smart meters are being incorporated into the grids, and ANN's ability to capture non-linear dynamics which is a limitation in the machine learning models [35].

Most of the work that is based on ANN considers the temporal analysis of the data. The work in [36] employs model-specific deep neural networks (DNNs) unrolled from iterative solvers for real-time state estimation, alongside deep RNNs for forecasting. This dual approach leverages historical voltage time series to predict future states, significantly improving performance over traditional methods. Further, [37] presents a scalable distribution systems state estimation approach using LSTM networks as surrogate models to enhance computational efficiency. It leverages LSTM's ability to capture temporal correlations between consecutive states and uses an autoencoder to reduce input dimensionality, thereby improving scalability and computational speed. This method significantly accelerates state estimation convergence in large systems. Moreover, the authors in [38] present a data-driven real-time SE model using deep ensemble learning. This approach incorporates dense Residual Neural Networks (ResNetD) as base-learners and a multivariate-linear regressor as the meta-learner. The model addresses challenges such as incomplete data sets by forecasting system states during instances of missing measurements, thereby enhancing the reliability and accuracy of SE in dynamic and uncertain operating conditions.

Finally, graph-based models are becoming more popular in analyzing state estimation problems because of their ability to capture spatial relationships between the buses. These models use a graph framework to model the grid, allowing for a more intuitive and efficient analysis of network topology. By representing buses as nodes and transmission lines as edges, graph-based approaches facilitate the identification of critical network components and paths and capture the interactions among the components of the system in the model [39]. The performance of the GNN (Graph Neural Networks) models is even enhanced when also considering the temporal dimension during training as implemented in [40]. This approach presents a TGCN (Temporal Graph Convolution Network) which combines the topological structure capturing capability of G-CNNs with the dynamic variation handling of gated recurrent units for improved SE accuracy.

In this study, the focus will be on temporal dynamics for state estimation, specifically leveraging the LSTM models, renowned for their effectiveness in processing time-series data.

2.3 Data-Driven Attack Detection and Localization

Data-driven detection algorithms for FDIA in smart grids are characterized by their independence from system models and parameters. According to [41], these model-free approaches are categorized into three main types based on their data usage: machine learning algorithms, data mining algorithms, and other algorithms that neither learn from data nor mine it for patterns. In this review, the focus is only on the machine learning-based models, and according to the same resource, the ML models can be classified into three categories: Supervised (labels are provided during training), Unsupervised (no labels are provided during the training), and Reinforcement learning models. It must be clear that the reliance on historical data is a defining aspect of ML techniques, as it is crucial for training the models to perform the required tasks. This dependency enables the algorithm to learn and make predictions or decisions based on past system

behavior. In the following review, the machine learning unsupervised and supervised models will be reviewed.

2.3.1 Unsupervised Models

In unsupervised learning, machines analyze unlabeled data to uncover hidden patterns and classifications. This method autonomously groups data points based on their intrinsic characteristics, which is particularly useful in detecting FDIA in smart grids, as these anomalies typically form distinct clusters separate from normal operational data. Unsupervised models excel in anomaly detection because they are trained on normal data—assumed attack-free—allowing them to identify deviations during testing as potential anomalies, given the absence of predefined attack labels. Therefore, these models are considered more agile to handle different types of attacks [42].

Since anomalies are usually rare [43] and mostly continuous [44], utilizing recurrent units like LSTM and GRU is very efficient in capturing anomaly behavior, and differentiating them from the normal data. According to [45] the models based on including RNN units can be classified into three categories: Prediction-based models, Autoencoders-based models, and hybrid models.

The basic idea behind prediction-based models, as implemented in various works such as [46-49] is comparing actual values against model forecasts. Simple methods might use a window-based approach to predict future values through statistical measures such as the median, and then flag deviations beyond a set threshold as anomalies [47]. More sophisticated techniques involve creating temporal models that predict the next value in a sequence. Anomalies are identified when observed values significantly diverge from these predictions, indicating unexpected behavior within the data. Thus, the prediction error is high enough to confirm the presence of anomalies in the network.

Various architectures have been implemented based on RNN units for more robust prediction. The work presented in [50] utilizes a single-layer LSTM for predictions, where a prediction error exceeding a certain limit signals a potential anomaly. A circular array records recent prediction errors to calculate two metrics: the percentage of anomalies and the sum of prediction errors. When both metrics surpass predefined thresholds, the corresponding sequence is classified as a collective anomaly, enabling the effective detection of irregular patterns in data sequences. In [51] the authors introduce a stacked LSTM model for identifying irregularities in time series data, distinguishing itself from robust or denoising LSTM Autoencoders (AE), which will be reviewed later, by not relying on dimensionally reduced features for input. Instead, it identifies anomalies through the assessment of discrepancies between actual and predicted data, employing variance analysis to quantify deviations.

The Autoencoder models are neural network approaches, by compressing input data into a lower-dimensional space and then reconstructing it, are adept at identifying anomalies through significant reconstruction errors. The novelty lies in their ability to discern complex, time-variant anomalies by learning normal system dynamics. This method's efficacy is enhanced by incorporating noise reduction and regularization techniques, allowing for robust detection of anomalies even in disturbed data, thereby setting a foundation for advanced anomaly detection in time-series data [52-53].

Some Variation based on AE models was introduced in Park’s work [54] which employs a probabilistic approach in both the encoding and decoding phases. This method translates input sequences into compressed, lower-dimensional representations and reconstructs them, focusing on significant features. Anomaly detection is executed through a log-likelihood ratio, assessing discrepancies between actual and reconstructed data. Finally, [55] introduced an enhanced

Seq2Seq LSTM network architecture for improved anomaly detection, featuring sparsely connected encoders and decoders with skip connections. These connections adjust based on input sequence information density, allowing for flexible cell state propagation. The architecture uses a shared copying layer for distributing a condensed feature vector, preventing overfitting, and enhancing generalization. The anomaly detection cost function aims to minimize reconstruction errors while incorporating a penalty term to manage information flow, optimizing anomaly detection performance.

The third and final approach of the unsupervised models is using hybrid networks where different deep neural networks or ML models are combined. The work in [56] applies the integration of LSTM neural networks with a One-Class Support Vector Machine (OCSVM) for enhanced anomaly detection in time series data. By combining LSTM's ability to learn temporal dependencies with OCSVM's capability for identifying data points that deviate from the learned normal behavior, while in [57] they used an autoencoder network combined with the OCSVM and followed the same approach. The work in [58] introduces a method that combines Convolutional Neural Networks (CNN) and Long LSTM networks to enable multidimensional anomaly detection. By leveraging the efficient compression capabilities of CNNs for high-dimensional data, the method can extract dependencies across multiple dimensions. The classification process in this method is based on cross-entropy.

2.3.2 Supervised Models

In supervised learning, the model is trained with a dataset that includes input-output pairs, where the outputs are labels indicating the category (nominal or anomalous) of each instance. This means the model learns to predict the output for a given input based on examples provided during training.

The use of the regular FFN (Forward Networks) for FDIA detection was introduced in various works. For example, the work presented in [59] built a fully connected network, where there are 60 Neurons per layer with Softmax activation function, achieving detection accuracy of 99% on the given dataset, surpassing the performance of regular ML models like SVM. Furthermore, the work in [60] introduces a technique that leverages FFN to concurrently execute distribution state estimation computations and identify FDIAs. Specifically, they utilize a single DNN model to carry out both regression and classification tasks, enabling simultaneous SE computation and FDIA detection.

Nonetheless, combining the FFN networks with RNN networks usually yields better results due to RNNs abilities to store and capture dynamic temporal relations as discussed earlier [61-62].

Additionally, several models that integrate CNNs and RNNs within a supervised framework have demonstrated effective outcomes, such as the study where CNN-LSTM and CNN-GRU were utilized [63]. By pairing RNN units to identify temporal patterns with CNN layers that use convolutional operations instead of conventional matrix multiplication, this approach effectively captures relational and dependent features, resulting in a robust detection mechanism. Also, [64] introduces an RNARXNN model which is a type of recurrent neural network that combines the features of Nonlinear AutoRegressive Exogenous Networks (NARX) with deep learning for time series forecasting. It incorporates both historical input and output data to predict future states. This model is structured to capture temporal dependencies and patterns within data, making it particularly effective for anomaly detection in time series data.

Finally, as outlined in Section 2.2, graph-based models are gaining prominence due to their significant potential. These models can also be effectively applied to detect anomalies within graph-based topologies, such as smart grids. In related work, the authors have employed Temporal

Graph Neural Networks (TGNN) – essentially a Graph Neural Network that utilizes a message-passing mechanism to discern the relationships between buses (nodes). This is coupled with a GRU unit to capture temporal dynamics, enabling the detection and localization of attacks with high precision, even when the attack intensity is low [65].

In Chapter 4, implementation and testing of several of these models on our dataset will take place to determine the most suitable model for our problem and dataset structure. Similar to SE, all models under consideration are temporal-based. The objective is to characterize the effects of limited observability on the performance of such models.

2.4 Optimal PMU Placement

As previously discussed, the task of PMU placement poses significant challenges due to budget constraints and the goal of achieving maximal network observability. Numerous scholars have explored this problem, leading to the development of a range of algorithms designed to navigate these complexities. Below, some of these innovative approaches are highlighted:

Integer Linear Programming (ILP) is a method used in OPP strategies aimed at minimizing the total number of PMUs required while guaranteeing the system's complete observability. Various ILP models have been devised, incorporating constraints such as zero injection buses and N-1 contingency scenarios to enhance the robustness of power system monitoring.

Heuristic algorithms such as Genetic Algorithms (GA) are a common method as well [67]. GAs are used for solving the OPP problem by mimicking the process of natural selection. These algorithms iteratively select, mutate, and crossover candidate solutions, efficiently navigating the search space to find near-optimal PMU configurations.

Moreover, Particle Swarm Optimization (PSO) is recognized as a population-based stochastic optimization approach inspired by the social behaviors observed in bird flocking. A

PSO-based strategy for addressing the OPP issue within a particular power grid configuration is introduced [68]. This strategy has been rigorously tested and confirmed effective on IEEE 14, 30, and 68-bus systems and has been applied to a significant portion of the Brazilian power grid to verify its applicability [69].

However, as discussed, the primary aim of these algorithms is to maximize grid observability and optimize PMU placement for enhanced state estimation. It is noted that few studies specifically address placement strategies under the threat of attacks or faults. A novel contribution in this domain introduced a greedy algorithm focused on defending against data integrity attacks, notably FDIA, in the power grid. This approach involves estimating the minimal number of sensors vulnerable to compromise for a successful attack and then employing a greedy algorithm to strategically place PMUs to thwart these attacks [20]. A later work presented in [86] investigates the limits of fault localization using synchrophasor data in power grids, particularly in scenarios where the number of PMUs is insufficient for complete grid observability. The authors propose a statistical analysis method based on the Kullback-Leibler (KL) divergence between distributions corresponding to different fault location hypotheses, highlighting how fault locations tend to cluster around certain areas of the grid more closely connected to the actual fault site. This leads to a PMU placement strategy aimed at achieving near-optimal fault localization resolution with a limited number of sensors.

As highlighted in Chapter 1, existing literature lacks a detailed analysis on the impact of unobservability during ongoing attacks, and primarily focuses on PMU placement to prevent the initiation of such attacks. Chapter 6 will shift the focus towards examining how PMU placement influences the detection capabilities when an attack is in progress, offering a new perspective on enhancing grid security by considering limited unobservable scenarios.

Chapter 3: Methodology, Dataset, and Attack Model

This chapter is established as the groundwork for the subsequent chapters, where the actual implementation of the study will be explored. The methodology adopted in this thesis is outlined here to pave the way toward achieving the final goal of conducting a comprehensive experimental analysis of the effect of bus unobservability on the detection and localization model. Following this, an in-depth examination of the dataset used in the research will be provided, offering insights into its composition and relevance. Additionally, the FDIA model will be discussed in detail, with its significance within the context of the study being highlighted. The chapter concludes with a presentation of the evaluation metrics that were utilized to assess the performance of the models. Through this structured approach, it is aimed to prepare the reader for the comprehensive experiments and analyses that are conducted in the following chapters.

3.1 Methodology

To explore the influence of unobservability on detection models, various detection models were developed, adapting and modifying architectures from the literature to suit our specific problem. This thesis evaluates both supervised and unsupervised detection models, aiming to identify the most effective approach; nevertheless, both models will be used when conducting the unobservability experiments to study the commonalities and differences between the two different approaches.

First, start by developing various models under the unsupervised model category. These models can be divided into 2 categories:

- State Estimation-Based Models: These include LSTM, GRU, Stacked LSTM, Stacked GRU, and Hybrid Stacked models.
- Non-State Estimation-Based Models: This category comprises LSTM-Autoencoders and LSTM-OCSVM models.

Chapter 5 will delve into the intricacies of these models. It is noteworthy that state estimation-based models possess a distinct advantage over their non-state estimation counterparts, as they can function in scenarios with unobservable buses by estimating their readings. In contrast, non-state estimation-based models require full observability, necessitating a preliminary state estimation to approximate the readings of unobservable buses before data input into the detection model.

Following the development of unsupervised models, our attention shifted towards creating supervised models, including Stacked LSTM, Stacked GRU, BiDirectional LSTM (BiLSTM)-based, and CNN-LSTM models. Like the unsupervised non-state estimation models, these too are limited by the need for full observability, thereby requiring SE before data input.

The state estimation models, initially paired with unsupervised state estimation-based models, are now solely tasked with estimating the state of unobservable buses. These estimated states, combined with the actual values for the observed buses, feed into the detection models.

Figure 3.1 illustrates the process flow in this mechanism. The process starts with the application of state estimation, utilizing the most effective model, which will be detailed in Chapter 4. The next step involves determining whether the training data are nominal (no attacks) or anomalous, meaning they contain cyberattacks. If the training data are found to be nominal, unsupervised learning models are used for further analysis. In the case that these unsupervised models are based on state estimation, an attack is indicated if the prediction error exceeds a specific

threshold (τ). For models that do not use state estimation, attack detection hinges on whether the reconstruction error from LSTM-AE or the output from LSTM-OCSVM surpasses the threshold.

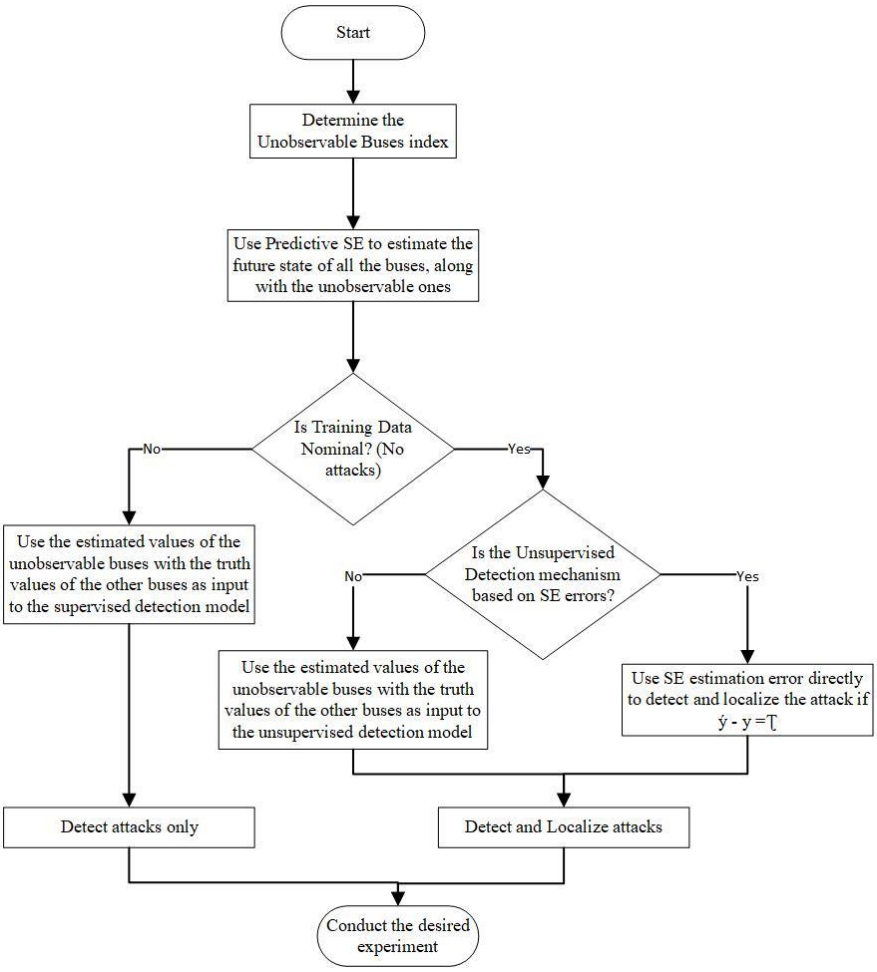

Figure 3.1 Flowchart of the methodology presented in this thesis.

Should the training data contain attacks, supervised models are then utilized. The binary prediction outputs from the neural network will determine whether a given time instance is under attack. These mechanisms will be discussed in depth in chapter 5.

Notably, while the used supervised models can detect attacks, unsupervised models extend to attack localization. The challenge with supervised models in pinpointing attack locations lies in their need for additional data features for effective training. Specifically, they require multiple

features per bus, such as voltage angles, voltage magnitude, and real power, to achieve accurate predictions, which in turn, greatly increases computational demands. However, in this study—especially considering the extensive number of experiments outlined in Chapter 6—only one feature (real power) is used during training to enhance computational efficiency. This decision is strategically made to facilitate a large volume of unobservability experiments while managing computational load effectively; thus, in this study, only unsupervised models are used for attack localization.

Before delving into the details of the mentioned models and their performance, it's essential to shed some light on the dataset itself to grasp its structure. Following this, the methods used to model and introduce attacks into the developed dataset will be explored.

3.2 Generation of the Nominal Dataset

The system used in this study is the IEEE-118 bus system [70] which is a widely recognized test case in power systems engineering used for conducting research and simulations. The system comprises 118 buses, 186 branches (including transmission lines and transformers), and 54 generators, making it a comprehensive model for studying the behavior of a large-scale power network. The IEEE 118 Bus System is often utilized for power flow analysis, stability studies, reliability assessment, and optimization algorithm testing. It provides a realistic and complex network structure, featuring a variety of load demands and generation capacities. Figure 3.2 shows a physical representation of the IEEE-118 Bus System.

In this study, time-series data for the power system is generated through power flow simulations conducted on the IEEE 118 bus system using MATPOWER 7.1. These simulations incorporated a dynamic load profile, which records the load patterns provided by the New York Independent System Operator (NYISO) [71], as outlined in previous work [72].

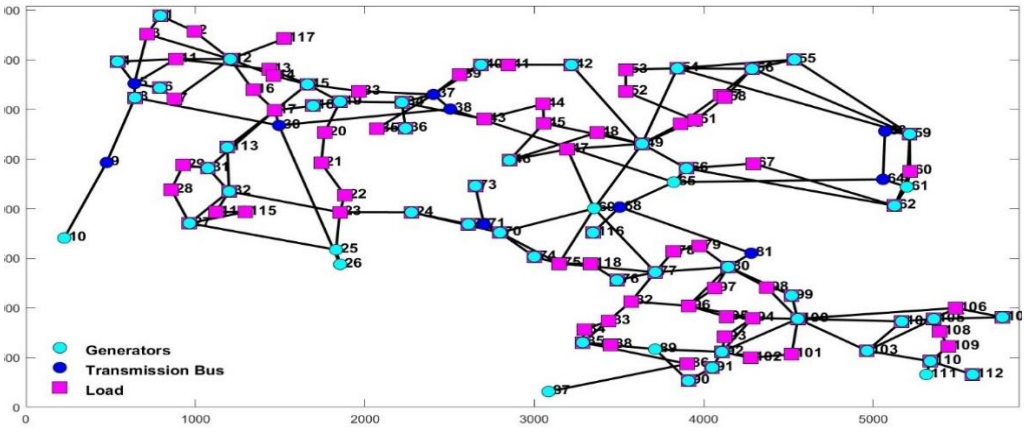

Figure 3.2 The IEEE 118 bus system physical topology.

By solving the power flow equation at each time instance, state measurements such as active power, reactive power, voltage angles, and voltage magnitude were recorded. The used NYISO dataset contains the load profile over 1 month – December 2019- and was sampled at 0.033 Hz (1 sample every 30 seconds), resulting of total 90210-time instances. For our analysis, the focus will be on real power as the primary feature of interest. Given the structure of our dataset, which encompasses 118 buses, each bus will be considered an individual feature within our model. This approach leads to the creation of a multivariate time series dataset, comprising 90,210 observations across 118 dimensions.

To analyze the relationships and dependencies across the different buses, a heatmap is employed of the correlation matrix of the real power and voltage angles, utilizing the sklearn and seaborn libraries in Python [73] (refer to Figure 3.3).

This visualization in Figure 3.3 illustrates the extent of correlation among the voltage angels' values at various buses. It reveals a predominantly positive correlation, with correlation coefficients ranging between 0.9 and 1, indicating a strong interconnection among all buses. This observation suggests that the buses influence each other's behavior, with a notably stronger

correlation observed among adjacent buses compared to those further apart. Yet even the distant buses still have high correlation values.

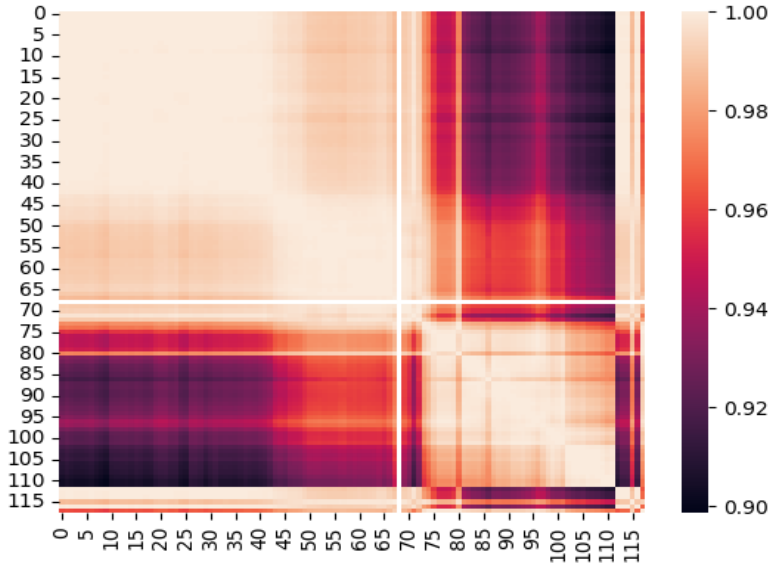

Figure 3.3 Heat map of correlation between the buses.

To effectively visualize the temporal dynamics of the data, we graphed the real power values for Bus 1 across one month as shown in Figure 3.4.

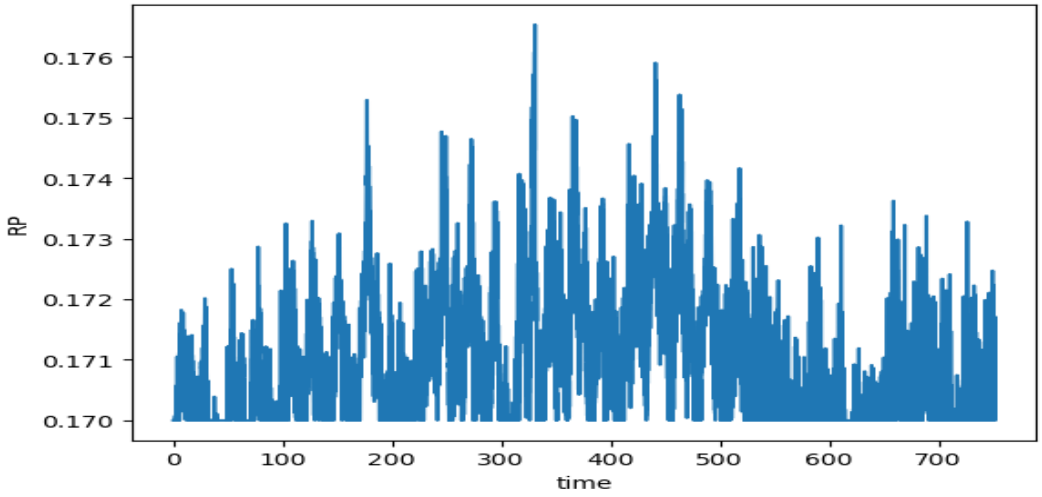

Figure 3.4 Hourly real power values for Bus 1 during December 2019 in the IEEE 118 bus system.

For enhanced clarity in the visualization, data points were aggregated on an hourly basis, thereby consolidating multiple samples into a single data point for each hour. This approach allows for a more coherent and simplified representation of trends over time. Figure 3.5 illustrates this analysis, showcasing how the real power at Bus 1 fluctuates throughout the observed month.

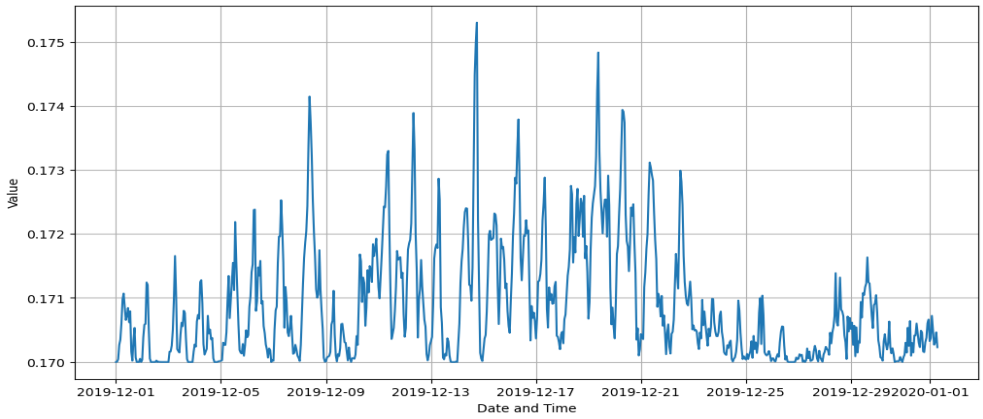

Figure 3.5 Hourly aggregation of the real power values for bus index 1 in the IEEE 118 bus system.

In concluding the discussion on data preparation, it's pertinent to highlight how the dataset was partitioned. In this work, 60% percent of the sequential data, amounting to 54,126 time samples, was allocated for training purposes. Validation and testing phases were allotted 15% and 25% of the dataset, corresponding to 13,531- and 22,553-time samples, respectively. This segmentation ensures a comprehensive approach to model training, validation, and testing. This segmentation is used across all the models that will be discussed in Chapters 4 and 5.

3.3 FDIA Modeling

This section aims to introduce the attack model used to inject FDIA attacks on our nominal dataset described in 3.2. The basic attack strategy of FDIA was briefly mentioned while reviewing the State Estimation in Section 2.2.1. The efficacy of traditional bad data detectors hinges on their ability to identify discrepancies between observed measurements Z, and those predicted by state

estimation $\hat{y}$ based on a predefined threshold (τ). This is quantified through the residue vector $r = |z - h(\hat{y})|^2$ which, when surpassing τ, signals the presence of anomalous data.

In the simulation of the FDIA used in this research, the approach from [74] is adopted. We- as the attackers- adept in FDIA methodologies engineering our data injections $Z_a = Z + a$ such that the residue resulting $|Z_a - \mathrm{h}(\hat{y})|^2$ remains below the detection threshold τ thus camouflaging the attack. To encapsulate this strategy within the broader framework of cyber-attacks, the attack vector is defined as shown in the below equation (3.1):

$$\mathrm{c(t)} = \mathrm{x}(n_A, t) + (-1)^b x' \tag{3.1}$$

where $\mathrm{b} \in 0,1$, and $|x'|$ is deliberately kept minimal to ensure that the introduction of false data does not prompt an immediate, noticeable disruption at the beginning of the attack, thereby circumventing the detection mechanisms integrated within the state estimation system. Essentially, the design of the FDIA discussed in this study aims to maintain the absolute deviation between the actual and the manipulated data, denoted x' below the detection threshold τ, ensuring the alterations remain undetected. In this work, the smallest possible $|x'|$ was assumed to be 0.004 p.u. which is usually less than 1% of the original value of the real power. To further model our attack scenarios, the following assumptions were made:

- Attacks within the network are infrequent yet sustained; once initiated, they persist for a discernible duration [43-44].
- The hypothetical attacker possesses significant resources, enabling them to compromise anywhere from one to twenty buses simultaneously. While this is a wide range relative to the size of the system, it has been investigated in this work for the purpose of a comprehensive analysis.

- The execution of an attack is synchronized across targeted buses. Consequently, if an attack targets two buses, it commences and concludes simultaneously for both.
- Buses that are not observable—either due to the absence of PMUs or because they are disconnected— are not the target of the attacks.

Table 3.1 shows the parameters used in the attack simulation across all the experiments.

Table 3.1 FDIA simulation parameters.

Parameter	**Values**
Gaussian Noise added to the measurements	45-55 dB [75]
Number of attack scenarios	• Supervised model: 200 (150 attacks in the training set, 50 attacks in the testing set) • Unsupervised model: 50 (0 attacks in the training set, 50 attacks in the testing set)
Attack length (Duration)	Randomly selected between (30-80) time instances for each scenario
Attack size (affected buses at a time) "*A*"	1,2,5,8,10,20
Location of attacks	For each scenario (attack) the location of the attacks is randomly selected
Attack severity	0.04 (high severity attack) 0.004 (low severity attack)

To provide a better understanding of the frequency and distribution of attacks within the dataset, table 3.2 presents the average ratio of time instances and the ratio of buses targeted during attacks across the whole *test* dataset, categorized by the number of buses attacked.

