Chapter 1

Introduction

The modern smart grid framework is evolving as a combination of both physical (generation, transmission, and distribution) and as complex cyber (communication infrastructure) systems. Rapid integration of complex communication infrastructures within the traditional power system has made the modern power grid more reliable. With the implementation of two-way digital communication capabilities followed by distributed intelligence, it can be seen that the conventional grid demonstrates a more efficient operation [3,4]. While modern communication protocols provide real-time grid information to the operator, it also makes the grid vulnerable to cyber attacks. An attack is an intrusion into the system. Hence, appropriate security enforcements need to be implemented to mitigate such vulnerabilities [5,6]. A modern grid has a high degree of automation. The evolving nature of automation of smart grids poses a serious threat to the systems. As substation automation is increasing day by day, there is an increasing risk as any intruder can interfere with the control signals as well as the data transferred to the upper levels of SCADA. Therefore, a cyber-attack may cause mal-operations (like tripping of healthy lines, shedding of essential loads, disturbing the economic load dispatch of the generators, and changing the locational marginal pricing of the network) of the grid. Attacks targeted against the wide-area measurement systems, RTUs and SCADA are more likely to damage the utilities as well as demonstrate a significant impact on the end consumers [7–15]. Hence, a smart grid architecture requires secure network communication and enhanced data privacy for a safe, reliable and stable operation.

Attacks can be defined over several modes of intrusions into the system. Embedded devices on the field are more critical to secure than the communication channels and

conduits as such devices come with vendor-specific software which can not be secured with general-purpose firewalls. The embedded field devices generally lack security protocols as well. The European Union (EU) smart grid mandate M490 has proposed a five-layer smart Grid architecture model (SGAM) framework [1]. Most of the present security protocols deal with the upper layers of the EU mandate as shown in Fig. 1.1. Out of the five layers reported in [1], the business layer is made more secure with updates and security protection. Presently, most utilities provide a firewall security to business and function layers, thereby making the component layer most susceptible to a possible cyber-attack. Therefore, proper security inspection of nodal endpoints (on-field devices) is essential with the other cyber-security aspects of the modern smart grid (includes communication, data, and the physical layer).

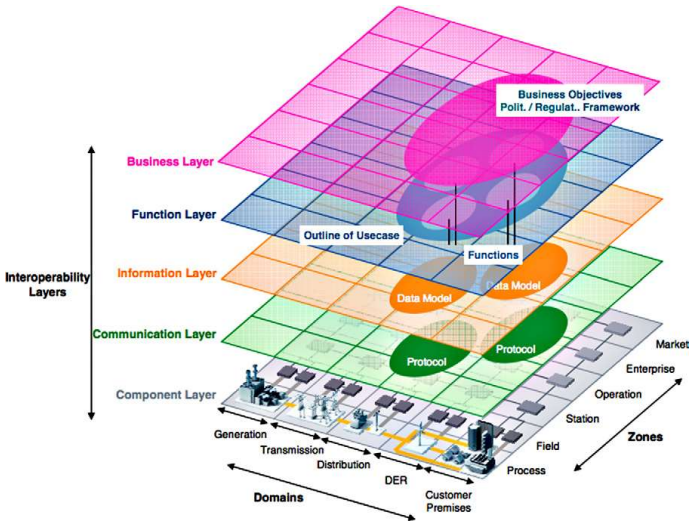

Figure 1.1: SGAM framework with interoperability layers [1]

1.1 Background

With an effective undermining of the critical vulnerabilities of the aforementioned loosely secured nodal endpoints like meters, sensors, RTUs, communication channels, etc. several genres of attack can be imposed on the power network. Although such attacks take place using different channels, their primary motive is to define critical scenarios in the power sector, hence leading to mal-operations of the grid. Fig. 1.2 furnishes some of the key prevalent attack strategies on the modern grid which can be briefly demonstrated as