Table 3.2 Ratio of the attacked buses and time instances to all instances across the testing set.

Number of attacked buses	**1**	**2**	**5**	**8**	**10**	**20**
Average Ratio of attacked buses	0.1%	0.21%	0.55%	0.89%	1.1%	2.2%
Average Ratio of attacked time instances	12%	12.1%	12.2%	12.5%	12.6%	12.7%

3.4 Evaluation Metrics

It is crucial to outline the evaluation metrics that will be employed to gauge the efficacy of our models. Given that our study encompasses two distinct types of models—state estimation models and attack detection models—two separate sets of performance metrics tailored to each model type will be utilized. This differentiation ensures that the assessment of each model aligns with its specific objectives and challenges, providing a comprehensive evaluation of its performance.

3.4.1 State Estimation Evaluation Metric

Since the framework of SE in this work is mainly based on predictive SE, the selected evaluation metrics are mainly based on the evaluation of regression problems. Two metrics will be used to evaluate the state estimation.

- Mean Squared Error (MSE) [76-77]: MSE assesses the average of the squares of the errors, thereby giving more weight to larger errors, so it becomes more sensitive to the outliers. It's calculated as in equation 3.2. MSE will serve as our main performance metric.

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \tag{3.2}$$

- R^2 score [78]: R^2 , often referred to as the coefficient of determination, measures the proportion of the variance in the dependent variable that is predictable from the independent variables. R^2 provides a sense of how well the observed outcomes are replicated by the model, based on the proportion of total variation of outcomes explained

by the model. Its formula can be found in equation 3.3. R^2 score also will be used as a secondary metric.

$$R^2 = 1 - \frac{(sum_{i=1}^{n}(y_i - \bar{y})^2)}{(sum_{i=1}^{n}(y_i - \hat{y}_i)^2)} \quad (3.3)$$

Other metrics such as Mean Absolute Percentage Error (MAPE) [79] were considered but not reported in this thesis. MAPE expresses the error as a percentage of the true values, providing an intuitive sense of the error magnitude relative to the actual values as shown in equation 3.4.

$$MAPE = \left(\frac{1}{n}\right) * 100\% * \sum_{i=1}^{n} \left|\frac{(y_i - \hat{y}_i)}{y_i}\right| \quad (3.4)$$

Despite being MAPE is easy to interpret but can be problematic for values close to zero; and since some of our real power values in the dataset are zeros, MAPE score couldn't give a correct reliable evaluation for these buses. Thus, it is not used as a primary or secondary metric in this research.

3.4.2 Detection and Localization Metrics

The primary objective of detection and localization models is to optimize the number of True Positives (TP) — accurate identifications of the target phenomenon — while concurrently reducing the occurrences of False Positives (FP) and False Negatives (FN), which represent incorrect alerts and missed detections, respectively. Typically, a confusion matrix serves as an effective tool for visualizing and assessing these metrics, offering a clear depiction of the model's performance in distinguishing between actual and predicted classifications. Another two metrics can be derived to give us more insights about the detection performance:

- Precision (Positive Predictive Value): Precision (equation 3.5) measures the accuracy of the anomaly predictions made by the model. It is defined as the ratio of true positives to the total number of instances predicted as positive (both true positives and false positives). High precision indicates a low false positive rate but does not account for false negatives.

$$\text{Precision} = \frac{\text{TP}}{(\text{TP} + \text{FP})} \tag{3.5}$$

- Recall (Sensitivity or True Positive Rate): Recall (equation 3.6) measures the model's ability to detect all relevant cases of anomalies. It is defined as the ratio of true positives to the actual positives (sum of true positives and false negatives). High recall indicates that the model is effective at identifying anomalies but does not consider the accuracy of those identifications:

$$\text{Recall} = \frac{\text{TP}}{(\text{TP} + \text{FN})} \tag{3.6}$$

- F1 score: The F1 score is highly valuable for anomaly detection due to its ability to equally consider precision and recall, offering a balanced measure that's crucial when both false positives and false negatives have significant impacts. Acting as the harmonic mean of precision and recall, the F1 score penalizes extreme discrepancies, ensuring a comprehensive evaluation. This is particularly useful in unbalanced datasets (please refer to table 3.2), a frequent scenario in anomaly detection, where it provides a nuanced view of a model's performance over mere accuracy. This balance makes the F1 score an excellent metric for accurately assessing anomaly detection systems, especially in environments where detecting every anomaly is as important as minimizing false alerts [80]; its formula is shown in equation 3.7. Due to its advantages and suitability to our problem, the F1 score will be used as our primary evaluation metric.

$$F1 = \frac{(2 * Precision * Recall)}{(Precision + Recall)} \tag{3.7}$$

Finally, Accuracy (equation 3.8) will be considered as it measures the overall correctness of the model across both anomalies and normal observations. It is calculated as the ratio of correctly predicted observations (both true positives and true negatives) to the total number of

observations. While a useful general metric, accuracy can be misleading in datasets with a significant imbalance between normal observations and anomalies, that's why accuracy will be used as a secondary metric:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+\text{FP}+\text{FN}} \tag{3.8}$$

3.5 System Configuration and Software Tools

The development and execution of SE models, alongside detection and localization algorithms that will be discussed in Chapters 4 and 5, were performed using Python version 3.9.16. This work incorporated a range of libraries, including TensorFlow, Scikit-learn, Keras, and Seaborn, to facilitate the implementation of the computational models and data visualization. Data generation and attack simulation were carried out using Matpower version 7.1, integrated with MATLAB Version 23.2.0.2365128, to ensure accurate and realistic simulation environments. The entire computational workload was processed on an Intel(R) Core (TM) i5-7300U CPU @ 2.60GHz.

Chapter 4: State Estimation Models

The objective of this chapter is to establish a state estimation model to be utilized in unobservability experiments. To achieve this, a variety of models were developed, primarily employing the resources and literature reviewed in Chapter 2. The aim is to evaluate the performance of these models and select the one that exhibits the best performance for conducting the unobservability experiments. However, it is crucial to note the following considerations regarding all models discussed in Chapters 4 and 5:

While these models were fundamentally derived from various pieces of literature, they do not strictly adhere to the same model structure; changes were made to some of the hyperparameters, alterations were made to some layers, and in certain cases, new layers were introduced to better align with the specific nature of our problem. For example, Batch Normalization (BN) layers were incorporated into some models (especially those with complex structures), not merely to mitigate overfitting but also to accelerate the training process by reducing internal covariance shift [81]. Given the extensive volume of experiments conducted, minimizing computational time during training is essential for this study.

Building on this point, it is pertinent to highlight that the "winning model" is identified not solely based on achieving the best performance according to the evaluation metrics outlined in Chapter 3, but also considering the training time. The optimal model is expected to deliver the highest possible performance while maintaining a reasonable training duration.

In this study, the developed models for SE will undergo evaluation using two distinct datasets to assess their performance under different conditions. The first dataset is free of any

cyber-attacks, serving as a baseline to determine the efficacy of the SE model under normal operating conditions. Conversely, the second dataset incorporates cyber-attacks, with an attack intensity set at $x' = 0.04\ p.u$ (refer to equation 3.1), and the number of attacked buses A =10. For both experiments, the number of random unobservable buses k is set to be= 10.

Also, the evaluation metrics MSE and R^2 score will be applied in two contexts: first, to assess the SE models' performance across the entire network of 118 buses, denoted as 'SE Global'; and second, to specifically evaluate their performance on the unobservable buses, referred to as 'SE Unobservable'.

In this chapter, the performance of five models—LSTM, GRU, Stacked LSTM, Stacked GRU, and a hybrid stacked approach—will be explored. Initially, we will detail the architecture of each model to provide a comprehensive understanding of their design and operational principles. Subsequently, the final section, titled 'Results and Conclusions,' will delve into a discussion of the performance outcomes for each model. This analysis will culminate in the identification of the Winning model, which will be selected based on its superior performance metrics and subsequently employed in the remainder of the unobservability experiments.

4.1 LSTM and GRU Models

In this section, we will discuss the architectures of the LSTM and GRU models together, as they share a similar structure with the primary distinction being the type of recurrent unit employed in each. Both models utilize a 'lookback' technique, hereafter referred to as *window size*, which leverages a predetermined number of past time instances to predict the subsequent instance in the sequence. The input for these models is formatted as a 3-dimensional array, denoted by $[t, i, n-k]$, where "t" denotes all the time instances, i is the window size, n is the total number of features (consistently set at 118), and k is the number of unobservable buses. Figure 4.1 shows

how this 3-D array is constructed, where $i = 10$, and the first sequence is being fed to the LSTM unit.

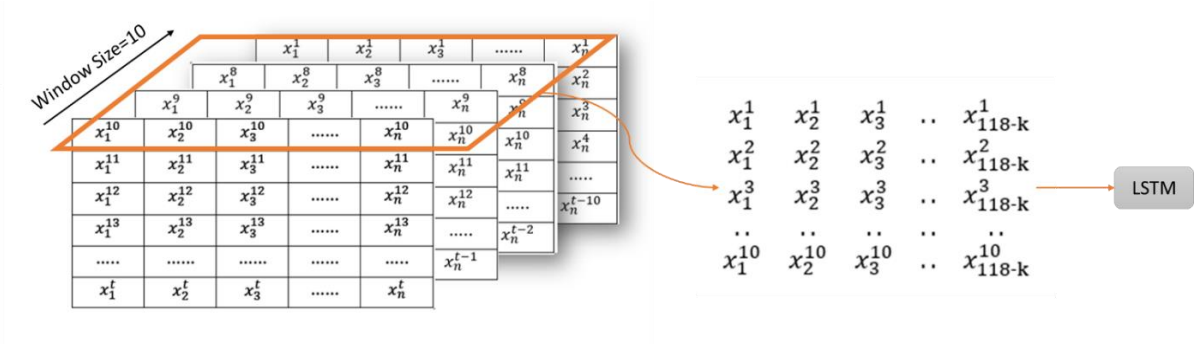

Figure 4.1 Dataset input structure for LSTM.

Subsequently, the LSTM unit is iteratively unfolded ' i ' times to apply sequential training, a process depicted in Figure 4.2.

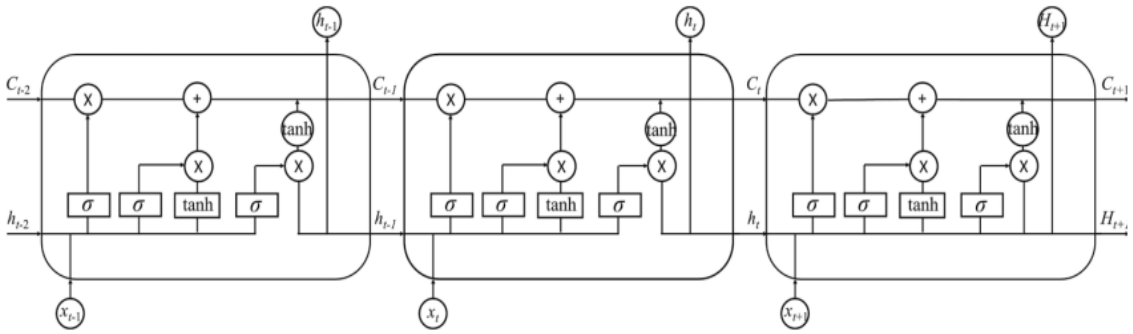

Figure 4.2 LSTM cell unfolding for sequential training. From "Dynamic evaluation method for time-variant reliability of structural safety of concrete-faced rockfill dam" by J. Yang, L. Pei, C. Kuang, Y. Li, & Y. Liu, 2023, Institution of Structural Engineers. Used with permission [85].

It is critical to note that, although the features of unobservable buses are not utilized as input during the model's training phase, any machine learning model necessitates historical target values for effective training. This requirement is exclusive to the training phase and does not extend to the testing phase. Consequently, accessing the power values of unobservable buses is essential for the training process. To acquire historical data for these buses, two primary

assumptions can be considered: these buses were previously equipped with measurement units that have since been disconnected due to physical disconnections or Denial of Service (DoS) attacks, as discussed in [7]; alternatively, deriving historical values through the application of power flow equations in conjunction with classical state estimation techniques. Although it has not been considered in this work, certain ML models including GNN models [82] and graph signal processing techniques [83] can estimate the state of unobservable ones from the relation among the nodes and do not require historical values in the training. Such models can be considered as future directions of research for this study.

The proposed model comprises a single LSTM layer, which includes multiple parallel units and is augmented by a dropout layer to prevent overfitting. This configuration is followed by a dense layer equipped with 118 neurons. To identify the optimal model configuration, a comprehensive evaluation of various parameter combinations was undertaken. The testable parameters and their respective combinations are detailed in Table 4.1. Using trial and error, the best combination of parameters is shown in the same table.

Table 4.1 The parameters being used while developing the various models.

Parameter	**Parameter Values**	**Selected Value**
Number of units per layer	4, 20, 64, 128	64
Window Size	2,10,30	10
Dropout	0, 0.1, 0.2	0.2
Recurrent Dropout	0,0.2	0.2
Activation	Relu, Sigmoid	Relu
Early stopping min_delta	$10e^{-3}$, $10e^{-5}$	$10e^{-5}$
Optimizer	Adam, SGD	Adam
Loss Function	MSE	MSE

Figure 4.3 provides a visual representation of the model per one sequence, illustrating its architecture with recurrent units depicted as LSTMs. While this figure specifically represents LSTM-based models, it is important to note that GRU models possess a similar structure. The key difference lies in the substitution of LSTM units with GRU units.

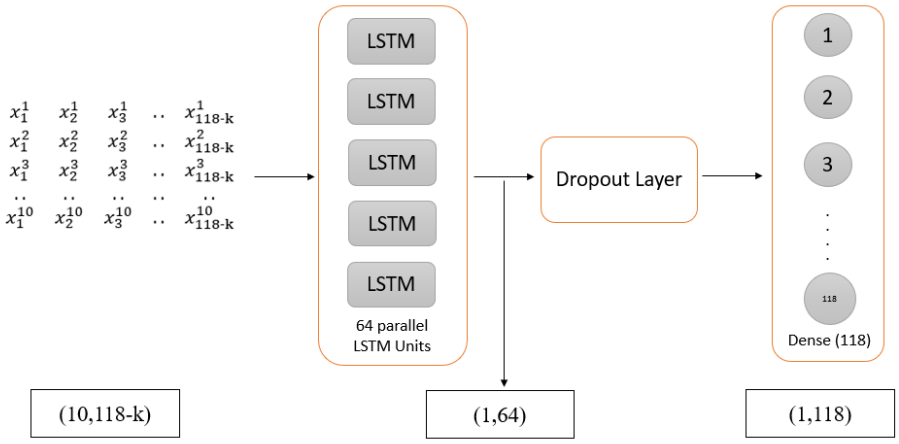

Figure 4.3 LSTM model structure with a single sequence as input.

4.2 Stacked LSTM and GRU Models

In this section, the architectures of the Stacked LSTM and GRU models will be explored. The distinguishing feature of this approach, compared to the previously discussed models in Section 4.1, is the layering of multiple LSTM or GRU layers atop one another. This design is intended to capture more complex temporal dependencies within sequential data. However, it is important to note that this increased complexity also raises the risk of model overfitting.

The input shape of the model adheres to the specifications outlined in Section 4.1. This model is configured with three GRU or LSTM layers, featuring 128, 64, and 64 neurons in each layer, respectively. Following each GRU or LSTM layer, a Dropout (DO) layer is applied to mitigate overfitting with a value of 0.2, succeeded by a Batch Normalization layer to enhance training stability and speed. Additionally, a ReLU activation function is employed to introduce

non-linearity, culminating in a dense layer to finalize the architecture. The detailed structure of the model is visually depicted in Figure 4.4.

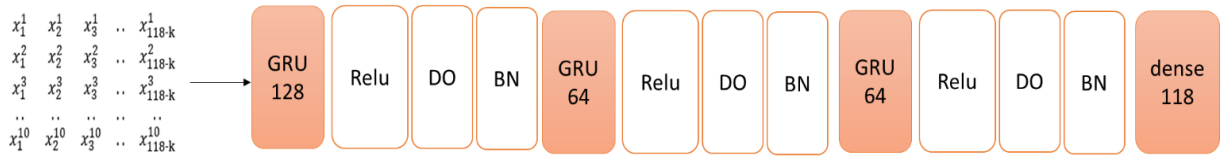

Figure 4.4 Stacked GRU model structure.

4.3 Hybrid Stacked Model

To the best of knowledge, this methodology is not documented within the power systems SE literature, the proposed model, which alternates between LSTM and GRU layers in a four-layer stacked configuration, demonstrated better performance relative to models exclusively composed of LSTM or GRU stacked layers. This model alternates between LSTM and GRU layers, effectively leveraging the unique strengths of both to enhance learning capabilities. The architecture of this model, detailed in Figure 4.5, illustrates its structured approach to integrate the LSTM and GRU layers.

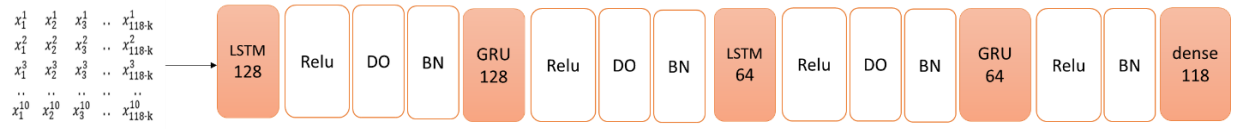

Figure 4.5 Hybrid stacked model structure.

It is believed that combining GRU and LSTM layers in a single model can harness the strengths of both architectures, potentially leading to enhanced performance on complex sequence modeling tasks. This approach offers the simplicity and efficiency of GRUs alongside the sophisticated long-term dependency capture of LSTMs, enabling the model to learn a wider range

of patterns and dependencies within the data. The combination of GRU and LSTM layers allows the model to learn a broader set of patterns and dependencies within the data. For example, the GRU layers might quickly capture the short-term dependencies, while the LSTM layers focus on retaining information over longer sequences. This can be particularly beneficial for complex sequence modeling tasks where different types of dependencies exist in the data. Such a mixed architecture can provide improved regularization, reduce the risk of overfitting, and offer greater flexibility and customization for the SE tasks.

4.4 Results and Discussions

In this section, the performance of the proposed models is discussed. It is important to mention that many scenarios were simulated to evaluate the performance of these models; however, the results shown below are for two specific scenarios that are believed to represent the other scenarios. The first scenario involved a dataset where no attacks were introduced, allowing us to assess the state estimation baseline performance of the models. The second scenario examined the performance of the models under FDIA attacks with a magnitude of $x' = 0.04\ p.u$, and the number of the attacked buses A =10. It is also pertinent to note that the models were uniformly trained across all scenarios, utilizing 64 batches and undergoing 40 epochs of training. This setup ensures a consistent basis for evaluating their performance under both standard and adversarial conditions.

Table 4.2 presents the results for the first scenario, where no attacks were introduced, highlighting both the MSE and R^2 score for clarity. Concurrently, Figure 4.6 offers a graphical depiction of the R^2 score values across all five models, facilitating a visual comparison of their performance. For the second scenario, where attacks are introduced, Tables 4.3, and Figure 4.7 show the performance of the models.

Table 4.2 Performance of SE under no-attacks scenario.

	SE Global (118 Buses)		SE of Unobservable Buses	
	MSE Global	R2 Global	MSE Unobserv	R2 Unobserv
LSTM	**0.00017**	**0.997**	**0.0001**	**0.998**
Hybrid Stacked	0.00045	0.994	0.00026	0.9965
LSTM Stacked	0.00049	0.993	0.00028	0.996
GRU Stacked	0.00049	0.993	0.00031	0.995
GRU	0.00069	0.991	0.00028	0.996

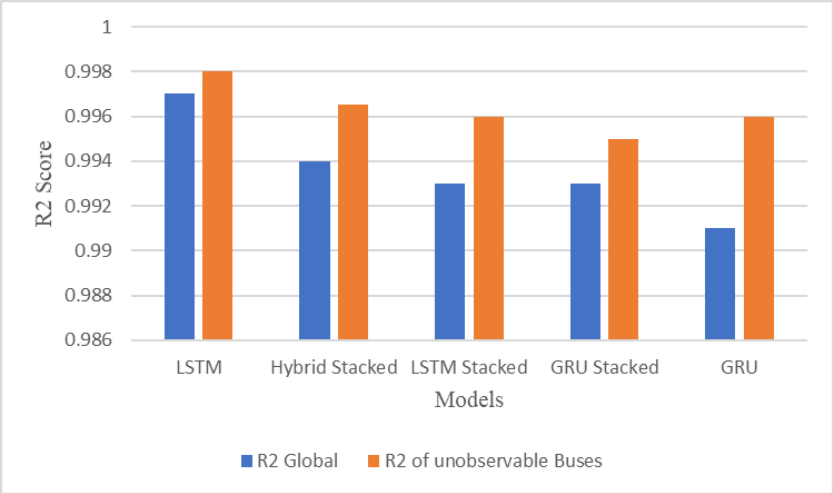

Figure 4.6 Comparison of R2 score of the proposed models under no attack scenario.

Table 4.3 Performance of SE under attack scenario where x' =0.04 p.u and A=10

	SE Global (118 Buses)		SE of Unobservable Buses	
	MSE Global	R2 Global	MSE Unobserv	R2 Unobserv
LSTM	**0.0070**	**0.7106**	**0.0056**	**0.9231**
Hybrid Stacked	0.0074	0.7	0.0084	0.901
LSTM Stacked	0.0079	0.64	0.014	0.79
GRU Stacked	0.0077	0.67	0.012	0.83
GRU	0.0076	0.69	0.011	0.85

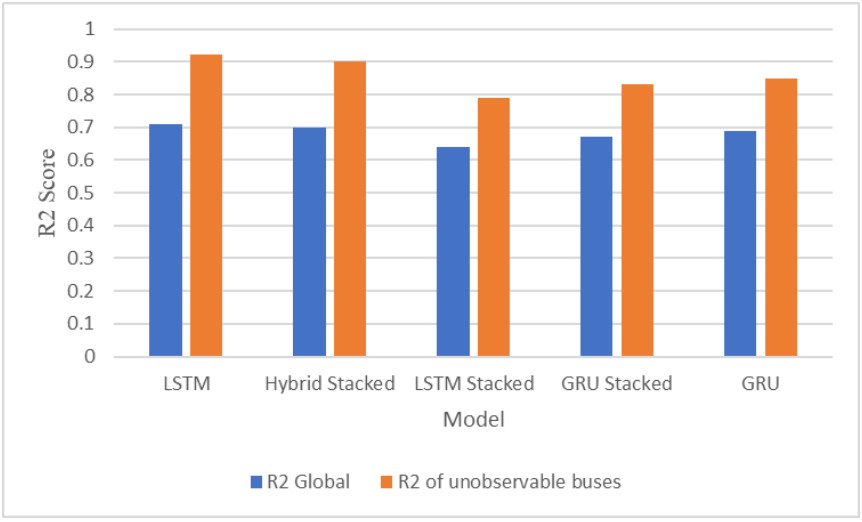

Figure 4.7 Comparison of R2 score of the proposed models under attack scenario, where $x' = 0.04$ p.u and A=10.

The results indicate that the basic LSTM model outperforms the other five models under consideration. Although the hybrid stacked approach exhibits encouraging outcomes, it ranks second to LSTM. Furthermore, as depicted in Figure 4.8, it also incurs the longest training duration. Consequently, the LSTM emerges as the preferred model for state estimation, balancing simplicity with efficacy. The findings suggest that, within this context, a less complex model achieves more accurate predictions, while more intricate models tend to underperform, likely due to overfitting. On the other hand, overly simplistic models, such as the GRU, fail to fully capture the temporal dependencies. Therefore, the LSTM stands out as the optimal model, striking a balance between simplicity, manageable training time, and superior performance.

It is also worth mentioning that the presence of the attacks highly affects our SE. The MSE drops by almost 1 digit when attacks are present. However, this should help us to detect the attacks as will be discussed in Chapter 5.

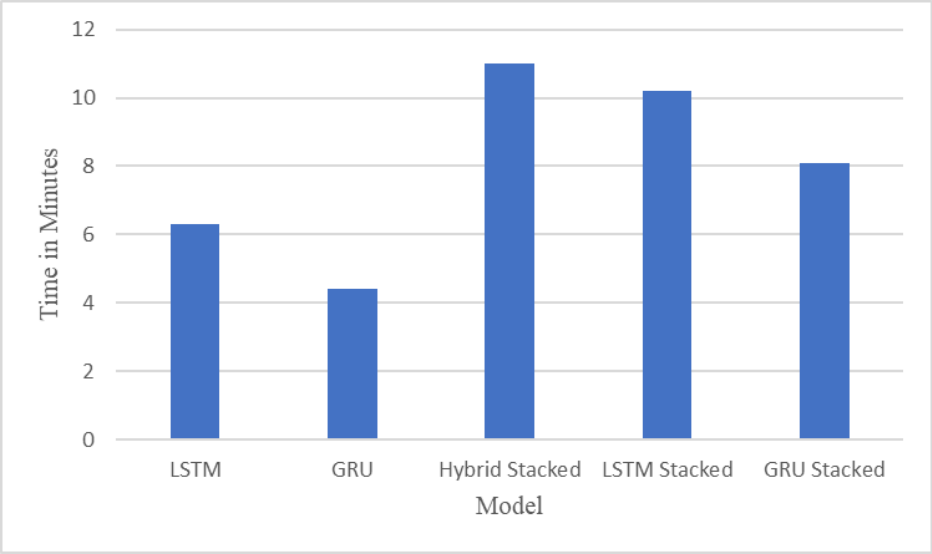

Figure 4.8 Training time in minutes of the models.

Figure 4.9 provides a detailed comparison of predicted versus actual power values for bus 1 for the LSTM model under the two distinct scenarios. As shown, Figure 4.9-a and Figure 4.9-b illustrate the comparison for scenario 1, where there are no attacks on the system, demonstrating how closely the predictions align with the actual data in a secure environment. Conversely, Figures 4.9-c and Figure 4.9-d present the comparison for scenario 2, which involves the FDIA attacks. These figures highlight the impact of such attacks on the accuracy of the SE predictions. These results are shown for bus 1 as an example but similar trends are observable for other buses.

Finally, a sensitivity analysis has been conducted. The outcomes of the sensitivity analysis are detailed in Figures 4.10 and 4.11. The experiment in scenario 2 was repeated, with two intensities $x' = 0.04$, and $x' = 0.004$. Figure 4.10 depicts the global MSE, and Figure 4.11 shows the MSE for unobservable buses. The results indicate that a decrease in attack severity (moving from $x' = 0.04$ to $x' = 0.004$) improves prediction accuracy. Moreover, it is observed that as the number of unobservable buses increases, there is a corresponding increase in the MSE.

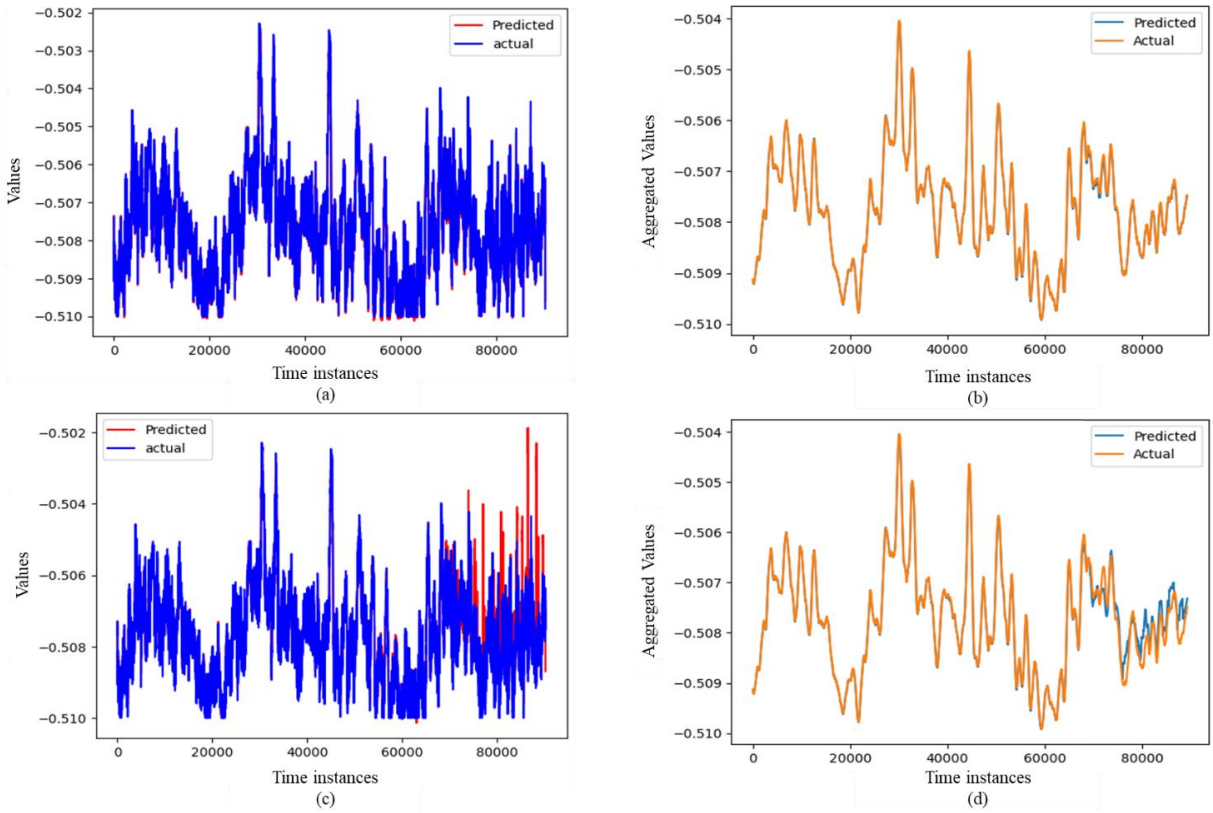

Figure 4.9 The predictions vs. actual real power values for bus 1. (a) all values under no attacks, (b) aggregated values under no attacks, (c) all values under FDIA attack with $x' = 0.04$, and (d) aggregated values under FDIA attack with $x' = 0.04$.

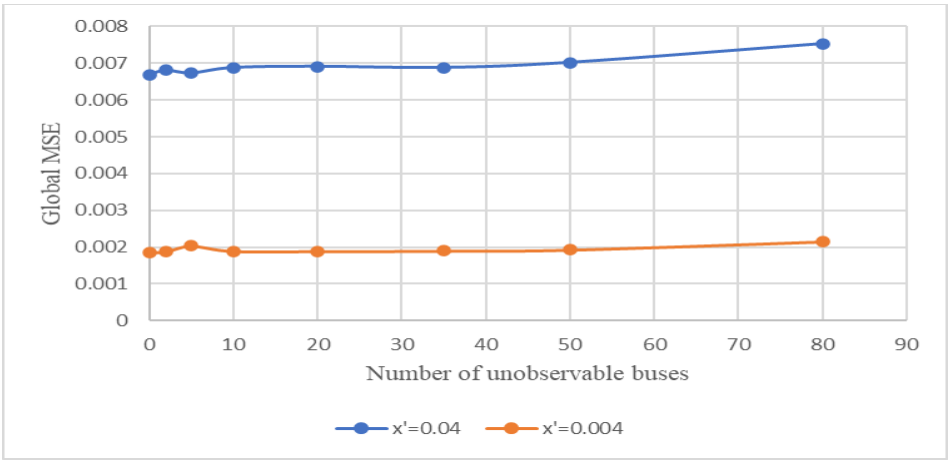

Figure 4.10 Global MSE under different attack intensities.

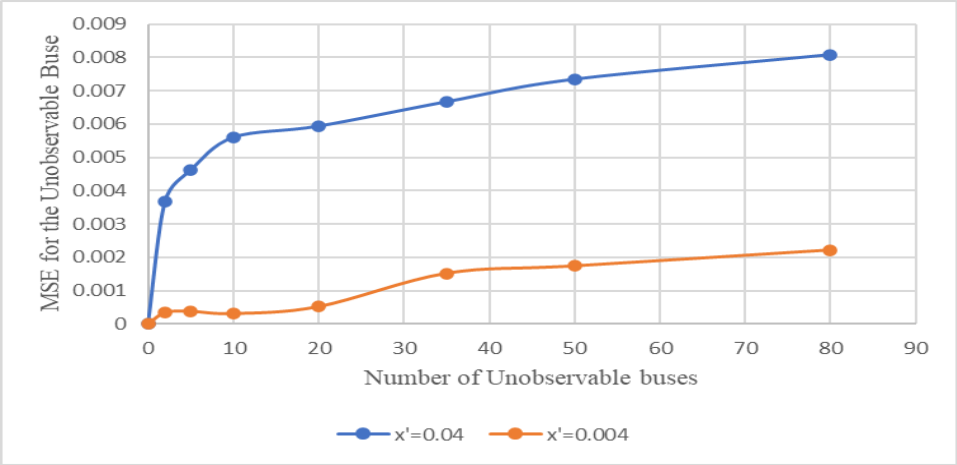

Figure 4.11 MSE of the unobservable buses under different attack intensities.

Chapter 5: Attack Detection and Localization Models

In this chapter, the focus is shifted towards the evaluation of various detection and localization models to identify the most effective one that will be used to conduct observability experiments detailed in Chapter 6. It is crucial to note that the models examined in this chapter are assessed based on their performance under conditions of full observability. Furthermore, as detailed in the SE chapter, many scenarios were studied, but the results presented in this chapter will focus on the most comprehensive scenario believed to represent the other scenarios adequately. Specifically, the attack intensity considered here is $x'=0.004$ p.u, based on the assumption that if the models are capable of detecting attacks at low intensity, they will inherently detect attacks of higher intensity.

The model that emerges as the most capable from this analysis will then be combined with the optimal model identified in Chapter 4, LSTM SE model, for undertaking experiments on unobservability in Chapter 6. Both unsupervised and supervised learning models are explored, aiming to provide a comprehensive understanding of their applicability and performance in different observability contexts.

5.1 Unsupervised Model

In this section, the assessment will begin with the unsupervised model. Two types of models have been evaluated: the SE-based models and the non-SE-based models. The SE-based model triggers a threshold "τ" if the SE error exceeds a certain limit, whereas the non-SE-based models make their final decision without explicitly depending on SE, although SE may play a role during the process. The exploration of models based on SE will be initiated first.

5.1.1 SE-Based Models

The models utilized in this section are the same as those described in Sections 4.1 and 4.2, specifically the LSTM, GRU, Stacked LSTM, and Stacked GRU. Therefore, the details of their architecture will not be revisited, as they have already been explained in Chapter 4. Instead, this part will focus on explaining how the detection and localization mechanisms operate following the completion of state estimation.

First, the detection mechanism will be addressed. Following the completion of the SE on the training set, the MSE for each time instance in the training set is calculated, with each time instance comprising 118 buses. This is done using the MSE equation in 5.1.

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n=118}(y_i - \hat{y_i})^2 \tag{5.1}$$

By applying this equation across all time instances of the training set, an MSE error vector $e(t)$, where t represents all time instances in the training set, is obtained. In this case, the error vector will have dimensions [54,126, 1], where 54,126 is the total time samples in the training set. It is crucial to recognize that, since the training was conducted on nominal data with no attacks introduced, all error values within $e(t)$ are considered nominal errors. Consequently, a histogram for the nominal data error can be plotted, as illustrated in Figure 5.1. It is noted that the histogram is skewed to the right, a result of eliminating negative errors through the squaring process in the MSE formula. This approach simplifies the process of dealing with a single threshold on the positive axis, rather than two.

The underlying assumption is as follows: given that all values in $e(t)$ are nominal, lying within the range of 0 to 0.0013 as depicted by the example histogram in Figure 5.1, during testing, any instances of attacks will result in an error exceeding the normal range of nominal error. Consequently, a threshold τ could be set at 0.0013 or a value close to it. For the testing dataset,

any MSE value exceeding this threshold would be identified as corresponding to an attack, thus the detection alarm could be flagged.

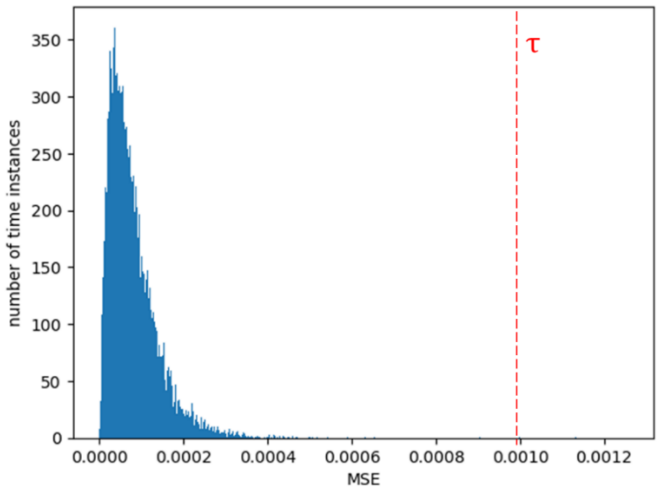

Figure 5.1 Histogram of detection MSE for the training data using the LSTM model.

For illustrative purposes, although not essential for the implementation, the MSE histogram of the testing set is depicted in Figure 5.2. Observation reveals that points beyond the established threshold, τ, are indicative of attacks. The histogram demonstrates an expanded MSE range, extending from 0.0013 to 0.035. Notably, any point exceeding the threshold of 0.0099 is classified as an attack in this case.

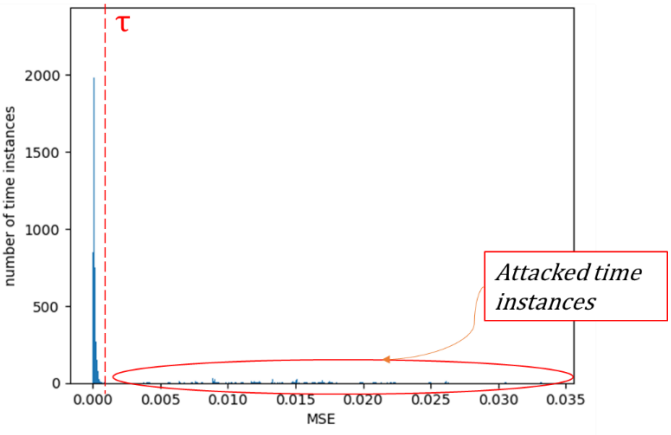

Figure 5.2 Histogram of detection MSE for the testing data using the LSTM model.

The approach for attack localization mirrors that of detection, with a key distinction: instead of computing the MSE for each time instance, the Absolute Error (AE) for each output is determined, as outlined in the following equation:

$$\mathrm{AE} = |y_i - \hat{y}_i| \tag{5.2}$$

Consequently, the resulting vector dimensions are [118*t, 1], where t represents the total number of time instances, in this case, 54,126. This yields a vector of dimensions [6,386,868, 1]. Subsequently, the AE can be visualized through histograms for both the training and testing datasets, as depicted in Figures 5.3 and 5.4.

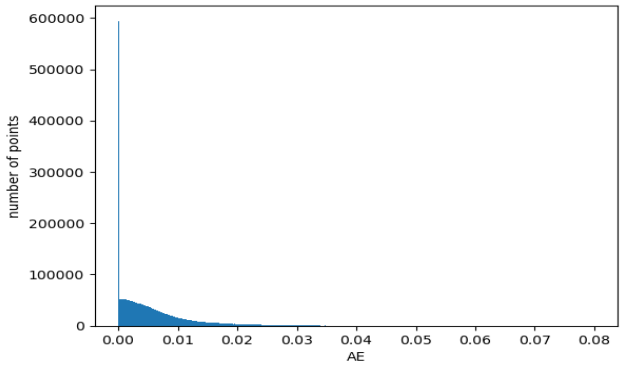

Figure 5.3 Histogram of localization MSE for the training data using LSTM model.

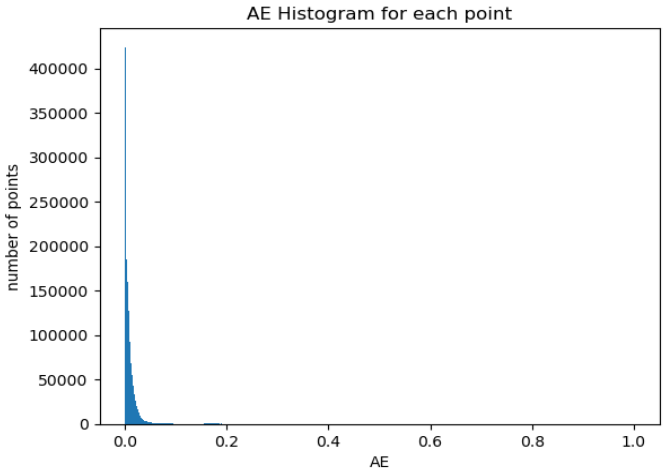

Figure 5.4 Histogram of localization MSE for the testing data using LSTM model.

The outcomes of detection and localization performances for the four models—LSTM, GRU, Stacked LSTM, and Stacked GRU—will be examined in detail in Section 5.3.

5.1.2 Non-SE-Based Models

In this section, two models that do not explicitly depend on SE for their final decision-making process will be discussed, although SE plays a role in their operations. The models in focus are AE and LSTM-OCSVM. Their architecture and decision-making mechanisms will be discussed in this section.

Starting with AE, as explored in Section 3.2.1, Autoencoders are designed to compress and subsequently reconstruct input data, with the goal of achieving as close a match as possible to the original input. The underlying principle is that, during training with nominal (i.e., normal or attack-free) data, the autoencoder learns specific weights for its encoder-decoder architecture that enable it to accurately reconstruct the input data. However, in the presence of anomalies or cyber-attacks, this reconstruction process is likely to be compromised, resulting in significant deviations from the original input and, consequently, high reconstruction errors.

Building upon the discussion in Section 5.1.1, it becomes apparent that these reconstruction errors, rather than prediction errors, serve as a crucial indicator for identifying the presence of attacks within the system. Figure 5.5 shows the architecture of the best-performing AE model.

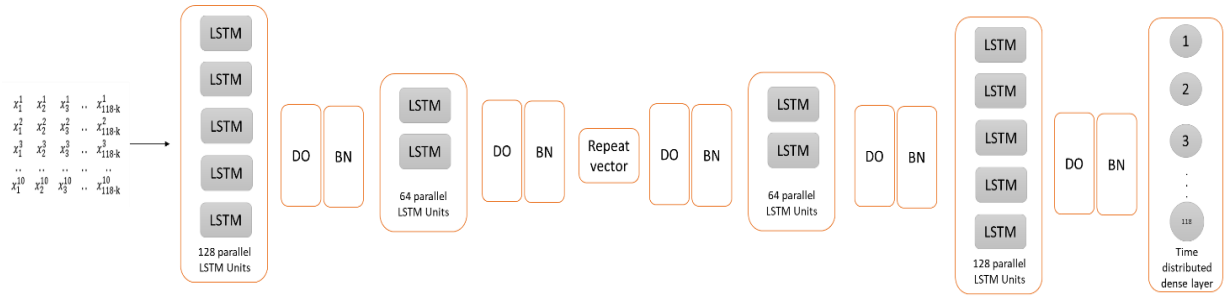

Figure 5.5 Architecture of LSTM autoencoders.

The model initiates by inputting data in the format previously detailed in Section 4.1, tailored to enable the LSTM network's processing of sequential information. It employs two stacked LSTM layers for the encoding process, containing 128 and 64 neurons each, to capture the temporal dependencies and features within the data effectively.

Following the encoding layers, a Repeat Vector layer is introduced. This layer serves a critical function by duplicating the output of the final LSTM encoder layer across the time steps required by the decoder. This replication ensures that the decoder receives input in a format that maintains the sequential context, enabling it to effectively reconstruct the sequential data output.

For the decoding process, a mirrored structure of the encoder is utilized, featuring two LSTM layers with 64 and 128 neurons, respectively. This symmetric architecture allows for the gradual reconstruction of the original input data from the encoded representation, aiming to replicate the initial sequence as closely as possible.

A TimeDistributed layer is then applied, which is essential for maintaining the independence of the time steps in the output sequence. It allows the model to apply a fully connected dense layer to every temporal slice of the input data, ensuring that the model can make predictions for each time step independently, thus preserving the temporal sequence structure in the output.

Each layer in the model is followed by a dropout layer, set at 0.2, to prevent overfitting by randomly ignoring a subset of neurons during training. Additionally, a batch normalization layer follows each LSTM layer, which normalizes the activations of the previous layer at each batch, maintaining the mean output close to 0 and the output standard deviation close to 1. This practice helps in accelerating the training process and achieving higher stability as discussed in Chapter 4.

Shifting to LSTM-OCSVM, this model combines the strengths of LSTM networks and OCSVM for anomaly detection. This hybrid approach leverages the sequential data processing capability of LSTM networks to capture temporal dependencies and features within the data, these features are then classified by OC-SVM, which distinguishes between normal and anomalous patterns by creating a boundary in the feature space. This LSTM model can be any of the models described in the previous sections. The model can be visualized as shown in Figure 5.6.

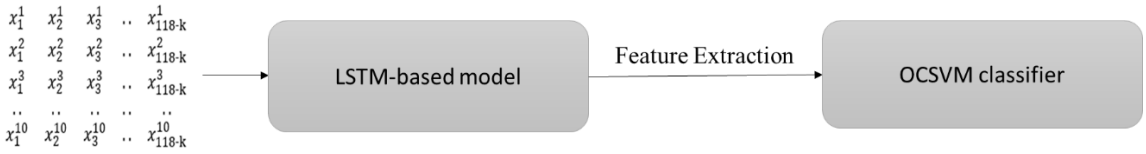

Figure 5.6 LSTM-OCSVM model.

In this work, both the LSTM and LSTM-AE were used for LSTM block part, and for the OCSVM part, testing was conducted with both RBF and linear kernels. Training the model with the linear kernel proved to be particularly challenging and time-consuming due to the difficulty in establishing linear boundaries. Regarding the ν (nu) parameter, which is pivotal in balancing the proportion of outliers against the decision boundary size around normal data points, various values were experimented with, including 0.01, 0.1, 0.2, and 0.5.

5.2 Supervised Models

In this work, the focus is on employing supervised models for attack detection within datasets that include labeled attacks. The discussion will cover four specific models: Stacked LSTM, Stacked GRU, CNN-LSTM, and BiLSTM. The decision to prioritize detection over localization stems from two main considerations. Firstly, the extensive training required for these models to achieve convergence for localization purposes necessitates more training epochs. Secondly, localization demands a significant increase in features per bus, such as voltage

magnitude and reactive power, making the process computationally expensive and less aligned with the goal of conducting numerous unobservability experiments. Consequently, the models are strategically directed towards detection rather than localization. Some of these models are similar to the models that were discussed previously, except for one major difference: they use binary cross entropy as a loss function instead of using MSE. Below is a description of each model.

Stacked LSTM/GRU models are very similar to the stacked GRU and LSTM models discussed in Section 4.2, with two major differences: the introduction of a dense layer with 32 neurons before the final layer, and the inclusion of a single-neuron dense layer activated by a sigmoid function for the output. Figure 5.7 illustrates the Stacked GRU model's architecture, with the LSTM model differing only in the use of LSTM units instead of GRU units.

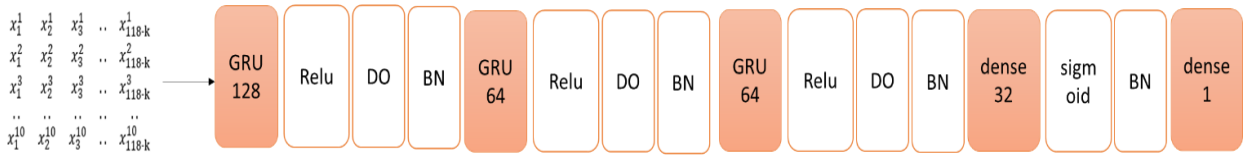

Figure 5.7 Supervised stacked GRU model.

BiLSTM-based model is based on The Bidirectional Long Short-Term Memory (BiLSTM) unit which is an advanced version of the traditional LSTM unit. Unlike standard LSTMs that process data in a forward direction, BiLSTMs analyze information in both forward and backward directions. This dual-path processing allows BiLSTMs to capture context from both past and future data points, which supposedly provides a richer understanding of the sequence context. The constructed model here has only one BiLSTM layer with 128 units in it, followed by a dense layer with 32 neurons, then a one-neuron dense layer. As usually practiced in this work, BN and 0.2 DO layers are employed. Figure 5.8 shows its construction.

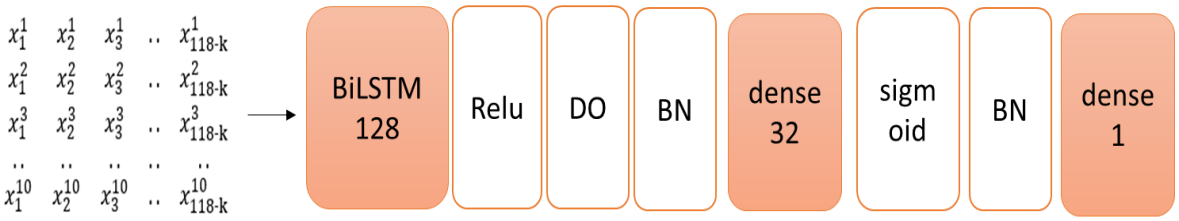

Figure 5.8 BiLSTM model architecture.

CNN-LSTM/GRU models combine the spatial data capturing capabilities of CNNs with the sequential data processing strengths of LSTM or GRU layers. Given the high positive correlation among features (buses) as noted in Figure 3.3 and given that buses with closely numbered indices are typically adjacent to each other, employing CNN layers initially helps in capturing spatial correlations between buses. This setup includes two 1D convolutional layers with 64 filters each, with a kernel size of three by one, effectively convolving features. Subsequently, a layer of either GRU or LSTM with 64 units is applied, followed by two dense layers—one with 100 neurons and another with a single neuron—to finalize the model's predictions. The construction of this model, illustrated in Figure 5.9, optimizes the handling of spatial and temporal dependencies.

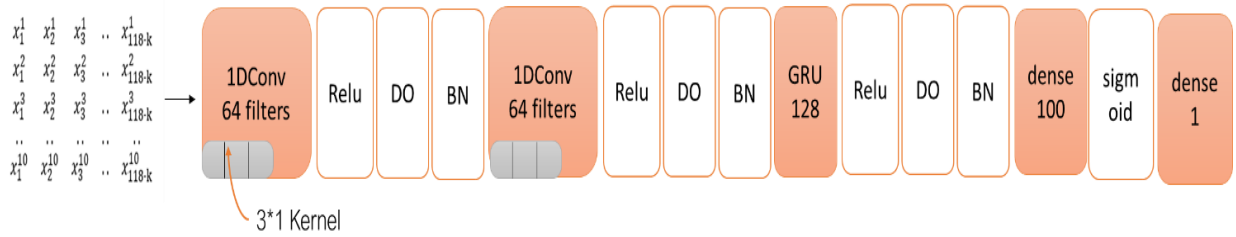

Figure 5.9 CNN-GRU architecture.

5.3 Results and Discussion

In the concluding section, the performance of previously discussed models is evaluated with the objective of selecting two models for the unobservability experiments in Chapter 6: one

unsupervised and one supervised. The evaluations are based on a specific scenario involving an attack intensity of $x' = 0.004$ p.u. and number of attacked buses A =10 buses, The scenario was chosen for its challenge in detection. Although various scenarios were explored, this particular setup is utilized to representatively showcase the models' capabilities under challenging conditions.

5.3.1 Unsupervised Models Results

Table 5.1 presents the F1 scores and accuracy for the six models reviewed in Section 5.1. It's crucial to note that the reported results for the SE-based models are derived at the optimal threshold for each respective model.

Table 5.1 Performance of unsupervised models.

Model	Detection **F1**	Localization **F1**	**Detection Accuracy**	**Localization Accuracy**
LSTM	**0.993028**	**0.970071**	**0.998758**	**0.999341**
GRU	0.99	0.96	0.998	0.9973
stacked GRU	0.62	0.6519	0.916	0.99
stacked LSTM	0.61	0.6219	0.91	0.988
AE	0.71	0.749	0.914	0.9932
LSTM_OCSVM	0.65	0.67	0.913	0.991

Further, Figures 5.10 and 5.11 show a graphical representation for both F1 and accuracy respectively for all the six models.

The results demonstrate that the LSTM model outperforms others in detection and localization, evidenced by its superior F1 scores and accuracy, followed by the GRU and AE models. This aligns with insights from Section 4.4, suggesting simpler models are more effective for this dataset, as complex models tend to overfit. Given its optimal SE performance noted in Section 4.4 and its efficiency in detection and localization tasks within a reasonable training

timeframe, the LSTM model is selected as the winning model for further experiments that will be conducted in Chapter 6.

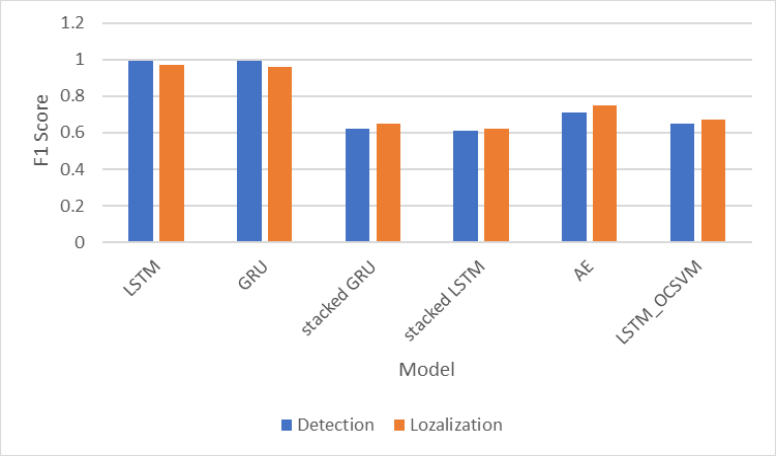

Figure 5.10 F1 score of the unsupervised models for attack detection and localization.

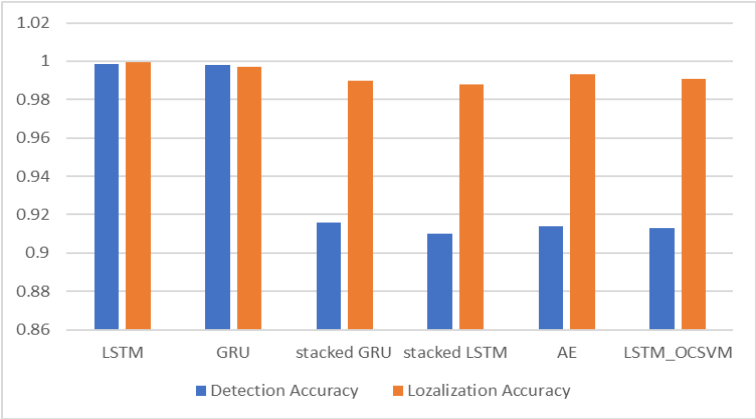

Figure 5.11 Accuracy of the unsupervised models for attack detection and localization.

Upon selecting the LSTM model, the challenge of establishing a consistent threshold for different datasets arises, given the slight variations in optimal thresholds across datasets. To overcome this, multiple datasets with varying parameters were generated. For each dataset, the relationship between the F1 score and various thresholds was charted, as depicted in Figure 5.12. These charts were then consolidated into a single F1 versus threshold curve to determine a unified,

optimal threshold. The optimal thresholds for both detection and localization for the winning LSTM model are 0.00099 for Detection and 0.14 for localization. The unifying threshold will facilitate a fair comparison in Chapter 6.

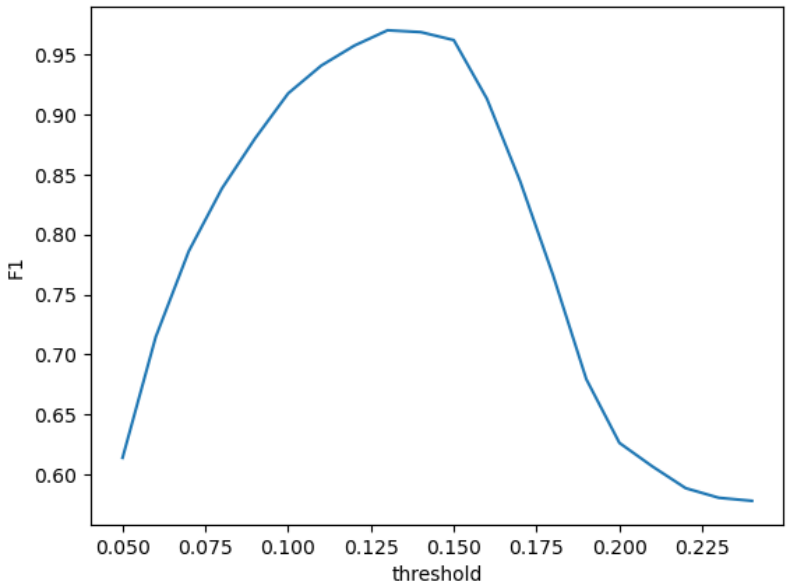

Figure 5.12 Localization threshold vs. F1 score under *x'=0.004,* and *A=10.*

5.3.2 Supervised Model Results

Table 5.3 presents the F1 Score and Accuracy for the studied 4 models. Figure 5.13 shows a graphical representation of the same data.

Table 5.2 Performance of supervised models.

	Detection F1	**Detection Accuracy**
CNN-LSTM	0.983	0.996
BiLSTM	0.81	0.96
stacked GRU	0.961	0.99
stacked LSTM	0.77	0.95

Figure 5.13 F1 and accuracy scores for the supervised models.

The CNN-LSTM model surpasses the other models in performance due to its ability to capture spatial features from the data, followed by Stacked GRU, BiLSTM, and Stacked LSTM. However, its significant disadvantage is the lengthy training time, as shown in Figure 5.14. The CNN-LSTM model's average training duration is approximately 22.5 minutes, which is impractical for the extensive experiments planned in Chapter 6. Therefore, despite its slightly inferior performance compared to CNN-LSTM, the Stacked GRU model, with a more reasonable training time of 11.5 minutes, will be utilized instead.

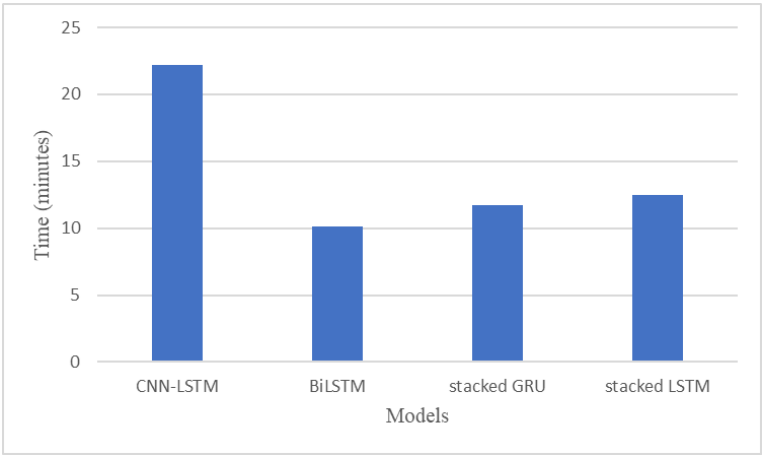

Figure 5.14 Average training time for the supervised models.