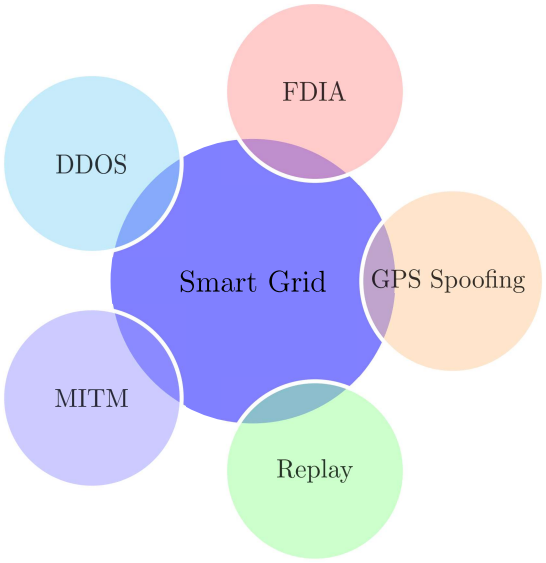

Figure 1.2: Various types of attacks on the grid

follows:

- DDOS attack:- This class of attack has the potential of injecting inadvertent delays in the communication layer of the grid [16–23]. Due to the lack of real-time data, operators may find it difficult to gain adequate measurements for state estimation algorithms. A DDOS attack can lead to a delay of control and measurement signals from the control center to the component layers and vice versa. Hence, it poses a critical challenge to grid operation and leads to diverse genres of attacks on the information and communication layer of the smart grid. The DDoS attack is an advanced version of the DoS (denial of service) attack where multiple sources are used for an attack and are spread by numerous hosts making the defense strategy difficult. Such an attack strategy also disturbs the targeted part of the network (part or whole of the grid) by targeting the AMI as the nodal endpoints or gateways and leads to devastating situations, thus bringing down a large grid infrastructure. The utilities generally do not provide any security firewall for the AMI. As a consequence, the DDoS attack becomes much more detrimental. An overview of country-wise DDOS attacks on the power grid can be demonstrated in Fig. 1.3.

- MITM attack:- These types of attacks are performed by intruding into the communication system between the host and the sender [23–28] where the attacker can listen and modify the data transferred between the host and the sender. This leads to a

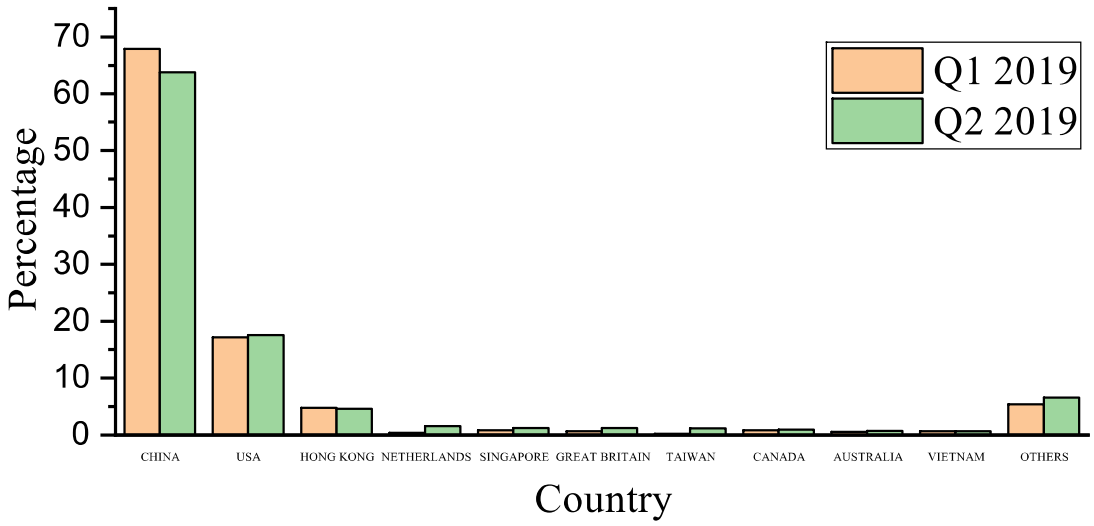

Figure 1.3: Country-wise DDOS attacks in the power grid [2]

loss of data integrity, safety, and confidentiality. The host remains unaware that the communication between the transmitter and receiver has been compromised. Such an attack tries to outmaneuver mutual authentication of the transmitter and the receiver. Hence, a MITM attack can succeed if and only if the attacker can emulate the nodal endpoints at the component layer successfully.