Chapter 6: Experimental Evaluation of Effects of Unobservability

In this chapter, the point is finally reached where the conduct of the unobservability analysis can be initiated, given that the necessary SE and attack detection and localization models are now in place. Several experiments are to be conducted in an attempt to answer the questions presented in Section 1.4. This section will be divided into two parts: one using a supervised LSTM model and the other using an unsupervised stacked GRU model, as discussed in Chapter 5. It is important to remember that the supervised models proposed in this study account only for attack detection without localization, while the unsupervised model is capable of both.

6.1 Experiment Based on Unsupervised Model

This section outlines a series of seven experiments to evaluate and compare the performance of the attack detection and localization unsupervised model under unobservability conditions. These experiments will document the performance of SE, alongside assessing the performance of the proposed attack detection model, which fundamentally relies on the performance metrics of SE.

6.1.1 Experiment 1: The Effect of Number of Unobservable Buses on the Detection and Localization Large Intensity Attack

The goal of this experiment is to study the effect of increasing the number of unobservable buses and to observe how the model behaves in response to increasing unobservability. This could assist in determining the minimum number of PMUs required to be installed before the detection model fails to detect and localize the attacks.

The following parameters were utilized in this experiment:

- Attack value $x'=0.04$
- Number of attacked buses $A \in \{2,5,8,10,20\}$
- Number of unobservable buses $k \in \{0,2,5,10,20,35,50,80\}$

Figure 6.1 shows the effect of increasing k on SE performance, while Figure 6.2 shows the effect of increasing k on detection and localization performance.

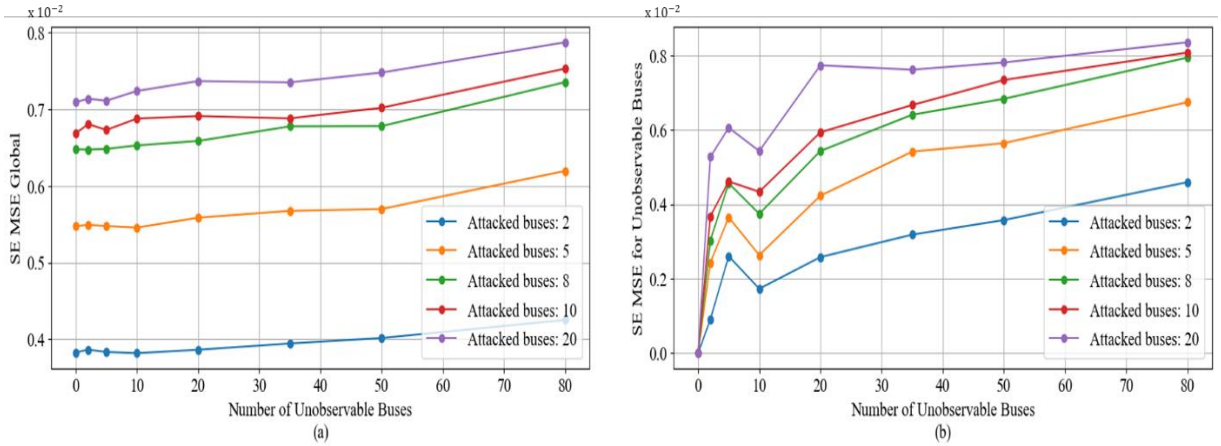

Figure 6.1 The effect of number of unobservable buses k on SE performance with $x'=0.04$ under the unsupervised model. (a) the effect of increasing k on SE MSE across all 118 buses, and (b) the effect of increasing k on SE MSE across only the unobservable buses.

According to Figure 6.2, detection and localization accuracy is significantly impacted by the number of attacked buses since larger-scale attack on many buses leads to a deterioration in SE performance by increasing the MSE as shown in Figure 6.1. Since our model concurrently detects attacks with SE, impaired SE accuracy triggers more thresholds, resulting in a higher number of true alarms (indicative of effective detection) but also an increased rate of false alarms (where normal data is incorrectly flagged as anomalous). Despite this observation does not directly relate to the problem of unobservability being studied, it is important to understand how the model behaves.

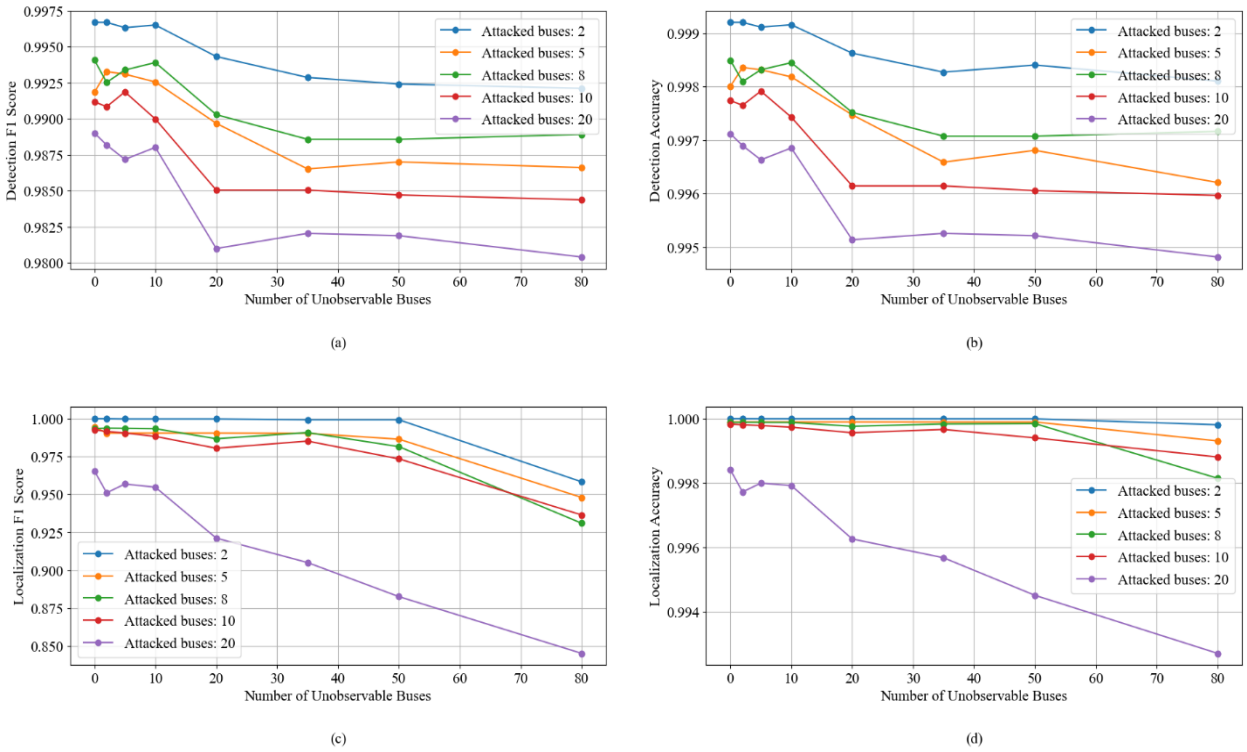

Figure 6.2 The effect of number of unobservable buses k on detection and localization performance with $x'=0.04$ under the unsupervised model. (a) the effect of increasing k on detection F1 score, (b) the effect of increasing k on detection accuracy, (c) the effect of increasing k on localization F1 score, and (d) the effect of increasing k on localization accuracy.

Moreover, an increase in the number of attacked buses results in a decrease in the F1 score, due to compromised SE performance as illustrated in Figures 6.2-a, and 6.2-c. This trend indicates that the detection mechanism is more effective when the attack is confined to fewer buses.

Notably, when the attack was limited to two buses ($A=2$), with either zero or two unobservable buses ($k=0,2$), the model achieved perfect localization of all data points. This is reflected by an F1 score of 1 and an accuracy of 100% in this case as shown in Figures 6.2-c and 6.2-d.

Moreover, it is evident that an increase in the number of unobservable buses negatively affects state estimation as illustrated in Figure 6.1, leading to reduced detection and localization performance according to Figure 6.2. The data demonstrates that detection capabilities degrade

more rapidly once the number of unobservable buses k reaches or exceeds 50, with this decline accelerating as the number of attacked buses A increases.

Finally, we can conclude that the F1 score emerges as a superior metric because it synthesizes *TP, TN, FP, and FN* into a single measure. Despite the less reliable nature of accuracy in highly unbalanced datasets, correlating the F1 score trend with accuracy trends is essential for a comprehensive validation of the model's effectiveness.

6.1.2 Experiment 2: The Effect of Number of Unobservable Buses on the Detection and Localization Low Intensity Attack

This experiment replicates Experiment 1, with the exception that the attack value is reduced ($x' = 0.004$). The objective is to determine how the performance of our models is influenced by the number of unobservable buses when a very low attack value is injected. Below are the parameters of this experiment:

- Attack value $x'=0.004$
- Number of attacked buses $A \in \{2,5,8,10,20\}$
- Number of unobservable buses $k \in \{0,2,5,10,20,35,50,80\}$

Figure 6.3 shows the effect of increasing k on SE performance, while Figure 6.4 shows the effect of increasing k on detection and localization performance.

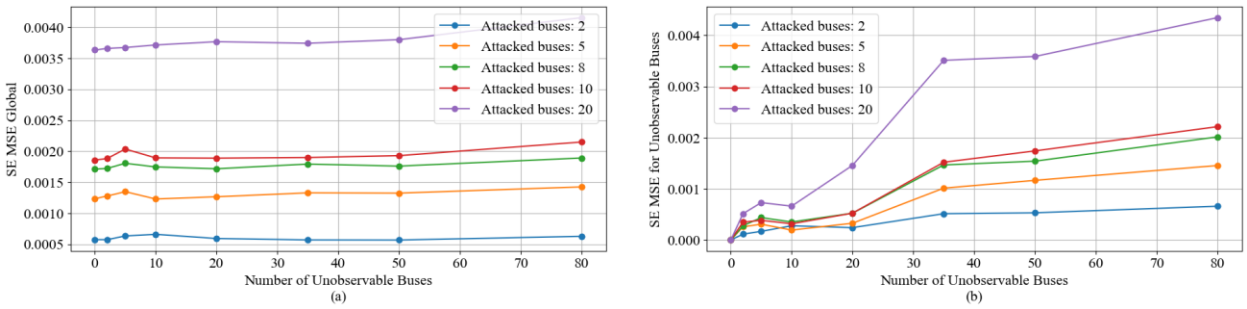

Figure 6.3 The effect of number of unobservable buses k on SE performance with $x'=0.004$ under the unsupervised model. (a) the effect of increasing k on SE MSE across all 118 buses, and (b) the effect of increasing k on SE MSE across only the unobservable buses.

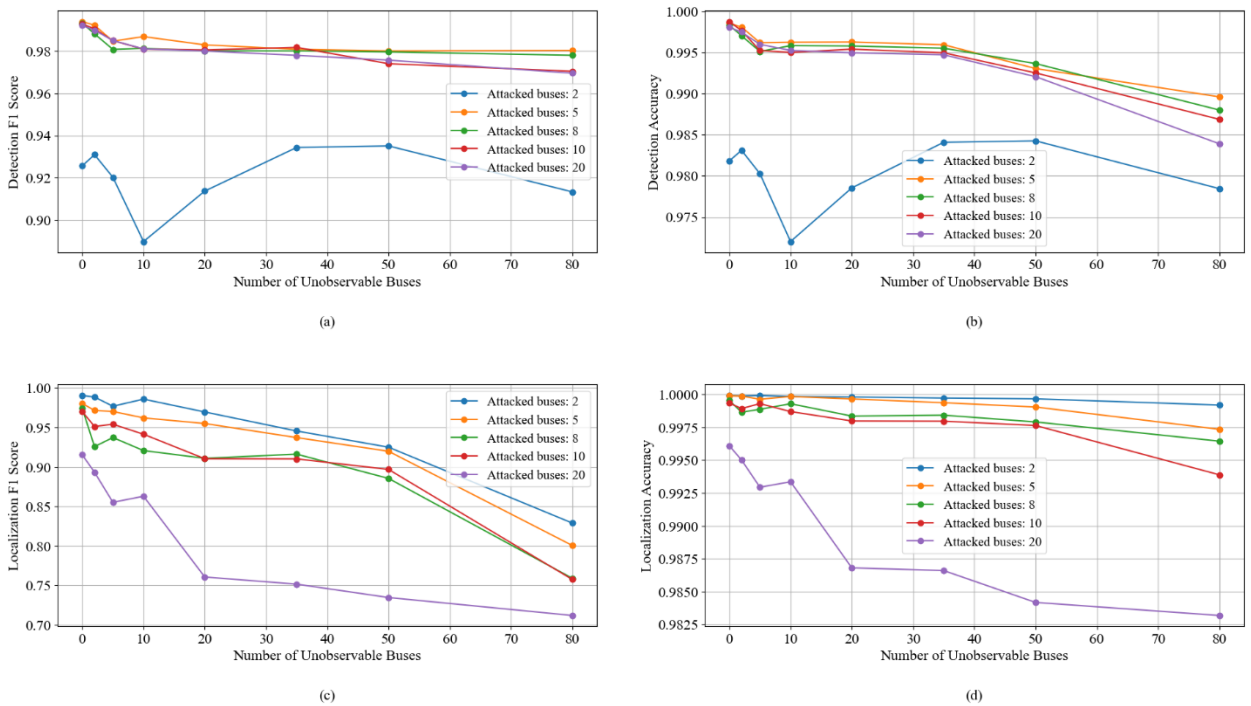

Figure 6.4 The effect of number of unobservable buses *k* on detection and localization performance with $x'=0.004$ under the unsupervised model. (a) the effect of increasing *k* on detection F1 score, (b) the effect of increasing *k* on detection accuracy, (c) the effect of increasing *k* on localization F1 score, and (d) the effect of increasing *k* on localization accuracy.

In line with Experiment 1, as presented in Figure 6.4, it is observed that both the F1 score and accuracy tend to decrease with an increase in the number of unobservable buses *k* and attacked buses *A*. This observation corroborates the initial findings, presenting a consistent pattern across our studies.

An exception was noted in one specific scenario, where the number of attacked buses, *A*, was set to 2. Contrary to other cases, the model's performance in attack detection exhibited unexpected variability, as highlighted by significant reductions in the F1 score and accuracy in Figures 6.4-a and 6.4-b. This outcome was perplexing, given that, according to prior trends, these metrics were anticipated to be at their highest with that condition. This discrepancy led to an investigation into the distinct behavior of the model under these circumstances. Upon closer

examination, it was discerned that this behavior could be linked to the threshold settings, particularly noting the preset threshold of 0.00099 as discussed in Section 5.3. In most experiments, the optimal threshold ranged slightly between 0.00095 and 0.001, which closely matched our predetermined threshold of 0.00099. However, in scenarios involving only two attacked buses, the optimal threshold exhibited significant deviation from the preset value as shown in Table 6.1.

Table 6.1 Detection threshold variation for $A=2$ under $x'=0.004$.

No unobservable buses	**0**	**2**	**5**	**8**	**10**	**20**	**35**	**50**
Set_threshold	0.00099	0.00099	0.00099	0.00099	0.00099	0.00099	0.00099	0.00099
Best_threshold	0.0006	0.00057	0.00065	0.00066	0.00058	0.00056	0.00053	0.00056

This marked shift leads to two inquiries: Why does the best threshold for this case *(A=2)* move to the left? and why is this adjustment not mirrored in scenarios with a higher attack intensity (x'=0.04)? To answer these questions, an exploration of the model's operational dynamics is crucial. The model assesses the MSE across all buses (118) for each time instance, employing this error in our histogram analyses (please refer to Section 5.1.1). With a mere two buses being attacked and at a lower intensity ($x'=0.004$), the aggregated error does not significantly alter the overall MSE per time instance, unlike in scenarios with a greater number of buses or higher attack intensity. As a result, some attacks blend within the error domain of normal data, necessitating a leftward adjustment in the optimal threshold.

Finally, in scenarios with a higher attack intensity of 0.04, the F1 score range for detection was observed to be narrower, spanning from 0.997 to 0.98, as demonstrated in Figure 6.2-a while localization scores varied from a perfect 1 to 0.84 as illustrated in Figure 6.2-c. Conversely, in the

lower intensity scenarios (0.004), excluding the anomalous case with two attacked buses, a wider range was noted: from 0.994 to 0.970 for detection (Figure 6.4-a) and from 0.98 to 0.71 for localization (Figure 6.4-c). This contrast underscores the significant influence of attack intensity on the performance of our model.

6.1.3 Experiment 3: Testing the Optimal PMU Placement Strategies under the Detection and Localization Model High Intensity Attack

The objective of this experiment is to evaluate the performance of various placement strategies, as identified in the literature, within the context of an attack detection model. While these strategies primarily focus on maximizing observability, aspects of attack detection and localization were not previously considered. Therefore, the central inquiry of this experiment is whether the OPP strategies also yield the best configurations for effective attack detection and localization. Based on the work cited in [84], three strategies (S1, S2, S3) will be examined. The specifics of these strategies are detailed in Table 6.2. To assess the effectiveness of various placement strategies, their performance will be compared to the random, unobservable case studied in Experiment 1, which naturally involves random placement. Specifically, we will utilize data from Experiment 1 with k=50, a condition closely resembling Strategy 3's setting of $k=51$. This comparison aims to evaluate and understand the relative performance of these strategies in detecting and localizing attacks. The test parameters are as follows:

- Attack value $x' = 0.04$
- Number of attacked buses $A \in \{2,5,8,10,20\}$

Figure 6.5 shows the effect of increasing A on SE performance, while Figure 6.6 shows the effect of increasing A on detection and localization performance considering the three placement strategies.

Table 6.2 Optimal PMU placement strategies adopted from [84].

Optimal PMU Set	Bus Index	Number of PMUs	Number of unobservable buses
S1	2, 5, 10, 11, 12, 17, 20, 23, 25, 29, 34, 37, 40, 45, 49, 50, 51, 52, 59, 65, 66, 71, 75, 77, 80, 85, 87, 91, 94, 101, 105, 110, 114, 116	34	84
S2	1, 5, 10, 12, 13, 17, 21, 25, 28, 34, 37, 40, 45, 49, 52, 56, 62, 63, 68, 70, 71, 75, 77, 80, 85, 87, 90, 94, 102, 105, 110, 114	32	86
S3	1, 4, 5, 6, 8, 9, 10, 11, 12, 17, 18, 19, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 34, 37, 40, 43, 45, 49, 50, 56, 59, 61, 62, 63, 64, 65, 67, 68, 69, 70, 71, 72, 73, 75, 77, 79, 80, 83, 85, 87, 89, 90, 92, 94, 96, 100, 101, 105, 106, 108, 110, 111, 112, 114, 116, 117, 118	67	51

The observations and conclusions drawn from Experiment 3 will be discussed in conjunction with those from Experiment 4, given their similar structures and the comparative insights they offer.

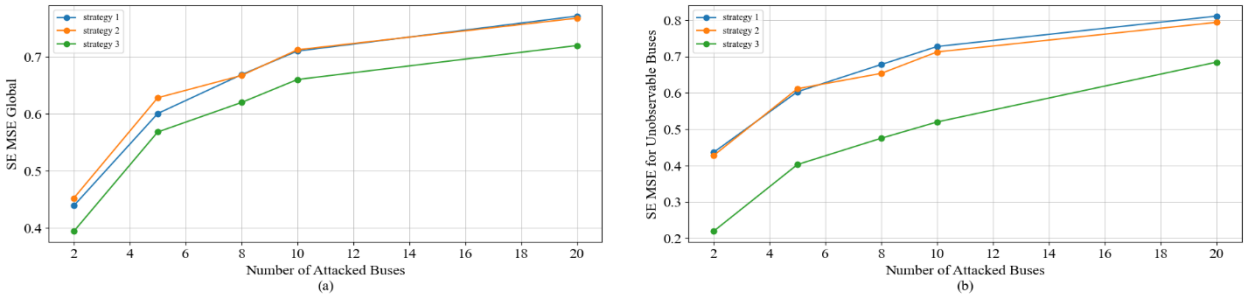

Figure 6.5 The effect of number of attacked buses *A* on SE performance with $x' = 0.04$ for the three placement strategies under the unsupervised model. (a) the effect of increasing *A* on SE MSE across all 118 buses, and (b) the effect of increasing *A* on SE MSE across only the unobservable buses.

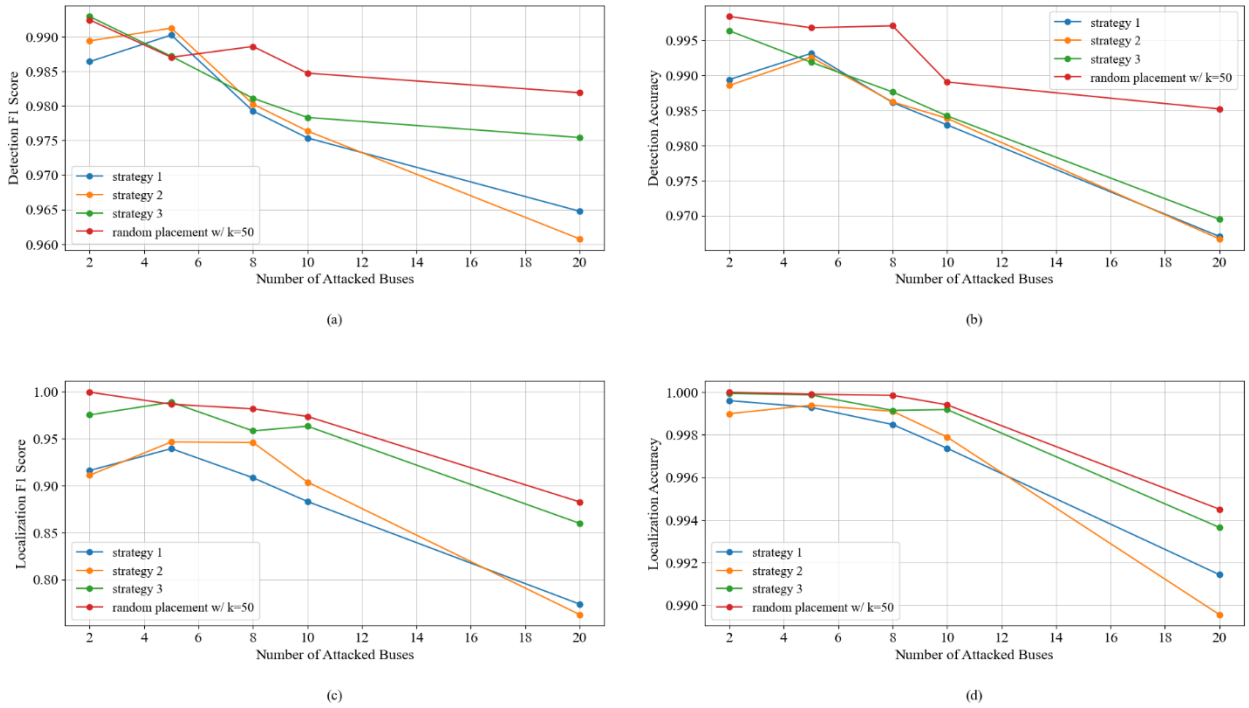

Figure 6.6 The effect of number of attacked buses A on detection and localization performance with x' =0.04 for the three placement strategies under the unsupervised model. (a) the effect of increasing A on detection F1 score, (b) the effect of increasing A on detection accuracy, (c) the effect of increasing A on localization F1 score, and (d) the effect of increasing A on localization accuracy.

6.1.4 Experiment 4: Testing the Optimal PMU Placement Strategies under the Detection and Localization Model Low Intensity Attack

Experiment 4 replicates Experiment 3, with the exception that the attack intensity is reduced to $x' = 0.004$. Figure 6.7 shows the effect of increasing A on SE performance, while Figure 6.8 shows the effect of increasing A on detection and localization performance considering the three placement strategies with the low intensity attack of $x' = 0.004$.

The outcomes of Experiment 3 with an intensity $x' = 0.04$ (Figure 6.6) and Experiment 4 with an intensity $x' = 0.004$ (Figure 6.8) showed analogous trends, revealing a uniform model response across varying levels of attack intensity. Naturally, the model exhibited improved performance in scenarios characterized by less severe attacks.

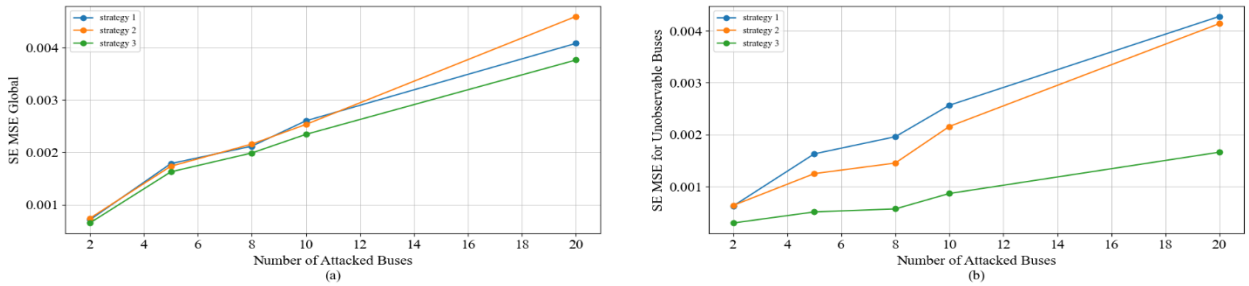

Figure 6.7 The effect of number of attacked buses A on SE performance with $x' = 0.004$ for the three placement strategies. (a) the effect of increasing A on SE MSE across all 118 buses, and (b) the effect of increasing A on SE MSE across only the unobservable buses.

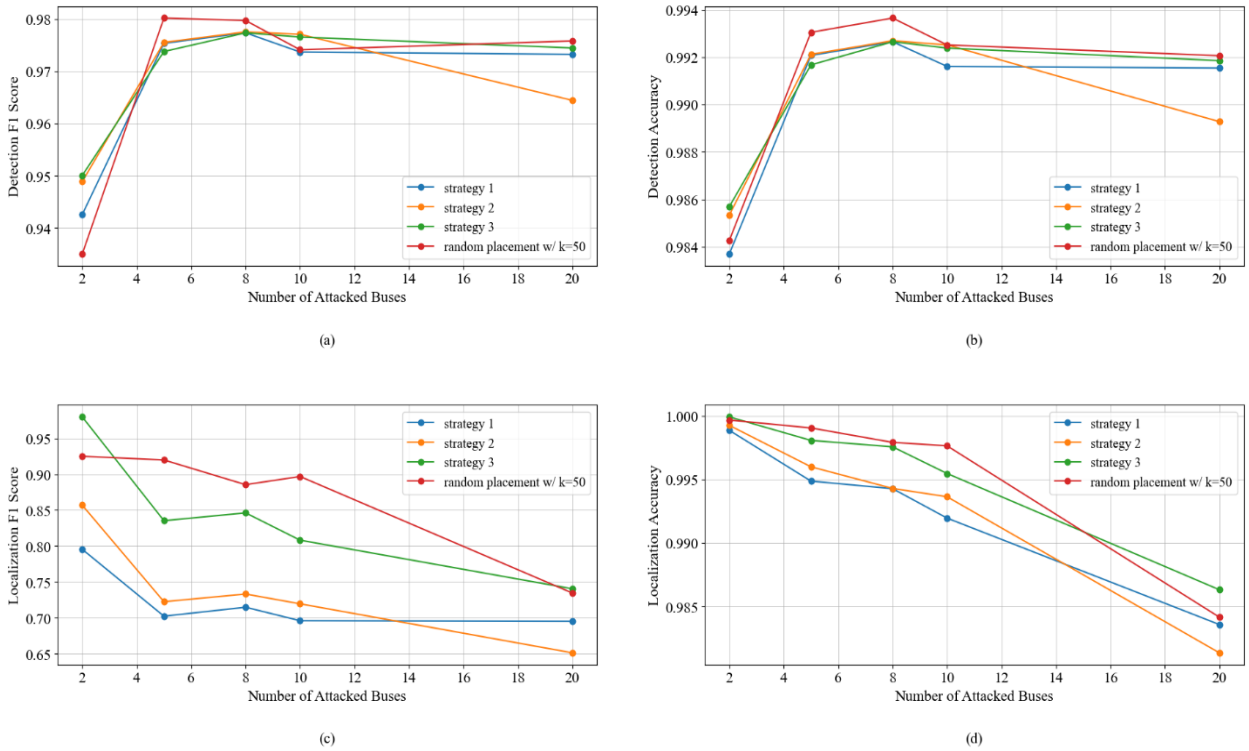

Figure 6.8 The effect of number of attacked buses A on detection and localization performance with $x' = 0.004$ for the three placement strategies under the unsupervised model. (a) the effect of increasing A on detection F1, (b) the effect of increasing A on detection accuracy, (c) the effect of increasing A on localization F1 score, and (d) the effect of increasing A on localization accuracy.

As expected, S3 outperformed S1 and S2 in both detection and localization as shown in Figures 6.6 and 6.8. This can be attributed to the number of unobservable buses—51 for S3 as opposed to 84 and 86 for S1 and S2, respectively.