- Replay attack:- An attack modeled in the network layer which malevolently repeats or delays the information during the transmission of traffic [29–35]. AMIs can be targeted as the prime sources of these attacks. Any repetition of sequences of control actions if given to the system with the aid of this attack may lead to cascading failures in the grid, hence causing a catastrophe. Attackers generally tend to interpret the data in the communication layer, and while gaining access, can duplicate transactions. The EMS module within SCADA which hosts the state estimation algorithm remains unaware of such an attack. Any replay attack has a two-layered methodology. The attacker first analyses and records a control action sent to the remote controller from the control center and then duplicates it in the next time frame.

- GPS spoofing attack:- A modern smart grid network uses PMUs for data measurement and data transfer between the on-field devices and the PDC, which aggregates the data and communicates it to the SCADA for efficient state estimation of the

Item No.	Type of attack	Targeting layer
1	DDOS	Communication
2	MITM	Communication
3	Replay attack	Communication
4	FDIA	Data/Information
5	GPS spoofing attack	Physical/Communication
6	Time synchronization attack	Physical
7	Delay attack	Physical/Communication
8	Load redistribution attack	Data/Information

Table 1.1: Various types of attacks on the smart grid

power network. Every PMU is enabled with GPS time stamping so that the SCADA may get accurate information of the field measurements and can make appropriate decisions. Such kind of a time-stamping of the acquired measurements leads to enhanced security at the physical layer of the on-field devices against FDIAs. To overcome this, the attacker can effectively modify the GPS time stamping of the PMUs and thus can launch an attack [36–41]. The measurements received at the SCADA seem to be redundant to the operator, thus bypassing the actual field measurements.

Table 1.1 summarizes different attacks at the different layers of the smart grid architecture. Though other types of cyberattacks exist (like load redistribution attacks, time-synchronization attack), the above-mentioned attack strategies are more prevalent and are highly detrimental to system operation. Although such aforesaid types of attacks on the grid are existing, this thesis undertakes the most detrimental attack amongst them, i.e. the FDIA. It can be seen that FDIA tries to develop false estimation measures of the operating states, hence developing mal-operations of the grid. Such attacks target the nodal endpoints present in the component layer like the RTUs, and meters. The sole intent of the attacker is to by pass the bad data identification algorithm and hamper the states estimated. The attacker may try to get some economic benefit, mal-trip the relays or redistribute the load by implementing such an attack. It can be seen from Fig. 1.4 that all such aforementioned genres of attack may be interlinked and may develop

critical scenarios in the power sector. The attacker may initially implement the MITM attack, from which an effective extraction of information pertaining to the grid topology and measurements can be achieved. Such informations are crucial and holds the primary underlying framework of the attacker to develop the topology matrix of the system, which leads to an effective implementation of FDIA. Such kind of interlinked attack strategies also hold for replay, DDOS and GPS spoofing attacks as well.