Furthermore, referring to the same figure, S2 surpasses S3 in performance when the number of attacked buses is equal to or less than 12-14. However, as the number of attacked buses exceeds 14, S3 shows better performance in detection and localization. This highlights the dynamic efficiency of S3 in handling wider-ranged attacks.

Comparison between S3 and the random placement with k=50 as adopted in Experiments 1 and 2, reveals that random placement outperforms S3 in both detection and localization in most of the cases. This is illustrated in Figures 6.7 and 6.9, where the random placement is depicted by the red line, contrasting with the green line that represents S3. Thus, it can be concluded that although these placement strategies satisfy the condition of full observability; however, in terms of attack detection these combinations may perform worse than our average. This implies the conclusion that the optimum placement sets – although achieving high observability – can cause more attack threat probability than other combinations. That could mean also that we might need to add some PMUs at some specific points to increase the detection and localization accuracy, which is the aim of experiment 5 to check the effect of each bus on the model performance.

6.1.5 Experiment 5: Assessing Detection and Localization with Sequentially Unobservable Buses – One at a Time.

The objective of this experiment is to identify specific locations within the power grid where the absence of PMUs or lack of observability might lead to diminished performance in attack detection and localization. It posits that equipping such critical buses with PMUs is essential. In this experiment, each bus will be made unobservable in turn, with the model's performance evaluated at each instance. The setup for the experiment is as follows:

- Attack value $x' \in \{0.04, 0.004\}$
- Number of attacked buses $A = 8$ (fixed)

Figure 6.9 shows the model performance in terms of F1 score and accuracy over the 118 buses for both intensities $x' \in \{0.04, 0.004\}$.

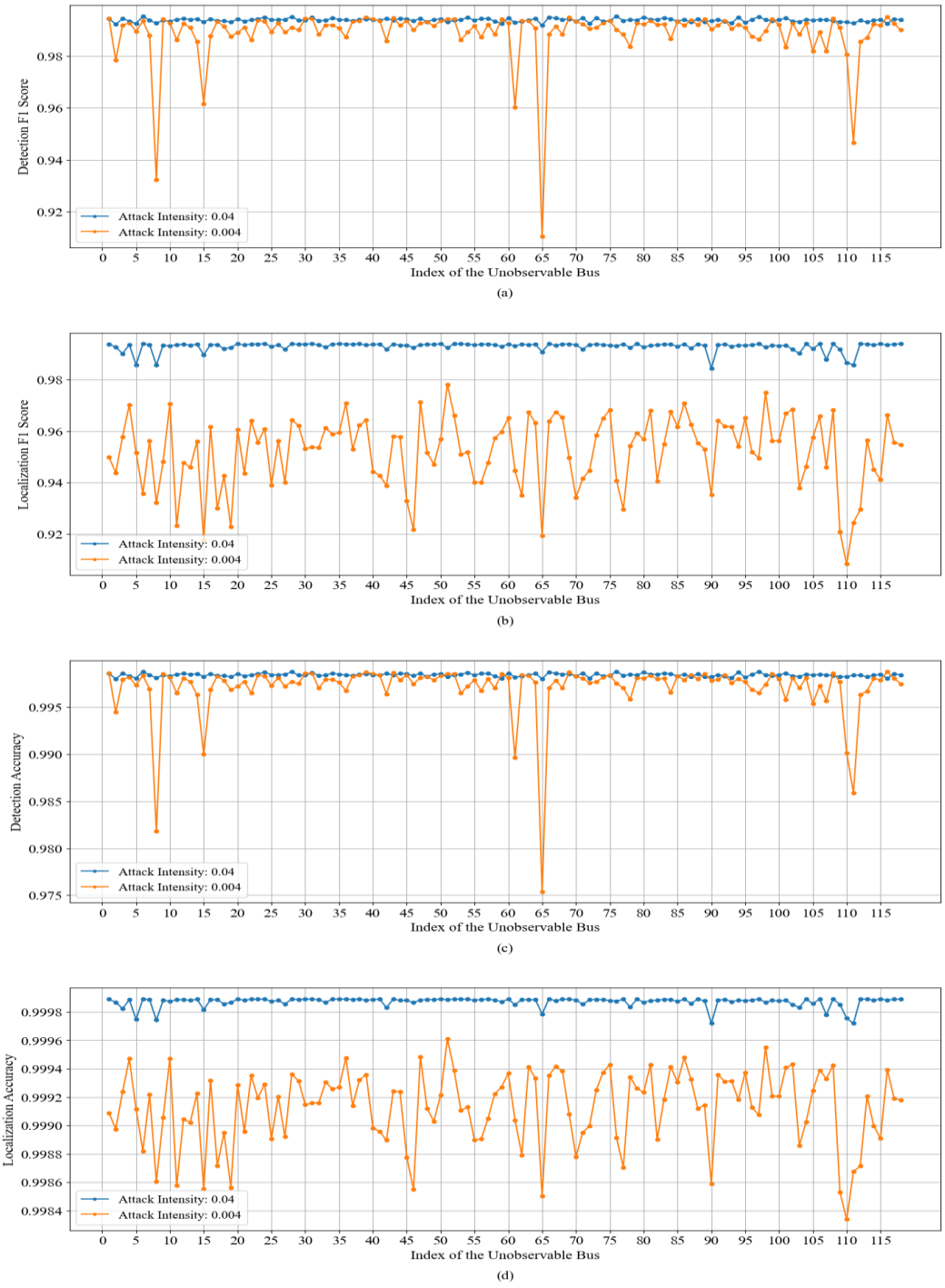

Figure 6.9 Detection performance across the 118 buses under the unsupervised model, with each bus being unobserved one at a time. (a) detection F1 score, (b) detection accuracy, (c) localization F1 score, and (d) localization accuracy.

Following the mentioned Figure, A drop in the F1 score and accuracy for the high-intensity attack $x' = 0.04$ when a bus is unobservable is likely to be followed by a drop at the same bus for the low-intensity attack $x' = 0.004$. However, the converse does not necessarily hold. A drop in performance at a specific bus with a low-intensity attack does not necessarily imply a similar drop with a higher intensity.

Furthermore, from the analysis of the graphs shown in Figure 6.9, it can be inferred that the absence of PMUs at certain specific buses leads to a significant drop in detection and localization performance, especially with low-intensity attacks. Buses such as 11, 15, 46, 65, 109, 110, and 111 are identified as requiring PMUs, regardless of whether the PMU placement strategy originally includes them.

Finally, generally, though not always, the weak points for both detection and localization tend to be consistent.

6.1.6 Experiment 6: Effect of Unobservability of Large Regions on the Detection and Localization Performance

The objective of this experiment is to evaluate the influence of clustering on detection and localization accuracy, drawing upon the work from [7]. In the cited work, the authors propose a multi-regional distributed SE, utilizing K-means clustering to divide the IEEE-118 bus system into five regions as delineated in Figure 6.10 below. The five regions have “almost” equal number of PMUs on each. Table 6.3 shows what PMUs belong to what region.

Originally, the purpose behind dividing the network into regions was to perform SE independently within each region using a local edge server. However, for this experiment, a different premise is considered: these edge servers act as local switches for their respective regions, forwarding the collected data to a control center for secondary analysis of the entire network. The

central question being addressed is the impact of a failure in one of these edge servers (due to physical disconnection or a cyber-attack) on detection and localization performance. Specifically, are some regions more critical than others, necessitating redundancy?

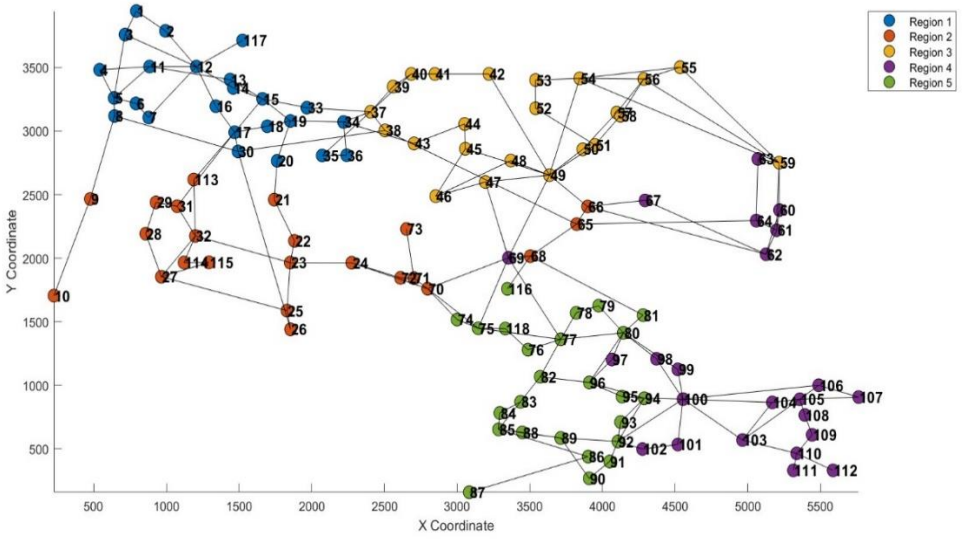

Figure 6.10 The five distributed SE regions- based on the region definition adopted from [7].

Table 6.3 PMUs for each of the five regions used for distributed state estimation-adopted from [7].

Region	BUS index	Number of PMUs
R1	1,2,3,4,5,6,7,8,11,12,13,14,15,16,17,18,19,20,30,33,34,35,36,117	24
R2	9,10,21,22,23,24,25,26,27,28,29,31,32,65,66,68,70,71,72,73,113,114,115	23
R3	37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,56	23
R4	59,60,61,62,63,64,67,69,97,98,99,100,101,102,103,104,105,106,107,108,109,110 ,111,112	24
R5	74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96,116,118	25

In this setup, each region will be considered unobservable in turn, and the impact on performance will be systematically analyzed. Below is the setup for this experiment:

- Attack value $x' \in \{0.04, 0.004\}$
- Number of attacked buses A= 8 (Fixed)

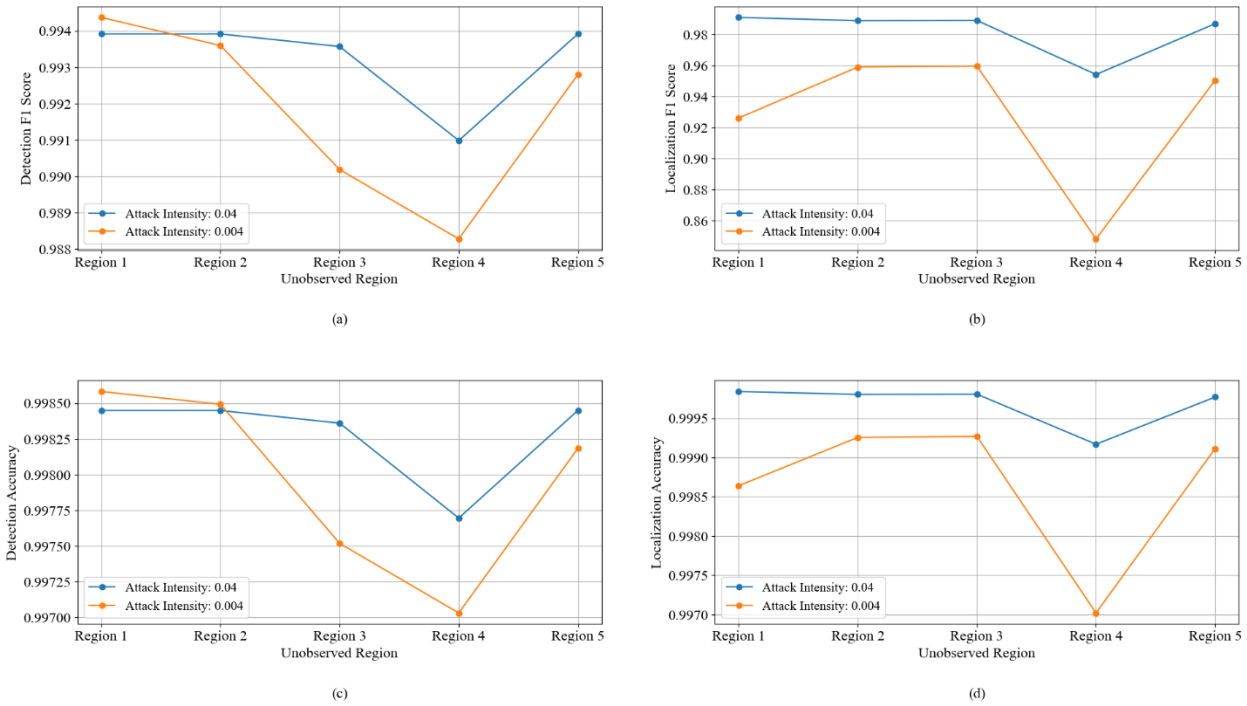

Figure 6.11 The impact of lack of unobservability on large defined regions on the detection and localization performance with high and low intensity attack under the unsupervised model. (a) detection F1 score, (b) detection accuracy, (c) localization F1 score, and (d) localization accuracy.

The analysis reveals that certain regions hold greater significance than others in terms of unobservability's impact. Specifically, with respect to detection, the unobservability of regions 3 and 4 markedly impairs detection capabilities as shown in Figures 6.11-a and 6.11-b. In terms of localization, performance significantly deteriorates when regions 1 and 4 are unobservable as illustrated in Figures 6.11-c and 6.11-d. Region 4 emerges as critical for observation, underscoring the necessity of maintaining uninterrupted connectivity to its local edge server. In essence, this indicates that redundancy is indispensable for region 4.

6.1.7 Experiment 7: Effect of Unobservable Clustered PMUs on the Detection and Localization Performance

This experiment extends the methodology of the previous one by dividing the region into smaller geographical units, resulting in a total of 17 clusters as outlined in Figure 6.12, and Table

6.4. It is important to note that the buses within each cluster are closely sequenced in terms of their indices. Consequently, obscuring a single cluster during the model's training phase leads to the concealment of a sequence of adjacent features.

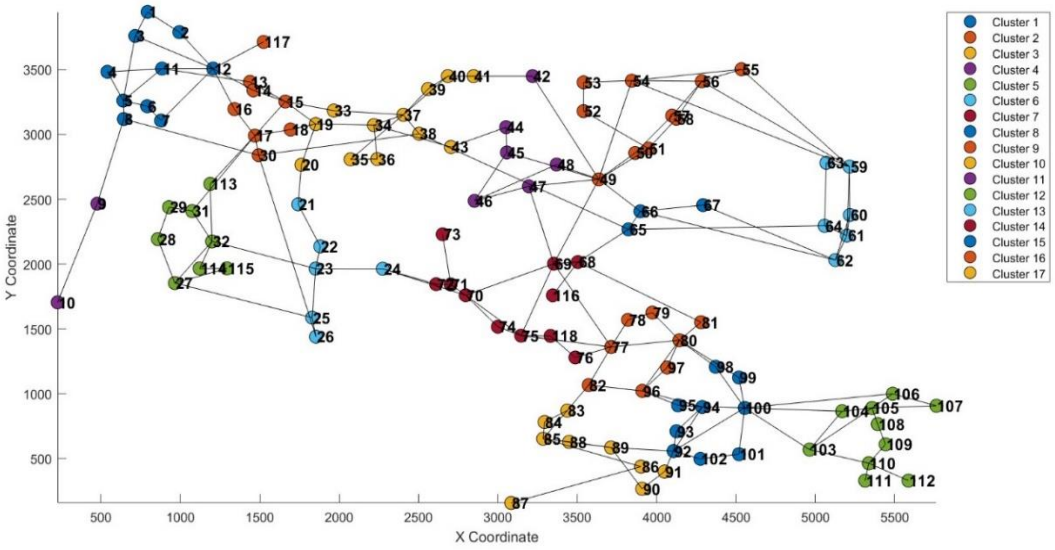

Figure 6.12 The clusters adopted in experiment 7.

Table 6.4 PMUs in each cluster in Experiment 7.

Clusters	BUS index	Number of PMUs
C1	1,2,3,4,5,6,7,8,11,12	10
C2	13,14,15,16,17,18,30,117	8
C3	33,34,35,36,19,20	6
C4	9,10	2
C5	28,27,114,115,32,31,29,113	8
C6	21,22,23,25,26,24	6
C7	70,71,72,73,	4
C8	65,66,67	3
C9	49,50,51,52,53,54,55,56,57,58,56	10
C10	37,38,39,40,41,43	6
C11	42,44,45,46,47,48	6
C12	103,104,105,106,107,108,109,110,111,112	10
C13	59,60,61,62,63,64	6
C14	69,68,116,74,75,118,76	7
C15	98,99,100,94,95,93,92,102,101	9
C16	78,79,77,82,96,97,80,81	8
C17	83,84,85,88,89,86,91,90,87	9

The purpose of this experiment is to investigate the impact of clustering by examining how the model's behavior changes when multiple clusters are hidden simultaneously. The process begins with obscuring just one cluster, followed by repeating this procedure with 15 different clusters chosen at random and compiling the results. The experiment then progresses to hiding two clusters at a time, with this step also being repeated 15 times, and continues in this manner.

Given the division into 17 clusters, hiding an additional cluster equates to obscuring approximately 7 more buses each time. Thus, hiding two clusters results in a total of 14 buses being concealed, three clusters lead to 21 hidden buses, and so on. This detail is crucial for drawing comparisons with the outcomes of Experiments 1 and 2, where the hiding strategy involved scattered buses. For a valid comparison, an equivalent number of unobserved scattered buses adopted from the first 2 experiments will be plotted, such that the number of unobservable scattered buses matches the number of unobservable buses at that cluster. For example, with three unobservable clusters, the average number of unobservable buses will be twenty-one. Thus, at the same point, the results from twenty-one scattered unobservable buses will be plotted. Below is the setup for this experiment:

- Attack value $x' \in \{0.04, 0.004\}$
- Number of unobserved clusters $C \in \{1,2,3,4,5,6,7,8,9,10\}$

In line with expected outcomes, an increase in the number of unobservable clusters correlates with a noticeable decline in our evaluation metrics as observed in Figure 6.13.

While not universally applicable, it is generally observed that, compared to the results from Experiments 1 and 2 in Figures 6.2 and 6.4, performance tends to improve when the unobservable buses are clustered.

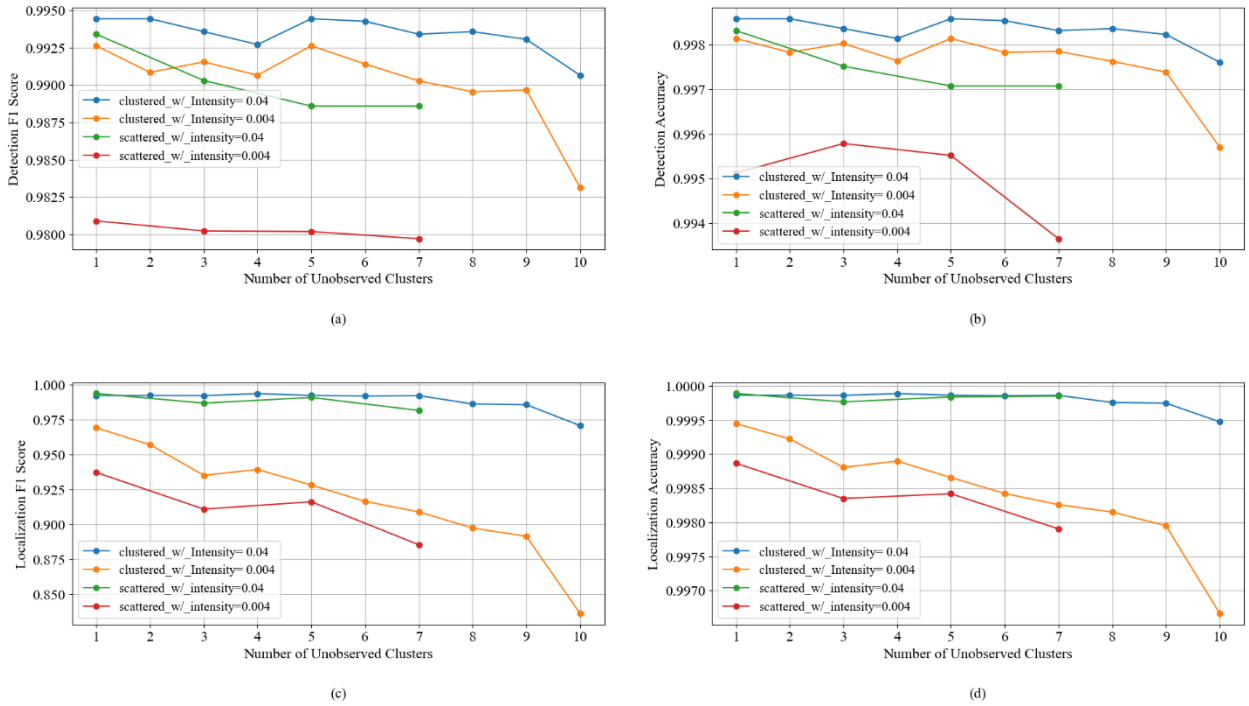

Figure 6.13 The impact of unobservable clustered PMUs on the detection and localization performance with high and low intensity attack under the unsupervised model. (a) detection F1 score, (b) detection accuracy, (c) localization F1 score, and (d) localization accuracy.

6.2 Experiment Based on Supervised Model

In this section, the experiments conducted in Section 6.1 are replicated with the setup remaining identical, with some key differences concerning the model's operational mechanism. These differences are outlined as follows: Unlike the unsupervised model, the training data, in this case, incorporates attacks, with a similar ratio to that observed in the testing data. Furthermore, SE is employed solely for the purpose of estimating the values of the unobserved buses, not all buses as in the unsupervised model scenario. The estimated values for the unobservable buses are then combined with the actual values of the observed buses. This aggregated dataset is subsequently input into the detection model, where F1 scores and accuracy metrics are calculated for each experiment. It is important to mention that these experiments are essentially duplicates of those detailed in Section 6.1; therefore, only the results of these experiments will be discussed in this

section. For comprehensive details regarding the setup of each experiment, a reference to Section 6.1 is recommended.

6.2.1 Experiment 1: The Effect of Number of Unobservable Buses on the Detection Large Intensity Attack

Figures 6.14 show the effect of increasing k on SE performance, while Figure 6.15 shows the effect of increasing k on detection performance.

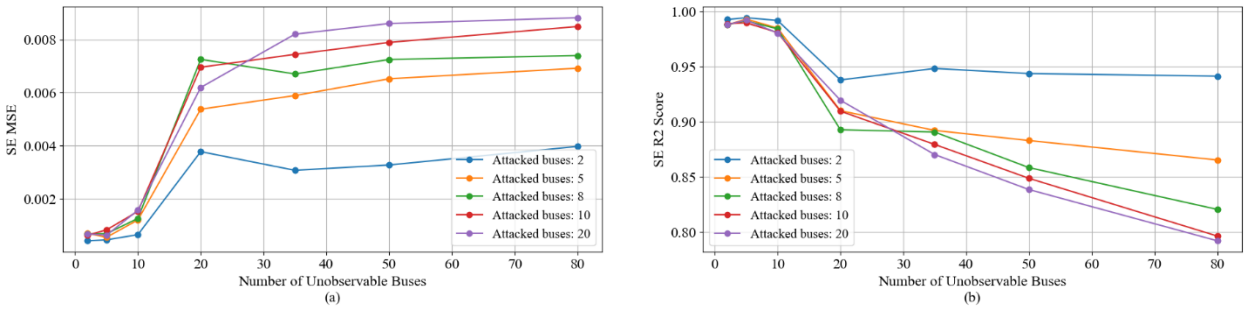

Figure 6.14 The effect of number of unobservable buses k on SE performance with $x'=0.04$ under the supervised model. (a) the effect of increasing k on SE MSE, and (b) the effect of increasing k on SE R^2 score.

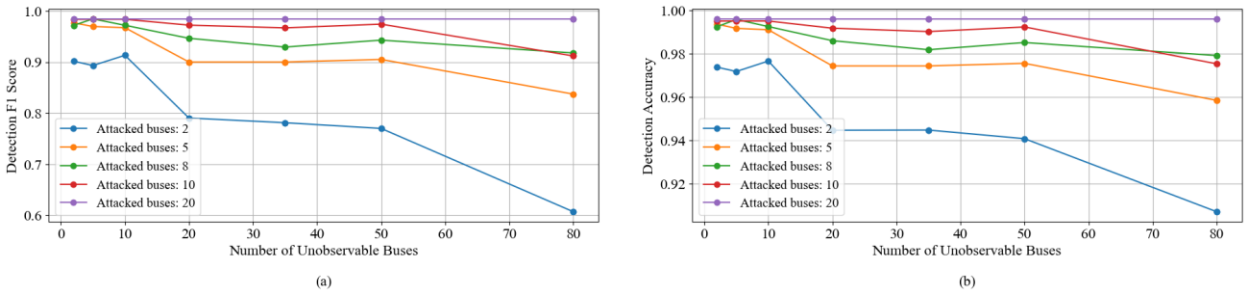

Figure 6.15 The effect of number of unobservable buses k on detection and localization performance with $x'=0.04$ under the supervised model. (a) the effect of increasing k on detection F1 score, and (b) the effect of increasing k on detection accuracy.

The data presented in Figures 6.14 and 6.15 align with the observations and trends previously identified in Figures 6.1 and 6.2. Specifically, as the number of unobservable buses k increases, SE performance deteriorates. This is illustrated by an increase in MSE (Figure 6.14-a)

and a decrease in the R^2 score (Figure 6.14-b). Moreover, with the rise in the number of unobservable buses *k*, there is a notable decline in the detection F1 score and accuracy, as shown in Figure 6.15. Two significant drops are observed: one after *k* exceeds 20 and another when *k* surpasses 50. This latter observation correlates with findings from Section 6.1.1, where a rapid performance decline was noted once *k* exceeded 50 in the context of the unsupervised model. Consequently, it is advisable to keep *k* below 50 to maintain reasonable performance levels.

Additionally, although not directly linked to the issue of observability, it is important to highlight that supervised and unsupervised models used in this thesis function inversely. In scenarios of large-scale attacks on numerous buses, large *A*, unsupervised models demonstrate reduced detection efficiency due to the significantly affected SE, as illustrated in Figures 6.2-a and 6.2-b. Conversely, supervised models exhibit improved detection capabilities as the scale of the attack increases.

6.2.2 Experiment 2: The Effect of Number of Unobservable Buses on the Detection Low Intensity Attack

Figures 6.16 show the effect of increasing *k* on SE performance, while Figure 6.17 shows the effect of increasing *k* on detection performance.

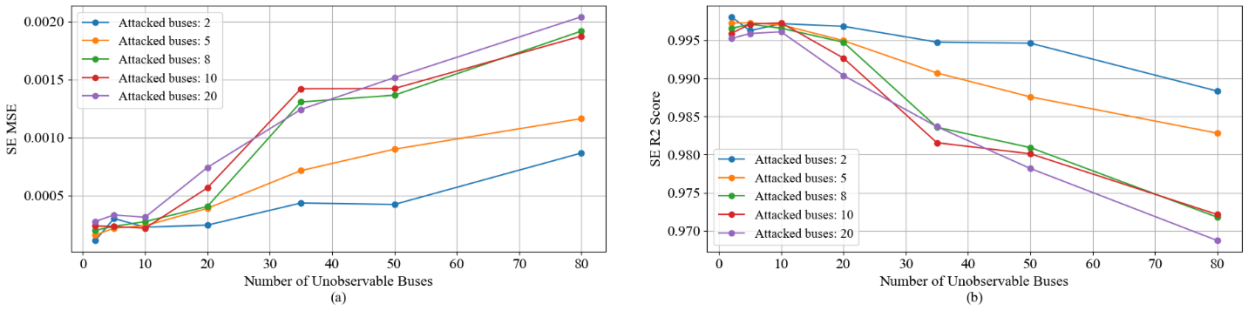

Figure 6.16 The effect of number of unobservable buses *k* on SE performance with $x'=0.004$ under the supervised model. (a) the effect of increasing *k* on SE MSE, and (b) the effect of increasing *k* on SE R^2 score.

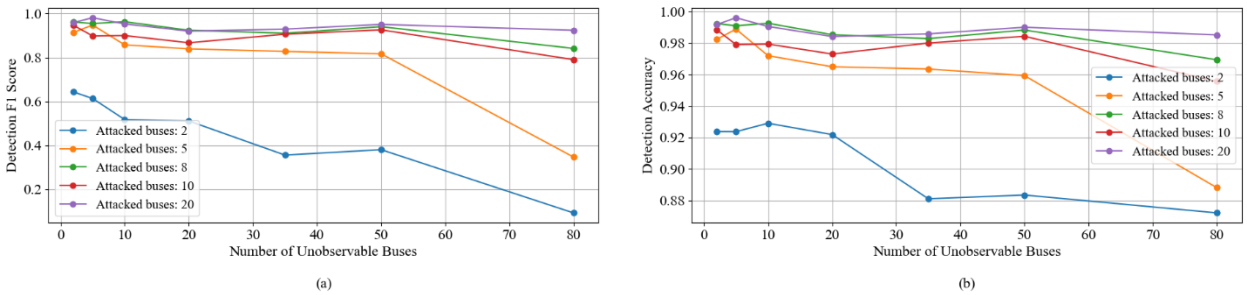

Figure 6.17 The effect of number of unobservable buses k on detection and localization performance with $x'=0.004$ under the supervised model. (a) the effect of increasing k on detection F1 score, and (b) the effect of increasing k on detection accuracy.