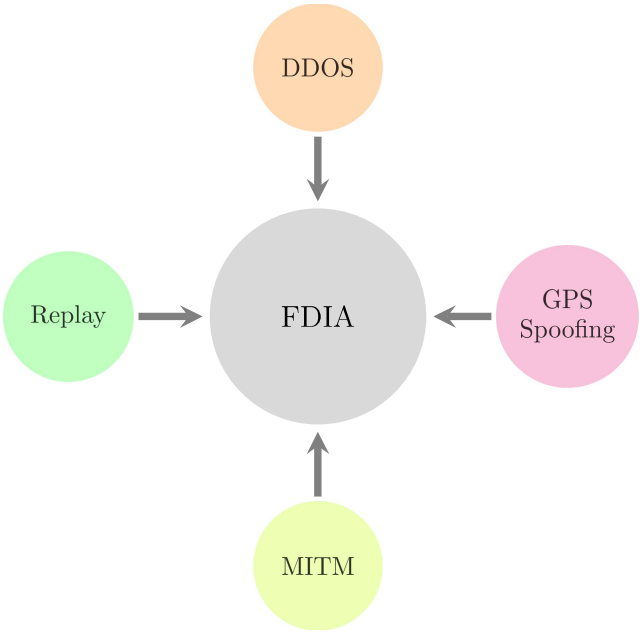

Figure 1.4: Interconnected attacks on the grid

1.2 Motivation

The modern power sector ensures a reliable, secure, and stable grid operation by incorporating contemporary IIOT technology, hence furnishing a bidirectional flow of power with information. It provides rapid operation of the grid along with automation. This inherently incorporates an advanced communication infrastructure that is capable of transferring measurement data from the PDC to the local control center and vice versa. This leads to a potential risk in modern grid operation [3]. Recently, a new genre of cyber-attack, more specifically a class of data integrity attacks targeting not only the communication system peers but also the state estimation algorithms has been reported (FDIA), which can effectively undermine the WAMS, hence posing a new vulnerability to the modern

smart grid [42]. It can easily circumvent the traditional BDDs, hence generating a set of forged state estimates. Such kinds of BDDs are implemented to filter the raw field measurements acquired at SCADA. The sole intent of such an attack is to falsify the system measurements of multiple RTUs and sensors in the component layer, hence misleading the decision-making process of the operator at the control center. The state estimation algorithm is an essential component of the modern EMS which helps to determine the current operating conditions of the grid from the set of available measurements [43,44]. It can be seen from [43] that critical grid operations like voltage regulation, optimal power flow, and dynamic electricity pricing. depend on the solution of the state estimation algorithms. Thus, any attack vector injected due to FDIA leads to a set of falsified operating states, hence demonstrating a critical operating scenario of the grid.

FDIA has also demonstrated its potential to develop transmission line congestion with significant financial losses [45]. Moreover, it can also lead to a potential interference of the generated control signals [46–48]. It can be inferred that with a limited topology, measurement, and parameter information, a perfect FDIA can still be successfully implemented [49–57]. Recently, a minimal attack vector formulation strategy has been demonstrated which shows its deleterious effects while targeting multiple state variables [58]. Furthermore, some recent studies have also furnished that the adversary may even gain some economic benefit from the electricity market [45, 59–64] or may even mal-trip the relays of healthy transmission lines [65–67] and even may redistribute the load at the respective buses [50, 68–71]. Such an attack may also lead to catastrophic consequences on the grid [72]. A diligent study on such attacks against both linear and nonlinear state estimators shows its calamitous nature [73–76]. Experts have also quantified a trade-off between the system model accuracy and the attack impact for various bad data detection schemes [77]. Recently, a massive electricity outage triggered by modern cyber-attacks (FDIA) have been reported on the Ukrainian power grid in 2015 [78]. Furthermore, cyber-attacks aiming to gain access to remote endpoints of the power network have been identified by the US Computer Emergency Readiness Team [79]. Grid operators of modern smart cities are still defining ways to combat and characterize such attacks. An overview of FDIA on the power grid can be represented in Fig. 1.5. It can be seen from Fig. 1.5 that the set of compromised measurements acquired at the control center may develop harmful consequences over the subsequent applications like unit

commitment, optimal power flow, etc. as these operations inherently depend on the state estimation algorithm in the EMS.

Attacks against the distribution sector like consumers, feeders, and substations have also been demonstrated which leads to a significant socio-economic impact on the power sector [80]. A set of falsified state estimates may eventually lead to a potential mal-operation of the grid, hence a new concept of holistic resilience cycle has been recently demonstrated which is primarily introduced to enhance the cyber-physical security of the grid [81]. With access to smart meters of the consumers, such attacks may target the data integrity of energy supply and demand and is capable of successfully modifying the measurements [82, 83]. Attacking the transmission sector with such kind of attacks by targeting the optimal power flow module within the EMS in the control center may also develop overloading of the transmission lines with a possibility of physical damage and power outage [84]. In the case of microgrids, FDIAs may effectively lead to power losses with significant disruption in dynamic microgrid partitioning [82, 85, 86]. Some of the prevalent approaches for defining effective FDIAs against the modern grid can be seen as per Fig. 1.6. Although linear transformation approach [87] and limited topology information [49] based FDIAs require the knowledge of the topology matrix, data-driven [88] and principal component analysis (PCA) [89] based schemes incorporate the acquired measurement subspace for an effective formulation of the attack vector. Some recent works have also shown effective attack vector formulation against residential buildings using game theoretic approaches [90].

It is seen that most of the attack vectors that can effectively bypass the residue test as employed by the traditional BDD are formulated on the basis of the full column space of the topology matrix. With access to an adequate number of measurements, low-rank subspace-based data-driven attack vector formulation using RSVD and FSVD has recently demonstrated a significant impact [53, 91]. It can be seen from [92, 93] that the intruder is capable of developing localized stealthy attack vectors even with limited topology information of the grid. A critical survey portraying the effects of false data injection attacks on the power sector can be seen in [94].

$\mathcal{L}_0$ and $\mathcal{L}_1$ norm-based security indices have been recently proposed which can critically define the severity of such attack vectors [95]. Classification of the measurements using an $\mathcal{L}_0$ norm-based safety index has also demonstrated promising results [96]. With a