The trends presented in Figures 6.16 and 6.17 are confirmed to align with expectations based on observations from Sections 6.1.2 and 6.2.1. As the number of unobservable buses k increases, an increase in SE MSE is observed, alongside a decrease in the R^2 score, and a reduction in attack detection F1 score and accuracy. A significant decrease in performance is observed in Figure 6.17-a, as previously demonstrated in Figure 6.15 when k exceeds 50. It is also noteworthy that a significant drop in detection performance is seen in this scenario, with a detection rate of $x'=0.004$, compared to the $x'=0.04$ result found in Section 6.2.1. The model's effectiveness in detecting attacks is completely compromised when $A=2$ and k reaches 80.

6.2.3 Experiment 3: Testing the Optimal PMU Placement Strategies with Detection High Intensity Attack

Figure 6.18 shows the effect of increasing A on SE performance, while Figure 6.19 shows the effect of increasing A on detection performance considering the three placement strategies.

Given the similarities between Experiments 3 and 4 outcomes, their conclusions will be discussed together at 6.2.4.

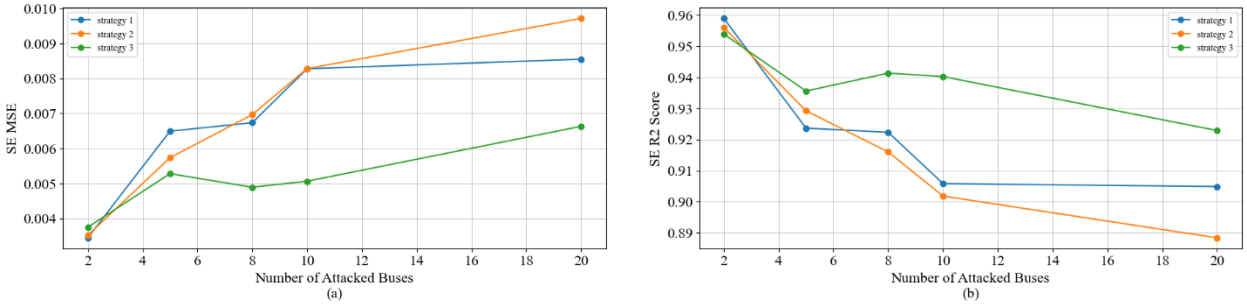

Figure 6.18 The effect of number of attacked buses A on SE performance with $x' = 0.04$ for the three placement strategies under the supervised model. (a) the effect of increasing A on SE MSE, and (b) the effect of increasing k on SE R^2 score.

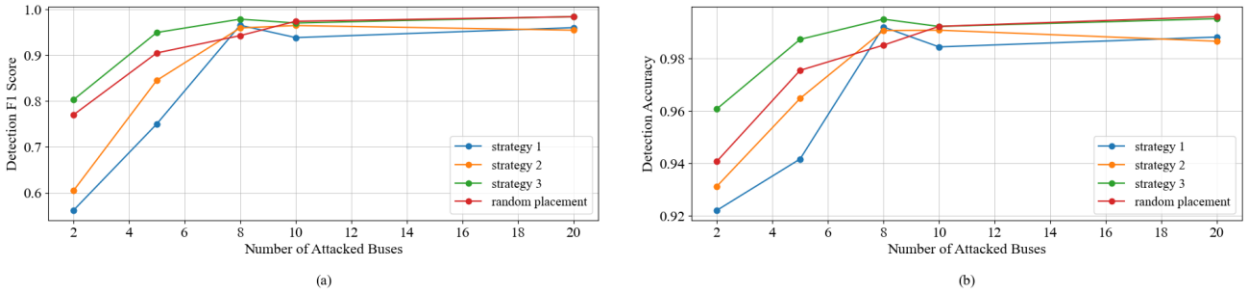

Figure 6.19 The effect of number of attacked buses A on detection performance under $x' = 0.04$ for the three placement strategies. (a) the effect of increasing A on detection F1 score, (b) the effect of increasing A on detection accuracy

6.2.4 Experiment 4: Testing the Optimal PMU Placement Strategies with Detection Low Intensity Attack

Experiment 4 replicates Experiment 3, with the exception that the attack intensity is reduced to $x' = 0.004$. Figure 6.20 shows the effect of increasing A on SE performance, while Figure 6.21 shows the effect of increasing A on detection performance considering the three placement strategies with the low intensity attack of $x' = 0.004$.

It can be observed that similar patterns are observed between Experiments 3 and 4, where Strategy S3 demonstrates superior performance over Strategies S1 and S2, as indicated in Figures 6.19 and 6.21. Strategy S2 outperforms S1 when the attack size A is below 16.

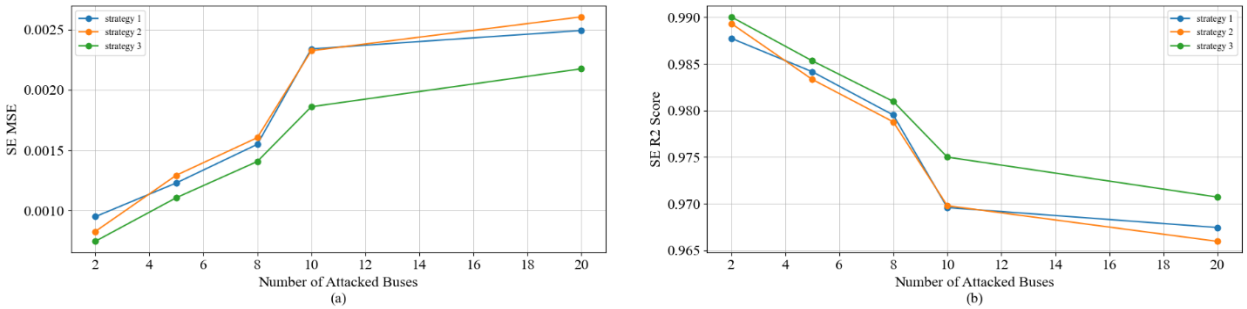

Figure 6.20 The effect of number of attacked buses A on SE performance with $x' = 0.004$ for the three placement strategies under the supervised model. (a) the effect of increasing A on SE MSE, and (b) the effect of increasing k on SE R^2 score.

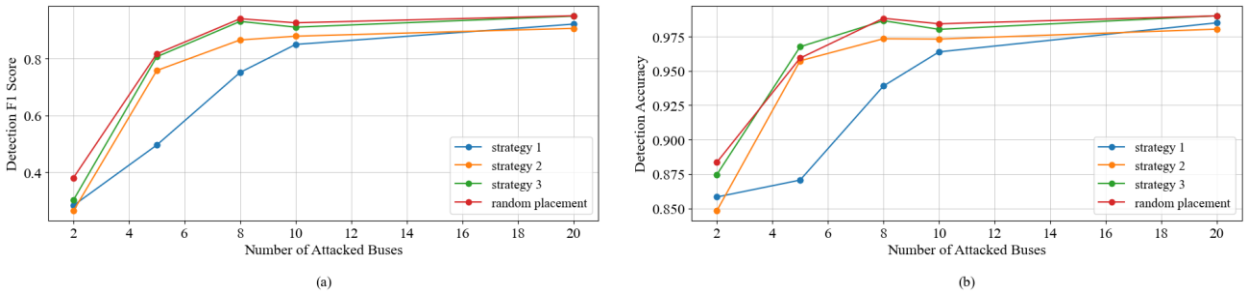

Figure 6.21 The effect of number of attacked buses A on detection performance under x' =0.004 for the three placement strategies under the supervised model. (a) the effect of increasing A on detection F1 score, (b) the effect of increasing A on detection accuracy

However, once A exceeds 16, these dynamic reverses, with S1 surpassing S2 in performance. This trend closely mirrors the results depicted in Figure 6.6 from Section 6.1.3 and Figure 6.8 from Section 6.1.4 for the unsupervised model, with a notable deviation in the transition point between S1 and S2; in the earlier sections, this shift occurs when A is between 12 and 14, whereas in the current analysis, it is observed between 16 and 18. Furthermore, the conclusion reached in Section 6.1.4 remains applicable: although these placement strategies enhance observability to the highest degree, they do not necessarily translate to the most effective attack detection capabilities. This assertion is further substantiated by the findings presented in Figures 6.20 and 6.22 where the random placements adopted from Experiments 1 and 2 with $k=50$ outperform S3 performance. Although for the case with x' =0.04, S3 outperforms the random

placement when $A<10$, as shown in Figure 6.20, the conclusion remains true for all the other cases tested in this work.

6.2.5 Experiment 5: Assessing Detection with Sequentially Unobservable Buses – One at a Time

Similar to Section 6.1.5, this experiment seeks to evaluate the influence of individual buses on the performance of the detection model. By systematically unobserving one bus at a time, the aim is to identify specific buses whose absence notably diminishes the model's accuracy. Figure 6.22 illustrates the variations in F1 score and detection accuracy corresponding to each bus being unobserved sequentially.

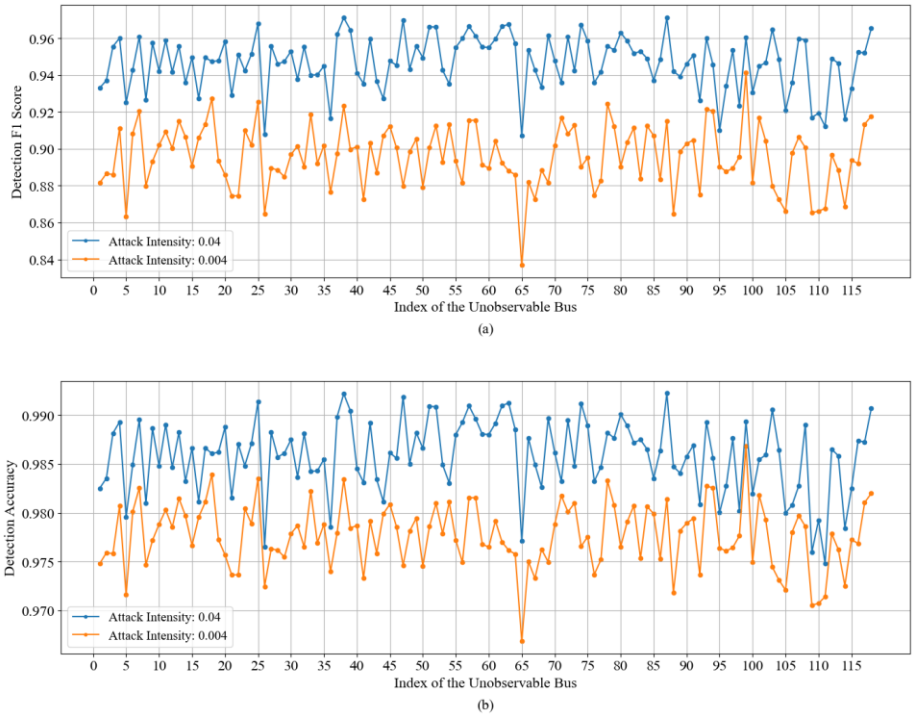

Figure 6.22 Detection performance across the 118 buses under the supervised model, with each bus being unobserved one at a time. (a) detection F1 score, (b) detection accuracy.

Mirroring the insights obtained from Section 6.1.5, the analysis presented in Figure 6.22 reveals consistent trends within the system across both low and high-attack scenarios. Furthermore, some buses, when unobserved, are considered to have a high impact on detection

capabilities. Identifying and monitoring these weak points is crucial for maintaining system security. Notably, some of these crucial buses, such as buses 65, 109, 110, and 111, are commonly identified by both supervised and unsupervised models, as highlighted in Figures 6.22 and 6.9, respectively. This consistency underscores a shared understanding of system dependencies and critical features across different modeling approaches. However, the emergence of new sensitive buses to unobservability in the supervised model analysis—such as buses 5, 26, and 46—underscores the distinct detection capabilities of both supervised and unsupervised models.

6.2.6 Experiment 6: Effect of Unobservability of Large Regions on the Detection Performance

Figure 6.23 shows the F1 score and accuracy when unobserving each of the five regions at a time that was introduced in Section 6.1.6

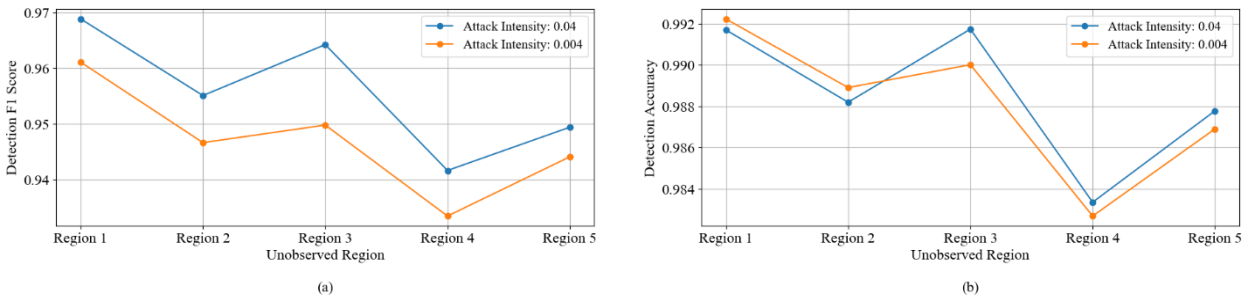

Figure 6.23 The impact of lack of observability on large defined regions on the detection performance with high and low intensity attacks under the supervised models. (a) detection F1 score, (b) detection accuracy.

As observed in Figure 6.23, certain regions exert a more pronounced impact on attack detection performance when left unobserved. According to the data from Figure 6.23 in Section 6.1.6 related to the unsupervised model, region 4 was identified as having the most significant impact, followed by region 3. In the experiments involving the supervised model, region 4 continues to show the highest negative influence upon being unobserved, with Region 5 emerging as the second most impactful, replacing Region 3. Therefore, the findings affirm the critical

importance of region 4 in the context of attack detection. Consequently, it is advisable to consider the deployment of a redundant edge server in Region 4 in case the primary server encounters failure.

6.2.7 Experiment 7: Effect of Unobservable Clustered PMUs on the Detection Performance

Figure 6.24 illustrates the F1 score and accuracy against the number of unobserved clusters. Consistently, performance declines with an increase in the number of unobservable clusters. Moreover, this experiment's results validate the observation in Section 6.1.7 that clustering unobserved PMUs, as opposed to scattering them randomly, often leads to improved performance. This is evident when comparing Figure 6.24, which represents clustered unobserved PMUs, with Figures 6.15 and 6.17, where the unobserved PMUs are dispersed.

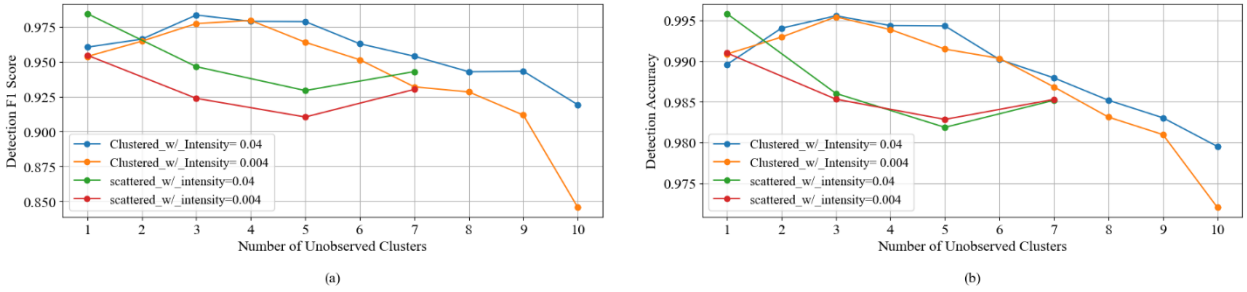

Figure 6.24 The impact of the number of unobservable clustered PMUs on the detection performance with high and low intensity attacks under the supervised model. (a) detection F1 score, (b) detection accuracy.

6.3 Experiments Conclusions and Remarks

The findings from this thesis present compelling insights into how unobservability affects the performance of the two distinct models in FDIA detection. The analysis indicates consistent trends across both models: performance deteriorates as the number of unobservable buses increases, specific buses becoming unobservable can significantly reduce performance, and clustering unobservable buses tends to yield better results.

However, the conducted experiments highlight the superior performance of the unsupervised model over its supervised counterpart used in this thesis, attributing this to several advantages: the unsupervised model is more adaptable to various types of anomalous data, simpler and quicker training process, and can localize attacks without extensive training on numerous features. In contrast, the supervised model requires detailed training on specific attacks, making it less efficient in detecting new or varied attacks. It also demands considerable time for training, as it involves training both the SE model followed by detection model and struggles with attack localization without extensive feature training. For these reasons, the unsupervised model demonstrates superior overall performance. However, while the unsupervised model generally outperforms the supervised model, the latter may have an edge in detecting large-scale attacks while the unsupervised model performance is being hindered by these large attacks.

In conclusion, while there are some differences between the performance and operation of both models, the consistent trend across both underscores that despite the model being used, unobservability inherently poses a significant threat to the effectiveness of cyber-attack detection.

Chapter 7: Conclusions and Future Work

7.1 Conclusions

Drawing upon the detailed analyses and findings from the experiments conducted, the conclusion of this thesis underscores several insights into the cybersecurity of smart grids, particularly focusing on the aspects of detection and localization accuracy in the face of cyber-attacks like FDIA under conditions of unobservability. The research meticulously outlined the significant impact that the number and distribution of unobservable buses have on the overall effectiveness of state estimation processes, detection, and localization accuracy.

It was demonstrated through many experiments with different parameters that the number of unobservable buses affects the detection and localization of the attacks. The work presented can give insights to the utilities on the minimum number of PMU units that must be installed in order to ensure system security and reliability. Moreover, through comprehensive experimentation, it was demonstrated that not all buses and regions within the grid hold equal significance in terms of maintaining system security. Specific buses and regions were identified as crucial nodes whose observability significantly influences the grid's ability to detect and localize attacks effectively.

Furthermore, the study revealed that current PMU placement strategies suggested in the literature may not necessarily offer the optimal configuration for attack detection and localization, even though they ensure the maximum possible network observability. This highlights the need for research to develop PMU placement strategies that prioritize both maximum observability and enhanced network resilience to attacks. Additionally, it was demonstrated that different configurations of unobservable buses can significantly impact attack detection capabilities.

Specifically, this work found that a clustered configuration for unobservable buses is more effective than a scattered configuration in terms of attack detection and localization capabilities.

The findings from the experiments could provide insights for future research directions, particularly in the development of dynamic and adaptive PMU placement strategies that can accommodate the evolving landscape of cyber-physical threats under conditions of unobservability to ensure not only complete network observability but also reliable attack detection and localization.

7.2 Future Work

The work explored in the thesis, which sheds light on the effects of bus unobservability on FDIA detection and localization can open several promising directions for future research that could significantly advance the field of smart grid cybersecurity.

Firstly, integrating spatial dynamics into the existing temporal models, particularly through the adoption of GNNs, presents a fertile ground for enhancement. GNNs, by their ability to capture spatial dependencies within graph-structured data, could offer a substantial improvement in modeling the complex interactions within power systems. This integration could lead to a more nuanced understanding of how attacks propagate through the network and how different nodes influence each other, thereby improving detection and localization accuracy under conditions of unobservability.

Secondly, in this work, for training the SE model, which primarily relies on machine learning techniques requiring target values, the approach must utilize previous temporal states of the unobservable buses so the training can be accomplished; therefore, assuming disconnections at a certain point in time or employing classical SE methods for data acquisition of the unobservable buses. Future enhancements could involve adopting models that do not depend on

the availability of previous states, such as those based on GNN or graph signal processing techniques. These advanced models are capable of estimating the states of unobservable nodes through the relationships among nodes, eliminating the need for historical training data.

Additionally, broadening the scope of research to encompass various cyber-physical events beyond FDIA could immensely benefit the resilience of power systems. While FDIA represents a critical threat to smart grids, other types of cyber-physical threats could also have profound impacts. By examining a wider array of cyber-physical events, researchers can gain comprehensive insights into the vulnerabilities of power systems and the effectiveness of different detection and localization strategies under unobservability conditions. This broader perspective could inform more holistic and robust PMU placement strategies, ensuring that the grid is not only resilient to FDIA but to a spectrum of potential threats.

References

[1] Hossain, E., Khan, I., Un-Noor, F., Sikander, S. S., & Mudasser, M. (2014). A review of smart technology: Smart Grid and its features. Proceedings of 2014 1st International Conference on Non-Conventional Energy (ICONCE 2014), Kalyani, WB, India. IEEE.

[2] Zhou, J., He, L., Li, C., Cao, Y., Liu, X., & Geng, Y. (2013). What's the difference between traditional power grid and smart grid? From dispatching perspective. Hunan University, Changsha, China.

[3] Brown, M. A., Zhou, S., & Ahmadi, M. (2018). Smart grid governance: An international review of evolving policy issues and innovations. WIREs Energy and Environment, e290.

[4] Kabalci, Y. (2016). A survey on smart metering and smart grid communication. Renewable and Sustainable Energy Reviews, 57, 302–318.

[5] Ahmed, M. M., Amjad, M., Qureshi, M. A., Imran, K., Haider, Z. M., & Khan, M. O. (2022). A Critical Review of State-of-the-Art Optimal PMU Placement Techniques. Energies, 15(6), 2125. https://doi.org/10.3390/en15062125.

[6] Yang, Z., Liu, H., Bi, T., Li, Z., & Yang, Q. (2020). An adaptive PMU missing data recovery method. International Journal of Electrical Power & Energy Systems, 116, 105577. https://doi.org/10.1016/j.ijepes.2019.105577.

[7] Hossain, M. J., & Rahnamay-Naeini, M. (2021). Data-driven, multi-region distributed state estimation for smart grids. In 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe) (pp. 1–6).

[8] Hyacinth, L. R., & Gomathi, V. (2021). Optimal PMU Placement Technique to Maximize Measurement Redundancy Based on Closed Neighbourhood Search. Energies, 14(16), 4782. https://doi.org/10.3390/en14164782.

[9] Yuill, W., Edwards, A., Chowdhury, S., & Chowdhury, S. P. (2011). Optimal PMU placement: A comprehensive literature review. In 2011 IEEE Power and Energy Society General Meeting. IEEE.

[10] Hossain, M. J. (2022). Data-Driven State Estimation for Improved Wide Area Situational Awareness in Smart Grids. USF Tampa Graduate Theses and Dissertations. Retrieved from https://digitalcommons.usf.edu/etd/9783.

[11] Dehghanpour, K., Wang, Z., Wang, J., Yuan, Y., & Bu, F. (2019). A Survey on State Estimation Techniques and Challenges in Smart Distribution Systems. IEEE Transactions on Smart Grid, 10(2), 2312.

[12] Primadianto, A., & Lu, C.-N. (2017). A Review on Distribution System State Estimation. IEEE Transactions on Power Systems, 32(5), 3875.

[13] Shivakumar, S. N. R., & Jain, A. (2008). A Review of Power System Dynamic State Estimation Techniques. ISBN 978-1-4244-1762-9. $25.00. ©2008 IEEE.

[14] Weng, Y., Negi, R., Faloutsos, C., & Ilic, M. D. (2017). Robust Data-Driven State Estimation for Smart Grid. IEEE Transactions on Smart Grid, 8(4), 1956. July 2017.

[15] Zhang, H., Liu, B., & Wu, H. (2016). Smart Grid Cyber-Physical Attack and Defense: A Review. IEEE Access. https://doi.org/10.1109/ACCESS.2017.DOI.

[16] Shehod, A. (2016). Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US (CISL# 2016-22). Sloan School of Management, Massachusetts Institute of Technology.

[17] Lee, R., Assante, M., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center & SANS Industrial Control Systems. Retrieved from http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[18] Yuan, Y., Li, Z., & Ren, K. (2011). Modeling load redistribution attacks in power systems. IEEE Transactions on Smart Grid, 2(2), 382-390.

[19] Kim, J., & Tong, L. (2013). On topology attack of a smart grid: Undetectable attacks and countermeasures. IEEE Journal on Selected Areas in Communications, 31(7), 1294-1305.

[20] Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao, "On Optimal PMU Placement-Based Defense Against Data Integrity Attacks in Smart Grid," IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1735, July 2017.

[21] Ding, W., Xu, M., Huang, Y., Zhao, P., & Song, F. (2021). Cyber attacks on PMU placement in a smart grid: Characterization and optimization. Reliability Engineering & System Safety, 212, 107586. https://www.elsevier.com/locate/ress.

[22] Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1985). Learning internal representations by error propagation. Tech. rep. ICS 8504. Institute for Cognitive Science, University of California, San Diego, CA.

[23] Jordan, M. I. (1986). Serial order: A parallel distributed processing approach. Tech. rep. ICS 8604. Institute for Cognitive Science, University of California, San Diego, CA

[24] Singh, A. (2017). Anomaly Detection for Temporal Data using Long Short-Term Memory (LSTM), School of Information and Communication Technology, KTH Royal Institute of Technology.

[25] Casolaro, A., Capone, V., Iannuzzo, G., & Camastra, F. (2023). Deep Learning for Time Series Forecasting: Advances and Open Problems. Information, 14(598). https://doi.org/10.3390/info14110598.

[26] Hochreiter, S., & Schmidhuber, J. (1997). Long Short-Term Memory. Neural Computation, 9(8), 1735–1780.

[27] Lindemann, B., Maschler, B., Sahlab, N., & Weyrich, M. (2021). A survey on anomaly detection for technical systems using LSTM networks. Computers in Industry, 131, 103498. https://www.elsevier.com/locate/compind.

[28] Musleh, A. S., Chen, G., Dong, Z. Y., Wang, C., & Chen, S. (2023). Spatio-temporal data-driven detection of false data injection attacks in power distribution systems. Electrical Power and Energy Systems, 145(108612). https://doi.org/10.1016/j.ijepes.2022.108612

[29] Althelaya, K. A., El-Alfy, E.-S. M., & Mohammed, S. (2018). Stock Market Forecast Using Multivariate Analysis with Bidirectional and Stacked (LSTM, GRU). Department of Information and Computer Science, College of Computer Sciences and Engineering, King Fahd University of Petroleum and Minerals, Dhahran 31261, Kingdom of Saudi Arabia.

[30] Liu, Y., Ning, P., & Reiter, M. K. (2009). False data injection attacks against state estimation in electric power grids. In Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS) (pp. 1–12).

[31] Singh, R., Pal, B. C., & Jabr, R. A. (2009). Choice of estimator for distribution system state estimation. IET Generation, Transmission & Distribution, 3, 666-678.

[32] Hassanzadeh, M., & Evrenosoglu, C. Y. (2012). Power system state forecasting using regression analysis. In Proc. IEEE/PES General Meeting (pp. 1–6). San Diego, CA, USA.

[33] Netto, M., & Mili, L. (2018). A robust data-driven Koopman Kalman filter for power systems dynamic state estimation. IEEE Transactions on Power Systems, 33(6), 7228-7237. https://doi.org/10.1109/TPWRS.2018.2846744.

[34] Abdel-Nasser, M., Mahmoud, K., & Kashef, H. (2018). A novel smart grid state estimation method based on neural networks. International Journal of Interactive Multimedia and Artificial Intelligence, 5(1).

[35] Zhang, L., Wang, G., & Giannakis, G. B. (2019). Real-time power system state estimation and forecasting via deep unrolled neural networks. IEEE Transactions on Signal Processing. Accepted June 28, 2019.

[36] Zhang, L., Wang, G., & Giannakis, G. B. (2019). Real-time power system state estimation and forecasting via deep unrolled neural networks. IEEE Transactions on Signal Processing. Accepted June 28, 2019.

[37] Cao, Z., Wang, Y., Chu, C.-C., & Gadh, R. (2020). Scalable distribution systems state estimation using long short-term memory networks as surrogates. IEEE Access, 8, https://doi.org/10.1109/ACCESS.2020.2967638.

[38] Bhusal, N., Shukla, R. M., Gautam, M., Benidris, M., & Sengupta, S. (2021). Deep ensemble learning-based approach to real-time power system state estimation. arXiv:2101.03457v1 [eess.SY].

[39] W. Liao, B. Bak-Jensen, J. R. Pillai, Y. Wang, and Y. Wang. A review of graph neural networks and their applications in power systems, 2021.

[40] Hossain, M. J., & Rahnamay-Naeini, M. (2021). State estimation in smart grids using temporal graph convolution networks. In 2021 North American Power Symposium (NAPS) (pp. 1-6). IEEE. https://doi.org/10.1109/NAPS52732.2021.9654642.

[41] Musleh, A. S., Chen, G., & Dong, Z. Y. (2020). A survey on the detection algorithms for false data injection attacks in smart grids. IEEE Transactions on Smart Grid, 11(3).

[42] Goldstein, M., & Uchida, S. (2016). A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. PLoS ONE, 11(4), Article e0152173. https://doi.org/10.1371/journal.pone.0152173.

[43] Foorthuis, R. (2021). On the nature and types of anomalies: a review of deviations in data. International Journal of Data Science and Analysis, 12(4), 297–331. https://doi.org/10.1007/s41060-021-00265-1.

[44] Lin, X., An, D., Cui, F., & Zhang, F. (2023). False data injection attack in smart grid: Attack model and reinforcement learning-based detection method. Frontiers in Energy Research. https://doi.org/10.3389/fenrg.2022.1104989.

[45] Lindemann, B., Maschler, B., Sahlab, N., & Weyrich, M. (2021). A survey on anomaly detection for technical systems using LSTM networks. Computers in Industry, 131, 103498. https://www.elsevier.com/locate/compind.

[46] Chen, Y., Xie, L., & Kumar, P. R. (2013). Dimensionality reduction and early event detection using online synchrophasor data. In Proceedings of the 2013 IEEE (pp. 1-6). IEEE.

[47] Basu, S., & Meckesheimer, M. (2006). Automatic outlier detection for time series: an application to sensor data. Knowledge and Information Systems, 11(3), 137–154. https://doi.org/10.1007/s10115-006-0029-5.

[48] Gupta, M., Gao, J., Aggarwal, C. C., & Han, J. (2014). Outlier detection for temporal data: A survey. IEEE Transactions on Knowledge and Data Engineering, 26(9), 2250-2267.

[49] Lee, M.-C., Lin, J.-C., & Gan, E.G. (2020). ReRe: A lightweight real-time ready-to-Go anomaly detection approach for time series. In 2020 IEEE 4th Annual Computers, Software and Applications Conference (COMPSAC) (pp. 322–327). https://doi.org/10.1109/COMPSAC48688.2020.0-226.

[50] Bontemps, L., Cao, V. L., McDermott, J., & Le-Khac, N.-A. (2016). Collective anomaly detection based on long short-term memory recurrent neural networks. In Springer International Publishing (pp. 141–152). https://doi.org/10.1007/978-3-319-48057-2_9.

[51] Malhotra, P., Vig, L., Shroff, G., & Agarwal, P. (2015). Long short term memory networks for anomaly detection in time series. In Proceedings of European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN) (pp. 89–94).

[52] Schmidhuber, J. (2015). Deep learning in neural networks: an overview. Neural Networks, 61, 85–117. https://doi.org/10.1016/j.neunet.2014.09.003.

[53] Naseer, S., et al. (2018). Enhanced network anomaly detection based on deep neural networks. IEEE Access, 6, 48231–48246. https://doi.org/10.1109/ACCESS.2018.2863036.

[54] Park, D., Hoshi, Y., & Kemp, C. (2018). A multimodal anomaly detector for robot-assisted feeding using an LSTM-based variational autoencoder. IEEE Robotics and Automation Letters, 3(3). https://doi.org/10.1109/LRA.2018.2801475.

[55] Kieu, T., Yang, B., Guo, C., & Jensen, C. S. (2019). Outlier detection for time series with recurrent autoencoder ensembles. Proceedings of the 28th International Joint Conference on Artificial Intelligence (IJCAI), 2725–2732. https://doi.org/10.24963/ijcai.2019/378.

[56] T. Ergen and S. S. Kozat, "Unsupervised Anomaly Detection With LSTM Neural Networks," in IEEE Transactions on Neural Networks and Learning Systems, vol. 31, no. 8, pp. 3127, August 2020.

[57] Elsayed, M. S., Le-Khac, N.-A., Dev, S., & Jurcut, A. D. (2020). Network Anomaly Detection Using LSTM Based Autoencoder. In Q2SWinet '20: Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks (pp. 223-226), Alicante, Spain. University College Dublin, Ireland.

[58] Kim, T.Y., & Cho, S.B. (2018). Web traffic anomaly detection using C-LSTM neural networks. Expert Systems With Applications, 106, 66–76. http://dx.doi.org/10.1016/j.eswa.2018.04.004.

[59] Ferragut, E. M., Laska, J., Olama, M. M., & Ozmen, O. (2017). Real-time cyber-physical false data attack detection in smart grids using neural networks. In Proceedings of the International Conference on Computer Science and Computational Intelligence (CSCI) (pp. 1-6).

[60] Radhoush, S., Vannoy, T., Whitaker, B. M., & Nehrir, H. (2022). Simultaneous state estimation and bad data detection on PMU measurements in active distribution power networks. In 2022 North American Power Symposium (NAPS). IEEE. https://doi.org/10.1109/NAPS56150.2022.10012150.

[61] Ayad, A., Farag, H. E. Z., Youssef, A., & El-Saadany, E. F. (2018). Detection of false data injection attacks in smart grids using recurrent neural networks. In Proceedings of the IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT) (pp. 1-5).

[62] Vimalkumar, K., & Radhika, N. (2017). A big data framework for intrusion detection in smart grids using Apache Spark. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 198-204).

[63] Mukherjee, D., Chakraborty, S., & Ghosh, S. (2021). Deep learning-based multilabel classification for locational detection of false data injection attack in smart grids. Electrical Engineering, 104(3), 259–282. https://doi.org/10.1007/s00202-021-01278-6.

[64] Ganjkhani, M., Fallah, S. N., Badakhshan, S., Shamshirband, S., & Chau, K.-w. (2019). A Novel Detection Algorithm to Identify False Data Injection Attacks on Power System State Estimation. Sensors, 19(11), 2554. https://doi.org/10.3390/s19112554.

[65] Haghshenas, S. H., Hasnat, M. A., & Naeini, M. (2022). A Temporal Graph Neural Network for Cyber Attack Detection and Localization in Smart Grids. arXiv:2212.03390v1 [cs.LG]. Retrieved from https://arxiv.org/abs/2212.03390.

[66] Babu, R., & Bhattacharyya, B. (2020). Optimal placement of PMU for complete observability of the interconnected power network considering zero-injection bus: A numerical approach. International Journal of Applied Power Engineering (IJAPE), 9(2), 135-146. http://doi.org/10.11591/ijape.v9.i2.pp135-146.

[67] Milosevic, B., & Begovic, M. (2003). Nondominated sorting genetic algorithm for optimal phasor measurement placement. IEEE Transactions on Power Systems, 18(1), 69-75.

[68] Peppanen, J., Alquthami, T., Molina, D., & Harley, R. (2012). Optimal PMU placement with binary PSO. In Proceedings of the 2012 IEEE Energy Conversion Congress and Exposition (ECCE) (pp. 1475-1482.

[69] Sefid, M., & Rihan, M. (2019). Optimal PMU placement in a smart grid: An updated review. International Journal of Smart Grid and Clean Energy, 8(1).

[70] Illinois Center for a Smarter Electric Grid (ICSEG). (n.d.). IEEE 118-Bus System. Retrieved July 15, 2022, from https://icseg.iti.illinois.edu/ieee-118-bus-system/.

[71] New York Independent System Operator. (n.d.). Load Data. Retrieved October 8, 2023, from https://www.nyiso.com/load-data.

[72] Zimmerman, R. D., Murillo-Sánchez, C. E., & Thomas, R. J. (2011). MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education. IEEE Transactions on Power Systems, 26(1), 12-19.

[73] Seaborn. (n.d.). seaborn.heatmap. Retrieved February 2nd, 2024, from https://seaborn.pydata.org/generated/seaborn.heatmap.html.

[74] Hasnat, M. A., & Rahnamay-Naeini, M. (2022). A Graph Signal Processing Framework for Detecting and Locating Cyber and Physical Stresses in Smart Grids. IEEE Transactions on Smart Grid. Advance online publication. https://doi.org/10.1109/TSG.2022.3177154.

[75] Sajan, K. S., Bariya, M., Basak, S., Srivastava, A., Dubey, A., von Meier, A., & Biswas, G. (2020). Realistic Synchrophasor Data Generation for Anomaly Detection and Event Classification. 2020 IEEE. https://doi.org/978-1-7281-8721-1/20/$31.00.

[76] Bhanja, S. (2020). Deep Neural Network for Multivariate Time-Series Forecasting. In Advances in Intelligent Systems and Computing (Vol. 981, Issue 15-7834-2_25). https://doi.org/10.1007/978-981-15-7834-2_25.

[77] Abdel-Nasser, M., Mahmoud, K., & Kashef, H. (2018). A Novel Smart Grid State Estimation Method Based on Neural Networks. International Journal of Interactive Multimedia and Artificial Intelligence, 5(1).

[78] Chicco, D., Warrens, M. J., & Jurman, G. (2021). The coefficient of determination R-squared is more informative than SMAPE, MAE, MAPE, MSE, and RMSE in regression analysis evaluation. PeerJ Computer Science, 623. https://doi.org/10.7717/peerj-cs.623.

[79] Theile, P., Towle, A. L., Karnataki, K., Crosara, A., Paridari, K., Turk, G., & Nordström, L. (2018). Day-ahead electricity consumption prediction of a population of households: analyzing different machine learning techniques based on real data from RTE in France. 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). doi: 10.1109/SmartGridComm.2018.8587496.

[80] Elmrabit, N., Zhou, F., Li, F., & Zhou, H. (2020). Evaluation of Machine Learning Algorithms for Anomaly Detection. In Proceedings of the International Conference on Cyber Security and Protection of Digital Services (Cyber Security).

[81] Ioffe, S., & Szegedy, C. (2015). Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift.

[82] Chen, S., Li, M., & Zhang, Y. (2020). Sampling and recovery of graph signals based on graph neural networks. arXiv preprint arXiv:2011.01412.

[83] Hasnat, M. A., & Rahnamay-Naeini, M. (2022). Power system state recovery using local and global smoothness of its graph signals. In 2022 IEEE Power & Energy Society General Meeting (PESGM) (pp. 01-05). Denver, CO, USA: IEEE. https://doi.org/10.1109/PESGM48719.2022.9917018.

[84] Manousakis, N. M., & Korres, G. N. (2020). Optimal allocation of phasor measurement units considering various contingencies and measurement redundancy. IEEE Transactions on Instrumentation and Measurement, 69(6), 3403–3411.

[85] Yang, J., Pei, L., Kuang, C., Li, Y., & Liu, Y. (2023). Dynamic evaluation method for time-variant reliability of structural safety of concrete-faced rockfill dam. Structures, 57, 105095.

[86] Jamei, M., Ramakrishna, R., Tesfay, T., Gentz, R., Roberts, C., Scaglione, A., & Peisert, S. (2020). Phasor measurement units optimal placement and performance limits for fault localization. IEEE Journal on Selected Areas in Communications, 38(1)

Appendix A: Copyright Permissions

The Permission below is for Figure 1.1

JOHN WILEY AND SONS LICENSE TERMS AND CONDITIONS

Feb 19, 2024

This Agreement between University of South Florida -- Moheb Abdelmalak ("You") and John Wiley and Sons ("John Wiley and Sons") consists of your license details and the terms and conditions provided by John Wiley and Sons and Copyright Clearance Center.

License Number	5724660873071
License date	Feb 09, 2024
Licensed Content Publisher	John Wiley and Sons
Licensed Content Publication	WILEY INTERDISCIPLINARY REVIEWS: ENERGY AND ENVIRONMENT
Licensed Content Title	Smart grid governance: An international review of evolving policy issues and innovations
Licensed Content Author	Majid Ahmadi, Shan Zhou, Marilyn A. Brown
Licensed Content Date	May 19, 2018
Licensed Content Volume	7
Licensed Content Issue	5
Licensed Content Pages	26
Type of Use	Dissertation/Thesis
Requestor type	University/Academic
Format	Electronic
Portion	Figure/table
Number of figures/tables	1
Will you be translating?	No
Title of new work	The effect of Bus observability on detection and localization of FDIA attacks in Smart grids
Institution name	University of south flroida
Expected presentation date	Feb 2024
Portions	Figure 1
Requestor Location	University of South Florida
Publisher Tax ID	EU826007151
Total	**0.00 USD**
Terms and Conditions	

TERMS AND CONDITIONS

This copyrighted material is owned by or exclusively licensed to John Wiley & Sons, Inc. or one of its group companies (each a"Wiley Company") or handled on behalf of a society with which a Wiley Company has exclusive publishing rights in relation to a particular work (collectively "WILEY"). By clicking "accept" in connection with completing this licensing transaction, you agree that the following terms and conditions apply to this transaction (along with the billing and payment terms and conditions established by the Copyright Clearance Center Inc., ("CCC's Billing and Payment terms and conditions"), at the time that you opened your RightsLink account (these are available at any time at http://myaccount.copyright.com).

Terms and Conditions

- The materials you have requested permission to reproduce or reuse (the "Wiley Materials") are protected by copyright.

- You are hereby granted a personal, non-exclusive, non-sub licensable (on a stand-alone basis), non-transferable, worldwide, limited license to reproduce the Wiley Materials for the purpose specified in the licensing process. This license, **and any CONTENT (PDF or image file) purchased as part of your order,** is for a one-time use only and limited to any maximum distribution number specified in the license. The first instance of republication or reuse granted by this license must be completed within two years of the date of the grant of this license (although copies prepared before the end date may be distributed thereafter). The Wiley Materials shall not be used in any other manner or for any other purpose, beyond what is granted in the license. Permission is granted subject to an appropriate acknowledgement given to the author, title of the material/book/journal and the publisher. You shall also duplicate the copyright notice that appears in the Wiley publication in your use of the Wiley Material. Permission is also granted on the understanding that nowhere in the text is a previously published source acknowledged for all or part of this Wiley Material. Any third party content is expressly excluded from this permission.

- With respect to the Wiley Materials, all rights are reserved. Except as expressly granted by the terms of the license, no part of the Wiley Materials may be copied, modified, adapted (except for minor reformatting required by the new Publication), translated, reproduced, transferred or distributed, in any form or by any means, and no derivative works may be made based on the Wiley Materials without the prior permission of the respective copyright owner.**For STM Signatory Publishers clearing permission under the terms of the STM Permissions Guidelines only, the terms of the license are extended to include subsequent editions and for editions in other languages, provided such editions are for the work as a whole in situ and does not involve the separate exploitation of the permitted figures or extracts,** You may not alter, remove or suppress in any manner any copyright, trademark or other notices displayed by the Wiley Materials. You may not license, rent, sell, loan, lease, pledge, offer as security, transfer or assign the Wiley Materials on a stand-alone basis, or any of the rights granted to you hereunder to any other person.

- The Wiley Materials and all of the intellectual property rights therein shall at all times remain the exclusive property of John Wiley & Sons Inc, the Wiley Companies, or their respective licensors, and your interest therein is only that of having possession of and the right to reproduce the Wiley Materials pursuant to Section 2 herein during the continuance of this Agreement. You agree that you own no right, title or interest in or to the Wiley Materials or any of the intellectual property rights therein. You shall have no rights hereunder other than the license as provided for above in Section 2. No right, license or interest to any trademark, trade name, service mark or other branding ("Marks") of WILEY or its licensors is granted hereunder, and you agree that you shall not assert any such right, license or interest with respect thereto

- NEITHER WILEY NOR ITS LICENSORS MAKES ANY WARRANTY OR REPRESENTATION OF ANY KIND TO YOU OR ANY THIRD PARTY, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO THE MATERIALS OR THE ACCURACY OF ANY INFORMATION CONTAINED IN THE MATERIALS, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, ACCURACY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, USABILITY, INTEGRATION OR NON-INFRINGEMENT AND ALL SUCH WARRANTIES ARE HEREBY EXCLUDED BY WILEY AND ITS LICENSORS AND WAIVED BY YOU.

- WILEY shall have the right to terminate this Agreement immediately upon breach of this Agreement by you.

- You shall indemnify, defend and hold harmless WILEY, its Licensors and their respective directors, officers, agents and employees, from and against any actual or threatened claims, demands, causes of action or proceedings arising from any breach of this Agreement by you.

- IN NO EVENT SHALL WILEY OR ITS LICENSORS BE LIABLE TO YOU OR ANY OTHER PARTY OR ANY OTHER PERSON OR ENTITY FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY OR PUNITIVE DAMAGES, HOWEVER CAUSED, ARISING OUT OF OR IN CONNECTION WITH THE DOWNLOADING, PROVISIONING, VIEWING OR USE OF THE MATERIALS REGARDLESS OF THE FORM OF ACTION, WHETHER FOR BREACH OF CONTRACT, BREACH OF WARRANTY, TORT, NEGLIGENCE, INFRINGEMENT OR OTHERWISE (INCLUDING, WITHOUT LIMITATION, DAMAGES BASED ON LOSS OF PROFITS, DATA, FILES, USE, BUSINESS OPPORTUNITY OR CLAIMS OF THIRD PARTIES), AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY PROVIDED HEREIN.

- Should any provision of this Agreement be held by a court of competent jurisdiction to be illegal, invalid, or unenforceable, that provision shall be deemed amended to achieve as nearly as possible the same economic effect as the original provision, and the legality, validity and enforceability of the remaining provisions of this Agreement shall not be affected or impaired thereby.

- The failure of either party to enforce any term or condition of this Agreement shall not constitute a waiver of either party's right to enforce each and every term and condition of this Agreement. No breach under this agreement shall be deemed waived or excused by either party unless such waiver or consent is in writing signed by the party granting such waiver or consent. The waiver by or consent of a party to a breach of any provision of this Agreement shall not operate or be construed as a waiver of or consent to any other or subsequent breach by such other party.

- This Agreement may not be assigned (including by operation of law or otherwise) by you without WILEY's prior written consent.

- Any fee required for this permission shall be non-refundable after thirty (30) days from receipt by the CCC.

- These terms and conditions together with CCC's Billing and Payment terms and conditions (which are incorporated herein) form the entire agreement between you and WILEY concerning this licensing transaction and (in the absence of fraud) supersedes all prior agreements and representations of the parties, oral or written. This Agreement may not be amended except in writing signed by both parties. This Agreement shall be binding upon and inure to the benefit of the parties' successors, legal representatives, and authorized assigns.

- In the event of any conflict between your obligations established by these terms and conditions and those established by CCC's Billing and Payment terms and conditions, these terms and conditions shall prevail.

- WILEY expressly reserves all rights not specifically granted in the combination of (i) the license details provided by you and accepted in the course of this licensing transaction, (ii) these terms and conditions and (iii) CCC's Billing and Payment terms and conditions.

- This Agreement will be void if the Type of Use, Format, Circulation, or Requestor Type was misrepresented during the licensing process.

- This Agreement shall be governed by and construed in accordance with the laws of the State of New York, USA, without regards to such state's conflict of law rules. Any legal action, suit or proceeding arising out of or relating to these Terms and Conditions or the breach thereof shall be instituted in a court of competent jurisdiction in New York County in the State of New York in the United States of America and each party hereby consents and submits to the personal jurisdiction of such court, waives any objection to venue in such court and consents to service of process by registered or certified mail, return receipt requested, at the last known address of such party.

WILEY OPEN ACCESS TERMS AND CONDITIONS

Wiley Publishes Open Access Articles in fully Open Access Journals and in Subscription journals offering Online Open. Although most of the fully Open Access journals publish open access articles under the terms of the Creative Commons Attribution (CC BY) License only, the subscription journals and a few of the Open Access Journals offer a choice of Creative Commons Licenses. The license type is clearly identified on the article.

The Creative Commons Attribution License

The Creative Commons Attribution License (CC-BY) allows users to copy, distribute and transmit an article, adapt the article and make commercial use of the article. The CC-BY license permits commercial and non-

Creative Commons Attribution Non-Commercial License

The Creative Commons Attribution Non-Commercial (CC-BY-NC)License permits use, distribution and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.(see below)

Creative Commons Attribution-Non-Commercial-NoDerivs License

The Creative Commons Attribution Non-Commercial-NoDerivs License (CC-BY-NC-ND) permits use, distribution and reproduction in any medium, provided the original work is properly cited, is not used for commercial purposes and no modifications or adaptations are made. (see below)

Use by commercial "for-profit" organizations

Use of Wiley Open Access articles for commercial, promotional, or marketing purposes requires further explicit permission from Wiley and will be subject to a fee.

Further details can be found on Wiley Online Library http://olabout.wiley.com/WileyCDA/Section/id-410895.html

Other Terms and Conditions:

The Permission below is for Figure 1.2

ELSEVIER LICENSE TERMS AND CONDITIONS

Feb 13, 2024

This Agreement between University of South Florida -- Moheb Abdelmalak ("You") and Elsevier ("Elsevier") consists of your license details and the terms and conditions provided by Elsevier and Copyright Clearance Center.

License Number	5725131440937
License date	Feb 09, 2024
Licensed Content Publisher	Elsevier
Licensed Content Publication	Renewable and Sustainable Energy Reviews
Licensed Content Title	A survey on smart metering and smart grid communication
Licensed Content Author	Yasin Kabalci
Licensed Content Date	May 1, 2016
Licensed Content Volume	57
Licensed Content Issue	n/a
Licensed Content Pages	17
Start Page	302
End Page	318
Type of Use	reuse in a thesis/dissertation
Portion	figures/tables/illustrations
Number of figures/tables/illustrations	2
Format	electronic
Are you the author of this Elsevier article?	No
Will you be translating?	No
Title of new work	The effect of Bus observability on detection and localization of FDIA attacks in Smart grids
Institution name	University of south flroida
Expected presentation date	Feb 2024
Portions	Figure 2
Requestor Location	University of South Florida
	Attn: University of South Florida
Publisher Tax ID	98-0397604
Total	**0.00 USD**
Terms and Conditions	

INTRODUCTION

1. The publisher for this copyrighted material is Elsevier. By clicking "accept" in connection with completing this licensing transaction, you agree that the following terms and conditions apply to this transaction (along with the Billing and Payment terms and conditions established by Copyright Clearance Center, Inc. ("CCC"), at the time that you opened your RightsLink account and that are available at any time at https://myaccount.copyright.com).

GENERAL TERMS

2. Elsevier hereby grants you permission to reproduce the aforementioned material subject to the terms and conditions indicated.

3. Acknowledgement: If any part of the material to be used (for example, figures) has appeared in our publication with credit or acknowledgement to another source, permission must also be sought from that source. If such permission is not obtained then that material may not be included in your publication/copies. Suitable acknowledgement to the source must be made, either as a footnote or in a reference list at the end of your publication, as follows:
"Reprinted from Publication title, Vol /edition number, Author(s), Title of article / title of chapter, Pages No., Copyright (Year), with permission from Elsevier [OR APPLICABLE SOCIETY COPYRIGHT OWNER]." Also Lancet special credit - "Reprinted from The Lancet, Vol. number, Author(s), Title of article, Pages No., Copyright (Year), with permission from Elsevier."
4. Reproduction of this material is confined to the purpose and/or media for which permission is hereby given. The material may not be reproduced or used in any other way, including use in combination with an artificial intelligence tool (including to train an algorithm, test, process, analyse, generate output and/or develop any form of artificial intelligence tool), or to create any derivative work and/or service (including resulting from the use of artificial intelligence tools).
5. Altering/Modifying Material: Not Permitted. However figures and illustrations may be altered/adapted minimally to serve your work. Any other abbreviations, additions, deletions and/or any other alterations shall be made only with prior written authorization of Elsevier Ltd. (Please contact Elsevier's permissions helpdesk here). No modifications can be made to any Lancet figures/tables and they must be reproduced in full.
6. If the permission fee for the requested use of our material is waived in this instance, please be advised that your future requests for Elsevier materials may attract a fee.
7. Reservation of Rights: Publisher reserves all rights not specifically granted in the combination of (i) the license details provided by you and accepted in the course of this licensing transaction, (ii) these terms and conditions and (iii) CCC's Billing and Payment terms and conditions.
8. License Contingent Upon Payment: While you may exercise the rights licensed immediately upon issuance of the license at the end of the licensing process for the transaction, provided that you have disclosed complete and accurate details of your proposed use, no license is finally effective unless and until full payment is received from you (either by publisher or by CCC) as provided in CCC's Billing and Payment terms and conditions. If full payment is not received on a timely basis, then any license preliminarily granted shall be deemed automatically revoked and shall be void as if never granted. Further, in the event that you breach any of these terms and conditions or any of CCC's Billing and Payment terms and conditions, the license is automatically revoked and shall be void as if never granted. Use of materials as described in a revoked license, as well as any use of the materials beyond the scope of an unrevoked license, may constitute copyright infringement and publisher reserves the right to take any and all action to protect its copyright in the materials.
9. Warranties: Publisher makes no representations or warranties with respect to the licensed material.
10. Indemnity: You hereby indemnify and agree to hold harmless publisher and CCC, and their respective officers, directors, employees and agents, from and against any and all claims arising out of your use of the licensed material other than as specifically authorized pursuant to this license.
11. No Transfer of License: This license is personal to you and may not be sublicensed, assigned, or transferred by you to any other person without publisher's written permission.
12. No Amendment Except in Writing: This license may not be amended except in a writing signed by both parties (or, in the case of publisher, by CCC on publisher's behalf).
13. Objection to Contrary Terms: Publisher hereby objects to any terms contained in any purchase order, acknowledgment, check endorsement or other writing prepared by you, which terms are inconsistent with these terms and conditions or CCC's Billing and Payment terms and conditions. These terms and conditions, together with CCC's Billing and Payment terms and conditions (which are incorporated herein), comprise the entire agreement between you and publisher (and CCC) concerning this licensing transaction. In the event of any conflict between your obligations established by these terms and conditions and those established by CCC's Billing and Payment terms and conditions, these terms and conditions shall control.
14. Revocation: Elsevier or Copyright Clearance Center may deny the permissions described in this License at their sole discretion, for any reason or no reason, with a full refund payable to you. Notice of such denial will be made using the contact information provided by you. Failure to receive such notice will not alter or invalidate the denial. In no event will Elsevier or Copyright Clearance Center be responsible or liable for any costs, expenses or damage incurred by you as a result of a denial of your permission request, other than a refund of the amount(s) paid by you to Elsevier and/or Copyright Clearance Center for denied permissions.

LIMITED LICENSE

The following terms and conditions apply only to specific license types:
15. **Translation**: This permission is granted for non-exclusive world **English** rights only unless your license was granted for translation rights. If you licensed translation rights you may only translate this content into the languages you requested. A professional translator must perform all translations and reproduce the content word for word preserving the integrity of the article.
16. **Posting licensed content on any Website**: The following terms and conditions apply as follows: Licensing material from an Elsevier journal: All content posted to the web site must maintain the copyright information line on the bottom of each image; A hyper-text must be included to the Homepage of the journal from which you are licensing at http://www.sciencedirect.com/science/journal/xxxxx or the Elsevier homepage for books at http://www.elsevier.com; Central Storage: This license does not include permission for a scanned version of the material to be stored in a central repository such as that provided by Heron/XanEdu.

Licensing material from an Elsevier book: A hyper-text link must be included to the Elsevier homepage at http://www.elsevier.com . All content posted to the web site must maintain the copyright information line on the bottom of each image.

Posting licensed content on Electronic reserve: In addition to the above the following clauses are applicable: The web site must be password-protected and made available only to bona fide students registered on a relevant course. This permission is granted for 1 year only. You may obtain a new license for future website posting.

17. **For journal authors:** the following clauses are applicable in addition to the above:

Preprints:

A preprint is an author's own write-up of research results and analysis, it has not been peer-reviewed, nor has it had any other value added to it by a publisher (such as formatting, copyright, technical enhancement etc.).

Authors can share their preprints anywhere at any time. Preprints should not be added to or enhanced in any way in order to appear more like, or to substitute for, the final versions of articles however authors can update their preprints on arXiv or RePEc with their Accepted Author Manuscript (see below).

If accepted for publication, we encourage authors to link from the preprint to their formal publication via its DOI. Millions of researchers have access to the formal publications on ScienceDirect, and so links will help users to find, access, cite and use the best available version. Please note that Cell Press, The Lancet and some society-owned have different preprint policies. Information on these policies is available on the journal homepage.

Accepted Author Manuscripts: An accepted author manuscript is the manuscript of an article that has been accepted for publication and which typically includes author-incorporated changes suggested during submission, peer review and editor-author communications.

Authors can share their accepted author manuscript:

- immediately
  - via their non-commercial person homepage or blog
  - by updating a preprint in arXiv or RePEc with the accepted manuscript
  - via their research institute or institutional repository for internal institutional uses or as part of an invitation-only research collaboration work-group
  - directly by providing copies to their students or to research collaborators for their personal use
  - for private scholarly sharing as part of an invitation-only work group on commercial sites with which Elsevier has an agreement
- After the embargo period
  - via non-commercial hosting platforms such as their institutional repository
  - via commercial sites with which Elsevier has an agreement

In all cases accepted manuscripts should:

- link to the formal publication via its DOI
- bear a CC-BY-NC-ND license - this is easy to do
- if aggregated with other manuscripts, for example in a repository or other site, be shared in alignment with our hosting policy not be added to or enhanced in any way to appear more like, or to substitute for, the published journal article.

Published journal article (JPA): A published journal article (PJA) is the definitive final record of published research that appears or will appear in the journal and embodies all value-adding publishing activities including peer review co-ordination, copy-editing, formatting, (if relevant) pagination and online enrichment.

Policies for sharing publishing journal articles differ for subscription and gold open access articles:

Subscription Articles: If you are an author, please share a link to your article rather than the full-text. Millions of researchers have access to the formal publications on ScienceDirect, and so links will help your users to find, access, cite, and use the best available version.

Theses and dissertations which contain embedded PJAs as part of the formal submission can be posted publicly by the awarding institution with DOI links back to the formal publications on ScienceDirect.

If you are affiliated with a library that subscribes to ScienceDirect you have additional private sharing rights for others' research accessed under that agreement. This includes use for classroom teaching and internal training at the institution (including use in course packs and courseware programs), and inclusion of the article for grant funding purposes.

Gold Open Access Articles: May be shared according to the author-selected end-user license and should contain a CrossMark logo, the end user license, and a DOI link to the formal publication on ScienceDirect.

Please refer to Elsevier's posting policy for further information.

18. **For book authors** the following clauses are applicable in addition to the above: Authors are permitted to place a brief summary of their work online only. You are not allowed to download and post the published electronic version of your chapter, nor may you scan the printed edition to create an electronic version. **Posting to a repository:** Authors are permitted to post a summary of their chapter only in their institution's repository.

19. **Thesis/Dissertation**: If your license is for use in a thesis/dissertation your thesis may be submitted to your institution in either print or electronic form. Should your thesis be published commercially, please reapply for permission. These requirements include

permission for the Library and Archives of Canada to supply single copies, on demand, of the complete thesis and include permission for Proquest/UMI to supply single copies, on demand, of the complete thesis. Should your thesis be published commercially, please reapply for permission. Theses and dissertations which contain embedded PJAs as part of the formal submission can be posted publicly by the awarding institution with DOI links back to the formal publications on ScienceDirect.