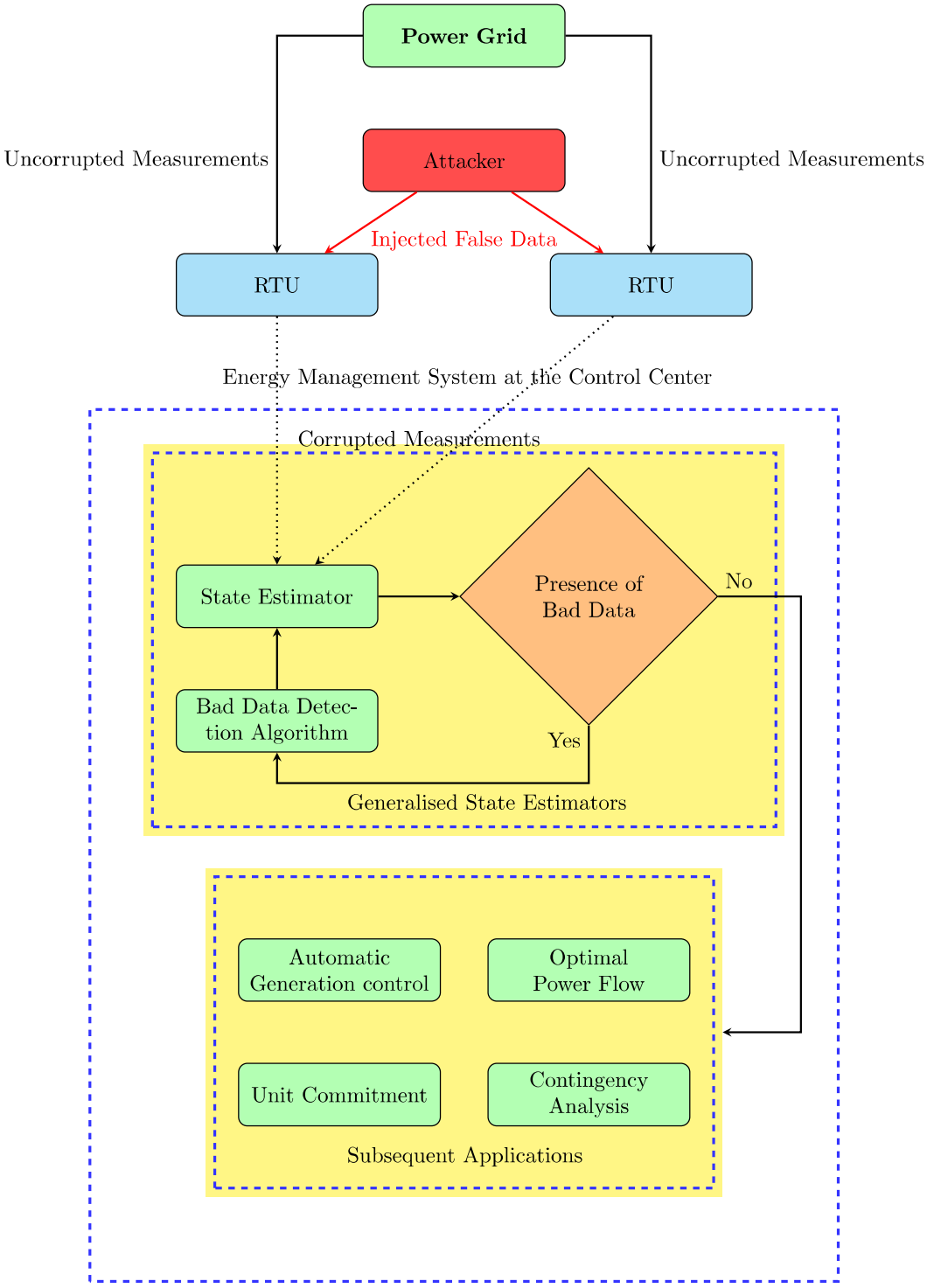

Figure 1.5: FDIA on the power grid

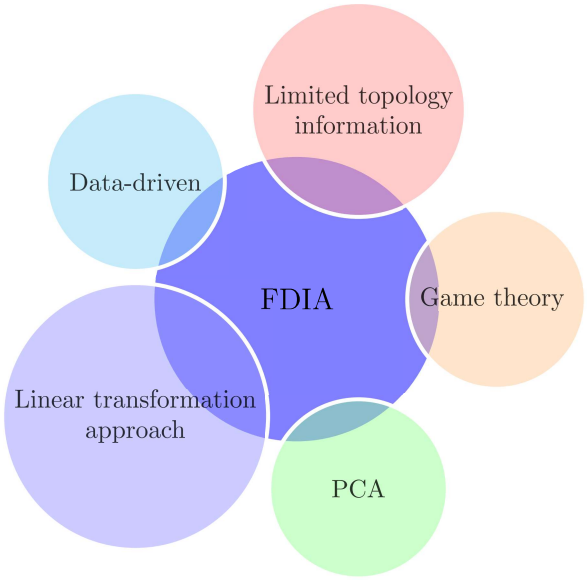

Figure 1.6: Existing methods for developing FDIA

minimal number of protected meters, attack vectors targeted for a specified state variable have also shown their detrimental outcomes [97].

It can be seen that the adversaries can compromise the operation of critical grid functions like protection and control actions using such kinds of attacks. For any intelligent electronic devices (IEDs) connected with a relay or potential or current transformers that use the standard IEC 61850-based substation automation, such attacks when injected within the data stream that is delivered to the control centre may lead to a maloperation [98]. Furthermore, it can be seen that by undermining the vulnerabilities of such IEDs, attack vectors may lead to compromised operation of the utilities [99]. An effective analysis of the GOOSE packets sent from the protection IEDs is henceforth necessary to detect such attacks and prevent the breakers from mal-tripping. Message authentication schemes as shown in [98] can reduce the latency in the data stream due to attack. An enhanced dependency on the IEC 61850 standard for the operation of modern substations may lead to a faster response and enhanced automation, but FDIAs have demonstrated that it can change the relay configurations, time-setting multipliers etc. Thus it may lead to apparent fault currents due to changes in loads and may also demonstrate incorrect response time during actual faults in the network [100]. In the case of control actions generated from the control centre, it can be seen that such attacks can eventually lead to a compromised operation of the automatic generation control [101]. Hence, resilient

controllers incorporating extended Kalman filters with artificial neural networks define an efficient framework [102]. It can be seen that FDIAs can also trigger inter-area oscillations in the power network by injecting malicious data within the sensors and the actuators. Robust designing of sliding mode controllers is henceforth necessary to mitigate the effect of such attacks [103].