Elsevier Open Access Terms and Conditions

You can publish open access with Elsevier in hundreds of open access journals or in nearly 2000 established subscription journals that support open access publishing. Permitted third party re-use of these open access articles is defined by the author's choice of Creative Commons user license. See our open access license policy for more information.

Terms & Conditions applicable to all Open Access articles published with Elsevier:

Any reuse of the article must not represent the author as endorsing the adaptation of the article nor should the article be modified in such a way as to damage the author's honour or reputation. If any changes have been made, such changes must be clearly indicated.

The author(s) must be appropriately credited and we ask that you include the end user license and a DOI link to the formal publication on ScienceDirect.

If any part of the material to be used (for example, figures) has appeared in our publication with credit or acknowledgement to another source it is the responsibility of the user to ensure their reuse complies with the terms and conditions determined by the rights holder.

Additional Terms & Conditions applicable to each Creative Commons user license:

CC BY: The CC-BY license allows users to copy, to create extracts, abstracts and new works from the Article, to alter and revise the Article and to make commercial use of the Article (including reuse and/or resale of the Article by commercial entities), provided the user gives appropriate credit (with a link to the formal publication through the relevant DOI), provides a link to the license, indicates if changes were made and the licensor is not represented as endorsing the use made of the work. The full details of the license are available at http://creativecommons.org/licenses/by/4.0.

CC BY NC SA: The CC BY-NC-SA license allows users to copy, to create extracts, abstracts and new works from the Article, to alter and revise the Article, provided this is not done for commercial purposes, and that the user gives appropriate credit (with a link to the formal publication through the relevant DOI), provides a link to the license, indicates if changes were made and the licensor is not represented as endorsing the use made of the work. Further, any new works must be made available on the same conditions. The full details of the license are available at http://creativecommons.org/licenses/by-nc-sa/4.0.

CC BY NC ND: The CC BY-NC-ND license allows users to copy and distribute the Article, provided this is not done for commercial purposes and further does not permit distribution of the Article if it is changed or edited in any way, and provided the user gives appropriate credit (with a link to the formal publication through the relevant DOI), provides a link to the license, and that the licensor is not represented as endorsing the use made of the work. The full details of the license are available at http://creativecommons.org/licenses/by-nc-nd/4.0. Any commercial reuse of Open Access articles published with a CC BY NC SA or CC BY NC ND license requires permission from Elsevier and will be subject to a fee.

Commercial reuse includes:

- Associating advertising with the full text of the Article
- Charging fees for document delivery or access
- Article aggregation
- Systematic distribution via e-mail lists or share buttons

Posting or linking by commercial companies for use by customers of those companies.

20. **Other Conditions**:

v1.10

Questions? E-mail us at customercare@copyright.com.

The Permission below is for Figure 2.1.

ELSEVIER LICENSE TERMS AND CONDITIONS

Feb 19, 2024

This Agreement between University of South Florida -- Moheb Abdelmalak ("You") and Elsevier ("Elsevier") consists of your license details and the terms and conditions provided by Elsevier and Copyright Clearance Center.

License Number	5724661185131
License date	Feb 09, 2024
Licensed Content Publisher	Elsevier
Licensed Content Publication	International Journal of Electrical Power & Energy Systems
Licensed Content Title	Spatio-temporal data-driven detection of false data injection attacks in power distribution systems
Licensed Content Author	Ahmed S. Musleh,Guo Chen,Zhao Yang Dong,Chen Wang,Shiping Chen
Licensed Content Date	Feb 1, 2023
Licensed Content Volume	145
Licensed Content Issue	n/a
Licensed Content Pages	1
Start Page	108612
End Page	0
Type of Use	reuse in a thesis/dissertation
Portion	figures/tables/illustrations
Number of figures/tables/illustrations	3
Format	electronic
Are you the author of this Elsevier article?	No
Will you be translating?	No
Title of new work	The effect of Bus observability on detection and localization of FDIA attacks in Smart grids
Institution name	University of south flroida
Expected presentation date	Feb 2024
Portions	Figures 1,2,3
Requestor Location	University of South Florida
	Attn: University of South Florida
Publisher Tax ID	98-0397604
Total	**0.00 USD**
Terms and Conditions	

INTRODUCTION

1. The publisher for this copyrighted material is Elsevier. By clicking "accept" in connection with completing this licensing transaction, you agree that the following terms and conditions apply to this transaction (along with the Billing and Payment terms and conditions established by Copyright Clearance Center, Inc. ("CCC"), at the time that you opened your RightsLink account and that are available at any time at https://myaccount.copyright.com).

GENERAL TERMS

2. Elsevier hereby grants you permission to reproduce the aforementioned material subject to the terms and conditions indicated.

3. Acknowledgement: If any part of the material to be used (for example, figures) has appeared in our publication with credit or acknowledgement to another source, permission must also be sought from that source. If such permission is not obtained then that material may not be included in your publication/copies. Suitable acknowledgement to the source must be made, either as a footnote or in a reference list at the end of your publication, as follows:

"Reprinted from Publication title, Vol /edition number, Author(s), Title of article / title of chapter, Pages No., Copyright (Year), with permission from Elsevier [OR APPLICABLE SOCIETY COPYRIGHT OWNER]." Also Lancet special credit - "Reprinted from The Lancet, Vol. number, Author(s), Title of article, Pages No., Copyright (Year), with permission from Elsevier."

4. Reproduction of this material is confined to the purpose and/or media for which permission is hereby given. The material may not be reproduced or used in any other way, including use in combination with an artificial intelligence tool (including to train an algorithm, test, process, analyse, generate output and/or develop any form of artificial intelligence tool), or to create any derivative work and/or service (including resulting from the use of artificial intelligence tools).

5. Altering/Modifying Material: Not Permitted. However figures and illustrations may be altered/adapted minimally to serve your work. Any other abbreviations, additions, deletions and/or any other alterations shall be made only with prior written authorization of Elsevier Ltd. (Please contact Elsevier's permissions helpdesk here). No modifications can be made to any Lancet figures/tables and they must be reproduced in full.

6. If the permission fee for the requested use of our material is waived in this instance, please be advised that your future requests for Elsevier materials may attract a fee.

7. Reservation of Rights: Publisher reserves all rights not specifically granted in the combination of (i) the license details provided by you and accepted in the course of this licensing transaction, (ii) these terms and conditions and (iii) CCC's Billing and Payment terms and conditions.

8. License Contingent Upon Payment: While you may exercise the rights licensed immediately upon issuance of the license at the end of the licensing process for the transaction, provided that you have disclosed complete and accurate details of your proposed use, no license is finally effective unless and until full payment is received from you (either by publisher or by CCC) as provided in CCC's Billing and Payment terms and conditions. If full payment is not received on a timely basis, then any license preliminarily granted shall be deemed automatically revoked and shall be void as if never granted. Further, in the event that you breach any of these terms and conditions or any of CCC's Billing and Payment terms and conditions, the license is automatically revoked and shall be void as if never granted. Use of materials as described in a revoked license, as well as any use of the materials beyond the scope of an unrevoked license, may constitute copyright infringement and publisher reserves the right to take any and all action to protect its copyright in the materials.

9. Warranties: Publisher makes no representations or warranties with respect to the licensed material.

10. Indemnity: You hereby indemnify and agree to hold harmless publisher and CCC, and their respective officers, directors, employees and agents, from and against any and all claims arising out of your use of the licensed material other than as specifically authorized pursuant to this license.

11. No Transfer of License: This license is personal to you and may not be sublicensed, assigned, or transferred by you to any other person without publisher's written permission.

12. No Amendment Except in Writing: This license may not be amended except in a writing signed by both parties (or, in the case of publisher, by CCC on publisher's behalf).

13. Objection to Contrary Terms: Publisher hereby objects to any terms contained in any purchase order, acknowledgment, check endorsement or other writing prepared by you, which terms are inconsistent with these terms and conditions or CCC's Billing and Payment terms and conditions. These terms and conditions, together with CCC's Billing and Payment terms and conditions (which are incorporated herein), comprise the entire agreement between you and publisher (and CCC) concerning this licensing transaction. In the event of any conflict between your obligations established by these terms and conditions and those established by CCC's Billing and Payment terms and conditions, these terms and conditions shall control.

14. Revocation: Elsevier or Copyright Clearance Center may deny the permissions described in this License at their sole discretion, for any reason or no reason, with a full refund payable to you. Notice of such denial will be made using the contact information provided by you. Failure to receive such notice will not alter or invalidate the denial. In no event will Elsevier or Copyright Clearance Center be responsible or liable for any costs, expenses or damage incurred by you as a result of a denial of your permission request, other than a refund of the amount(s) paid by you to Elsevier and/or Copyright Clearance Center for denied permissions.

LIMITED LICENSE

The following terms and conditions apply only to specific license types:

15. **Translation**: This permission is granted for non-exclusive world **English** rights only unless your license was granted for translation rights. If you licensed translation rights you may only translate this content into the languages you requested. A professional translator must perform all translations and reproduce the content word for word preserving the integrity of the article.

16. **Posting licensed content on any Website**: The following terms and conditions apply as follows: Licensing material from an Elsevier journal: All content posted to the web site must maintain the copyright information line on the bottom of each image; A hyper-text must be included to the Homepage of the journal from which you are licensing at http://www.sciencedirect.com/science/journal/xxxxx or the Elsevier homepage for books at http://www.elsevier.com; Central Storage: This license does not include permission for a scanned version of the material to be stored in a central repository such as that provided by Heron/XanEdu.

Licensing material from an Elsevier book: A hyper-text link must be included to the Elsevier homepage at http://www.elsevier.com . All content posted to the web site must maintain the copyright information line on the bottom of each image.

Posting licensed content on Electronic reserve: In addition to the above the following clauses are applicable: The web site must be password-protected and made available only to bona fide students registered on a relevant course. This permission is granted for 1 year only. You may obtain a new license for future website posting.

17. **For journal authors:** the following clauses are applicable in addition to the above:

Preprints:

A preprint is an author's own write-up of research results and analysis, it has not been peer-reviewed, nor has it had any other value added to it by a publisher (such as formatting, copyright, technical enhancement etc.).

Authors can share their preprints anywhere at any time. Preprints should not be added to or enhanced in any way in order to appear more like, or to substitute for, the final versions of articles however authors can update their preprints on arXiv or RePEc with their Accepted Author Manuscript (see below).

If accepted for publication, we encourage authors to link from the preprint to their formal publication via its DOI. Millions of researchers have access to the formal publications on ScienceDirect, and so links will help users to find, access, cite and use the best available version. Please note that Cell Press, The Lancet and some society-owned have different preprint policies. Information on these policies is available on the journal homepage.

Accepted Author Manuscripts: An accepted author manuscript is the manuscript of an article that has been accepted for publication and which typically includes author-incorporated changes suggested during submission, peer review and editor-author communications.

Authors can share their accepted author manuscript:

- immediately
  - via their non-commercial person homepage or blog
  - by updating a preprint in arXiv or RePEc with the accepted manuscript
  - via their research institute or institutional repository for internal institutional uses or as part of an invitation-only research collaboration work-group
  - directly by providing copies to their students or to research collaborators for their personal use
  - for private scholarly sharing as part of an invitation-only work group on commercial sites with which Elsevier has an agreement
- After the embargo period
  - via non-commercial hosting platforms such as their institutional repository
  - via commercial sites with which Elsevier has an agreement

In all cases accepted manuscripts should:

- link to the formal publication via its DOI
- bear a CC-BY-NC-ND license - this is easy to do
- if aggregated with other manuscripts, for example in a repository or other site, be shared in alignment with our hosting policy not be added to or enhanced in any way to appear more like, or to substitute for, the published journal article.

Published journal article (JPA): A published journal article (PJA) is the definitive final record of published research that appears or will appear in the journal and embodies all value-adding publishing activities including peer review co-ordination, copy-editing, formatting, (if relevant) pagination and online enrichment.

Policies for sharing publishing journal articles differ for subscription and gold open access articles:

Subscription Articles: If you are an author, please share a link to your article rather than the full-text. Millions of researchers have access to the formal publications on ScienceDirect, and so links will help your users to find, access, cite, and use the best available version.

Theses and dissertations which contain embedded PJAs as part of the formal submission can be posted publicly by the awarding institution with DOI links back to the formal publications on ScienceDirect.

If you are affiliated with a library that subscribes to ScienceDirect you have additional private sharing rights for others' research accessed under that agreement. This includes use for classroom teaching and internal training at the institution (including use in course packs and courseware programs), and inclusion of the article for grant funding purposes.

Gold Open Access Articles: May be shared according to the author-selected end-user license and should contain a CrossMark logo, the end user license, and a DOI link to the formal publication on ScienceDirect.

Please refer to Elsevier's posting policy for further information.

18. **For book authors** the following clauses are applicable in addition to the above: Authors are permitted to place a brief summary of their work online only. You are not allowed to download and post the published electronic version of your chapter, nor may you scan the printed edition to create an electronic version. **Posting to a repository**: Authors are permitted to post a summary of their chapter only in their institution's repository.

19. **Thesis/Dissertation**: If your license is for use in a thesis/dissertation your thesis may be submitted to your institution in either print or electronic form. Should your thesis be published commercially, please reapply for permission. These requirements include

permission for the Library and Archives of Canada to supply single copies, on demand, of the complete thesis and include permission for Proquest/UMI to supply single copies, on demand, of the complete thesis. Should your thesis be published commercially, please reapply for permission. Theses and dissertations which contain embedded PJAs as part of the formal submission can be posted publicly by the awarding institution with DOI links back to the formal publications on ScienceDirect.

Elsevier Open Access Terms and Conditions

You can publish open access with Elsevier in hundreds of open access journals or in nearly 2000 established subscription journals that support open access publishing. Permitted third party re-use of these open access articles is defined by the author's choice of Creative Commons user license. See our open access license policy for more information.

Terms & Conditions applicable to all Open Access articles published with Elsevier:

Any reuse of the article must not represent the author as endorsing the adaptation of the article nor should the article be modified in such a way as to damage the author's honour or reputation. If any changes have been made, such changes must be clearly indicated.

The author(s) must be appropriately credited and we ask that you include the end user license and a DOI link to the formal publication on ScienceDirect.

If any part of the material to be used (for example, figures) has appeared in our publication with credit or acknowledgement to another source it is the responsibility of the user to ensure their reuse complies with the terms and conditions determined by the rights holder.

Additional Terms & Conditions applicable to each Creative Commons user license:

CC BY: The CC-BY license allows users to copy, to create extracts, abstracts and new works from the Article, to alter and revise the Article and to make commercial use of the Article (including reuse and/or resale of the Article by commercial entities), provided the user gives appropriate credit (with a link to the formal publication through the relevant DOI), provides a link to the license, indicates if changes were made and the licensor is not represented as endorsing the use made of the work. The full details of the license are available at http://creativecommons.org/licenses/by/4.0.

CC BY NC SA: The CC BY-NC-SA license allows users to copy, to create extracts, abstracts and new works from the Article, to alter and revise the Article, provided this is not done for commercial purposes, and that the user gives appropriate credit (with a link to the formal publication through the relevant DOI), provides a link to the license, indicates if changes were made and the licensor is not represented as endorsing the use made of the work. Further, any new works must be made available on the same conditions. The full details of the license are available at http://creativecommons.org/licenses/by-nc-sa/4.0.

CC BY NC ND: The CC BY-NC-ND license allows users to copy and distribute the Article, provided this is not done for commercial purposes and further does not permit distribution of the Article if it is changed or edited in any way, and provided the user gives appropriate credit (with a link to the formal publication through the relevant DOI), provides a link to the license, and that the licensor is not represented as endorsing the use made of the work. The full details of the license are available at http://creativecommons.org/licenses/by-nc-nd/4.0. Any commercial reuse of Open Access articles published with a CC BY NC SA or CC BY NC ND license requires permission from Elsevier and will be subject to a fee.

Commercial reuse includes:

- Associating advertising with the full text of the Article
- Charging fees for document delivery or access
- Article aggregation
- Systematic distribution via e-mail lists or share buttons

Posting or linking by commercial companies for use by customers of those companies.

20. **Other Conditions:**

v1.10

Questions? E-mail us at customercare@copyright.com.

The Permission below is for Figure 4.2.

ELSEVIER LICENSE TERMS AND CONDITIONS

Feb 19, 2024

This Agreement between University of South Florida -- Moheb Abdelmalak ("You") and Elsevier ("Elsevier") consists of your license details and the terms and conditions provided by Elsevier and Copyright Clearance Center.

License Number	5724670012798
License date	Feb 09, 2024
Licensed Content Publisher	Elsevier
Licensed Content Publication	Structures
Licensed Content Title	Dynamic evaluation method for Time-variant reliability of structural safety of Concrete-faced rockfill dam
Licensed Content Author	Jiahui Yang,Liang Pei,Chufeng Kuang,Yanling Li,Yi Liu
Licensed Content Date	Nov 1, 2023
Licensed Content Volume	57
Licensed Content Issue	n/a
Licensed Content Pages	1
Start Page	105095
End Page	0
Type of Use	reuse in a thesis/dissertation
Portion	figures/tables/illustrations
Number of figures/tables/illustrations	1
Format	electronic
Are you the author of this Elsevier article?	No
Will you be translating?	No
Title of new work	The effect of Bus observability on detection and localization of FDIA attacks in Smart grids
Institution name	University of south flroida
Expected presentation date	Feb 2024
Portions	Figure 1
Requestor Location	University of South Florida
	Attn: University of South Florida
Publisher Tax ID	98-0397604
Total	**0.00 USD**
Terms and Conditions	

INTRODUCTION

1. The publisher for this copyrighted material is Elsevier. By clicking "accept" in connection with completing this licensing transaction, you agree that the following terms and conditions apply to this transaction (along with the Billing and Payment terms and conditions established by Copyright Clearance Center, Inc. ("CCC"), at the time that you opened your RightsLink account and that are available at any time at https://myaccount.copyright.com).

GENERAL TERMS

2. Elsevier hereby grants you permission to reproduce the aforementioned material subject to the terms and conditions indicated.

3. Acknowledgement: If any part of the material to be used (for example, figures) has appeared in our publication with credit or acknowledgement to another source, permission must also be sought from that source. If such permission is not obtained then that material may not be included in your publication/copies. Suitable acknowledgement to the source must be made, either as a footnote or in a reference list at the end of your publication, as follows:
"Reprinted from Publication title, Vol /edition number, Author(s), Title of article / title of chapter, Pages No., Copyright (Year), with permission from Elsevier [OR APPLICABLE SOCIETY COPYRIGHT OWNER]." Also Lancet special credit - "Reprinted from The Lancet, Vol. number, Author(s), Title of article, Pages No., Copyright (Year), with permission from Elsevier."
4. Reproduction of this material is confined to the purpose and/or media for which permission is hereby given. The material may not be reproduced or used in any other way, including use in combination with an artificial intelligence tool (including to train an algorithm, test, process, analyse, generate output and/or develop any form of artificial intelligence tool), or to create any derivative work and/or service (including resulting from the use of artificial intelligence tools).
5. Altering/Modifying Material: Not Permitted. However figures and illustrations may be altered/adapted minimally to serve your work. Any other abbreviations, additions, deletions and/or any other alterations shall be made only with prior written authorization of Elsevier Ltd. (Please contact Elsevier's permissions helpdesk here). No modifications can be made to any Lancet figures/tables and they must be reproduced in full.
6. If the permission fee for the requested use of our material is waived in this instance, please be advised that your future requests for Elsevier materials may attract a fee.
7. Reservation of Rights: Publisher reserves all rights not specifically granted in the combination of (i) the license details provided by you and accepted in the course of this licensing transaction, (ii) these terms and conditions and (iii) CCC's Billing and Payment terms and conditions.
8. License Contingent Upon Payment: While you may exercise the rights licensed immediately upon issuance of the license at the end of the licensing process for the transaction, provided that you have disclosed complete and accurate details of your proposed use, no license is finally effective unless and until full payment is received from you (either by publisher or by CCC) as provided in CCC's Billing and Payment terms and conditions. If full payment is not received on a timely basis, then any license preliminarily granted shall be deemed automatically revoked and shall be void as if never granted. Further, in the event that you breach any of these terms and conditions or any of CCC's Billing and Payment terms and conditions, the license is automatically revoked and shall be void as if never granted. Use of materials as described in a revoked license, as well as any use of the materials beyond the scope of an unrevoked license, may constitute copyright infringement and publisher reserves the right to take any and all action to protect its copyright in the materials.
9. Warranties: Publisher makes no representations or warranties with respect to the licensed material.
10. Indemnity: You hereby indemnify and agree to hold harmless publisher and CCC, and their respective officers, directors, employees and agents, from and against any and all claims arising out of your use of the licensed material other than as specifically authorized pursuant to this license.
11. No Transfer of License: This license is personal to you and may not be sublicensed, assigned, or transferred by you to any other person without publisher's written permission.
12. No Amendment Except in Writing: This license may not be amended except in a writing signed by both parties (or, in the case of publisher, by CCC on publisher's behalf).
13. Objection to Contrary Terms: Publisher hereby objects to any terms contained in any purchase order, acknowledgment, check endorsement or other writing prepared by you, which terms are inconsistent with these terms and conditions or CCC's Billing and Payment terms and conditions. These terms and conditions, together with CCC's Billing and Payment terms and conditions (which are incorporated herein), comprise the entire agreement between you and publisher (and CCC) concerning this licensing transaction. In the event of any conflict between your obligations established by these terms and conditions and those established by CCC's Billing and Payment terms and conditions, these terms and conditions shall control.
14. Revocation: Elsevier or Copyright Clearance Center may deny the permissions described in this License at their sole discretion, for any reason or no reason, with a full refund payable to you. Notice of such denial will be made using the contact information provided by you. Failure to receive such notice will not alter or invalidate the denial. In no event will Elsevier or Copyright Clearance Center be responsible or liable for any costs, expenses or damage incurred by you as a result of a denial of your permission request, other than a refund of the amount(s) paid by you to Elsevier and/or Copyright Clearance Center for denied permissions.

LIMITED LICENSE

The following terms and conditions apply only to specific license types:
15. **Translation**: This permission is granted for non-exclusive world **English** rights only unless your license was granted for translation rights. If you licensed translation rights you may only translate this content into the languages you requested. A professional translator must perform all translations and reproduce the content word for word preserving the integrity of the article.
16. **Posting licensed content on any Website**: The following terms and conditions apply as follows: Licensing material from an Elsevier journal: All content posted to the web site must maintain the copyright information line on the bottom of each image; A hyper-text must be included to the Homepage of the journal from which you are licensing at http://www.sciencedirect.com/science/journal/xxxxx or the Elsevier homepage for books at http://www.elsevier.com; Central Storage: This license does not include permission for a scanned version of the material to be stored in a central repository such as that provided by Heron/XanEdu.

Licensing material from an Elsevier book: A hyper-text link must be included to the Elsevier homepage at http://www.elsevier.com . All content posted to the web site must maintain the copyright information line on the bottom of each image.

Posting licensed content on Electronic reserve: In addition to the above the following clauses are applicable: The web site must be password-protected and made available only to bona fide students registered on a relevant course. This permission is granted for 1 year only. You may obtain a new license for future website posting.

17. **For journal authors**: the following clauses are applicable in addition to the above:

Preprints:

A preprint is an author's own write-up of research results and analysis, it has not been peer-reviewed, nor has it had any other value added to it by a publisher (such as formatting, copyright, technical enhancement etc.).

Authors can share their preprints anywhere at any time. Preprints should not be added to or enhanced in any way in order to appear more like, or to substitute for, the final versions of articles however authors can update their preprints on arXiv or RePEc with their Accepted Author Manuscript (see below).

If accepted for publication, we encourage authors to link from the preprint to their formal publication via its DOI. Millions of researchers have access to the formal publications on ScienceDirect, and so links will help users to find, access, cite and use the best available version. Please note that Cell Press, The Lancet and some society-owned have different preprint policies. Information on these policies is available on the journal homepage.

Accepted Author Manuscripts: An accepted author manuscript is the manuscript of an article that has been accepted for publication and which typically includes author-incorporated changes suggested during submission, peer review and editor-author communications.

Authors can share their accepted author manuscript:

- immediately
  - via their non-commercial person homepage or blog
  - by updating a preprint in arXiv or RePEc with the accepted manuscript
  - via their research institute or institutional repository for internal institutional uses or as part of an invitation-only research collaboration work-group
  - directly by providing copies to their students or to research collaborators for their personal use
  - for private scholarly sharing as part of an invitation-only work group on commercial sites with which Elsevier has an agreement
- After the embargo period
  - via non-commercial hosting platforms such as their institutional repository
  - via commercial sites with which Elsevier has an agreement

In all cases accepted manuscripts should:

- link to the formal publication via its DOI
- bear a CC-BY-NC-ND license - this is easy to do
- if aggregated with other manuscripts, for example in a repository or other site, be shared in alignment with our hosting policy not be added to or enhanced in any way to appear more like, or to substitute for, the published journal article.

Published journal article (JPA): A published journal article (PJA) is the definitive final record of published research that appears or will appear in the journal and embodies all value-adding publishing activities including peer review co-ordination, copy-editing, formatting, (if relevant) pagination and online enrichment.

Policies for sharing publishing journal articles differ for subscription and gold open access articles:

Subscription Articles: If you are an author, please share a link to your article rather than the full-text. Millions of researchers have access to the formal publications on ScienceDirect, and so links will help your users to find, access, cite, and use the best available version.

Theses and dissertations which contain embedded PJAs as part of the formal submission can be posted publicly by the awarding institution with DOI links back to the formal publications on ScienceDirect.

If you are affiliated with a library that subscribes to ScienceDirect you have additional private sharing rights for others' research accessed under that agreement. This includes use for classroom teaching and internal training at the institution (including use in course packs and courseware programs), and inclusion of the article for grant funding purposes.

Gold Open Access Articles: May be shared according to the author-selected end-user license and should contain a CrossMark logo, the end user license, and a DOI link to the formal publication on ScienceDirect.

Please refer to Elsevier's posting policy for further information.

18. **For book authors** the following clauses are applicable in addition to the above: Authors are permitted to place a brief summary of their work online only. You are not allowed to download and post the published electronic version of your chapter, nor may you scan the printed edition to create an electronic version. **Posting to a repository**: Authors are permitted to post a summary of their chapter only in their institution's repository.

19. **Thesis/Dissertation**: If your license is for use in a thesis/dissertation your thesis may be submitted to your institution in either print or electronic form. Should your thesis be published commercially, please reapply for permission. These requirements include

permission for the Library and Archives of Canada to supply single copies, on demand, of the complete thesis and include permission for Proquest/UMI to supply single copies, on demand, of the complete thesis. Should your thesis be published commercially, please reapply for permission. Theses and dissertations which contain embedded PJAs as part of the formal submission can be posted publicly by the awarding institution with DOI links back to the formal publications on ScienceDirect.

Elsevier Open Access Terms and Conditions

You can publish open access with Elsevier in hundreds of open access journals or in nearly 2000 established subscription journals that support open access publishing. Permitted third party re-use of these open access articles is defined by the author's choice of Creative Commons user license. See our open access license policy for more information.

Terms & Conditions applicable to all Open Access articles published with Elsevier:

Any reuse of the article must not represent the author as endorsing the adaptation of the article nor should the article be modified in such a way as to damage the author's honour or reputation. If any changes have been made, such changes must be clearly indicated.

The author(s) must be appropriately credited and we ask that you include the end user license and a DOI link to the formal publication on ScienceDirect.

If any part of the material to be used (for example, figures) has appeared in our publication with credit or acknowledgement to another source it is the responsibility of the user to ensure their reuse complies with the terms and conditions determined by the rights holder.

Additional Terms & Conditions applicable to each Creative Commons user license:

CC BY: The CC-BY license allows users to copy, to create extracts, abstracts and new works from the Article, to alter and revise the Article and to make commercial use of the Article (including reuse and/or resale of the Article by commercial entities), provided the user gives appropriate credit (with a link to the formal publication through the relevant DOI), provides a link to the license, indicates if changes were made and the licensor is not represented as endorsing the use made of the work. The full details of the license are available at http://creativecommons.org/licenses/by/4.0.

CC BY NC SA: The CC BY-NC-SA license allows users to copy, to create extracts, abstracts and new works from the Article, to alter and revise the Article, provided this is not done for commercial purposes, and that the user gives appropriate credit (with a link to the formal publication through the relevant DOI), provides a link to the license, indicates if changes were made and the licensor is not represented as endorsing the use made of the work. Further, any new works must be made available on the same conditions. The full details of the license are available at http://creativecommons.org/licenses/by-nc-sa/4.0.

CC BY NC ND: The CC BY-NC-ND license allows users to copy and distribute the Article, provided this is not done for commercial purposes and further does not permit distribution of the Article if it is changed or edited in any way, and provided the user gives appropriate credit (with a link to the formal publication through the relevant DOI), provides a link to the license, and that the licensor is not represented as endorsing the use made of the work. The full details of the license are available at http://creativecommons.org/licenses/by-nc-nd/4.0. Any commercial reuse of Open Access articles published with a CC BY NC SA or CC BY NC ND license requires permission from Elsevier and will be subject to a fee.

Commercial reuse includes:

- Associating advertising with the full text of the Article
- Charging fees for document delivery or access
- Article aggregation
- Systematic distribution via e-mail lists or share buttons

Posting or linking by commercial companies for use by customers of those companies.

20. **Other Conditions:**

v1.10

Questions? E-mail us at customercare@copyright.com.