1.2.1 Defence strategies

Several researchers have also proposed effective solutions to detect FDIA in real-time followed by its mitigation strategies [104–107]. Efficient identification of the such class of attacks within the raw measurements at SCADA is a potential research prospect [108–111]. The primary defense strategies adopted in practice can be categorized into two different classes like physical defending policy and data-driven detection schemes. In the case of physical defending policy, the grid operator defines a critical set of RTUs and sensors on the basis of which the full rank topology matrix can be formulated [71, 112–115], hence ensuring grid observability under all circumstances [116, 117]. With an optimal allocation of PMUs, the set of acquired measurements can be protected from such a class of attacks, hence improving the resiliency of the state estimation algorithms [97, 118–120]. An algorithm has been recently formulated which defines the measurements that need to be protected based on the adversary's choice of sparsest measurement set. Moreover, two specific scenarios have been considered like protecting an individual sensor or PMU with its respective measurement along with protection of all such units connected to a specific bus. However, such an approach has an inherent shortcoming as the number of sensors needed to be protected is generally large. The minimal set of on-field sensors and their corresponding measurements that needs to be protected in order to ensure a secure grid operation can be seen as per [121]. Furthermore, a novel security index has also been proposed which indicates the power flow measurements that are easier for the attacker to manipulate [96]. It can be also seen from [96] that for most practical scenarios of attack, the adversarial needs to compromise a number of measurements in the order of $(3n + 1)$, where n represents any positive integer. The primary drawback of physical defending policy using PMUs is the high cost and minimal possibility of reconfiguration and reallocation of such devices followed by the selection of the critical set of measurements needed to be protected. Furthermore, there is a drop in measurement redundancy, hence

an optimal solution of the estimation model can not be guaranteed under all operating conditions [122]. Although PMUs and PDCs are considered to be secured and robust phasor measurement units of the smart grid against FDIAs, it is evident that modern collusive false data injection attacks can compromise them. A decentralized homomorphic computation paradigm has demonstrated an efficient resilience against such advanced attacks [123].

Recently, with the implementation of graph signal processing and graph Fourier transform, detection of undetectable stealthy FDIA with high accuracy has been achieved [124, 125]. Tree pruning-based approximation algorithms have also defined a scalable attack detection policy [126]. Anomaly detection approaches undertaking the forecasted and the estimated set of operating states at SCADA have also defined a prospective FDIA detection scheme [108, 109, 127–129]. A generalized likelihood estimator based on historical data of operating states has also showcased an effective attack detection policy [105]. With the grid under steady-state operating conditions, matrix factorization schemes based on the dc state estimation algorithm incorporating low-rank structures have also shown an effective FDIA detection strategy. Such an approach is robust and showcases lesser false alarm rates. The proposed strategy fails to showcase higher accuracy in real-time identification of FDIA when the grid faces contingency scenarios [130].

Another key improvement in the defense strategy for such attacks has been furnished which tries to enhance and further improve the residue test-based BDDs. Recently, a comparative analysis between the L_∞ and L_2 norm-based BDDs have also been demonstrated [131, 132]. Advanced statistical BDDs capable of identifying such attacks which incorporate adaptive cumulative sum charts along with generalized likelihood ratio tests have been also furnished [105, 133–138].

The operator may also implement a probing scheme for efficient detection of such attacks [139]. Such a scheme usually incorporates some change in the admittances of the transmission line or the network parameters by the operator and is followed up with the estimation of states using the state estimation algorithm. Efficient detection of FDIA can be achieved if the expected change of the estimated states does not converge to the original set of state estimates. Such an approach of detecting FDIAs by changing the admittances of the transmission lines of the grid has also been implemented using D-FACTS devices as well [140, 141].

Recent works have also promoted distributed system state estimation where the operator usually disintegrates the large grid into several parts and implements the state estimation algorithm individually. Such an approach defines a robust technique against attack vector intrusions [142–144]. With sparse structures of the attack matrix, a novel attack detection scheme using the low-rank structure of the uncorrupted measurements has recently furnished promising results [111]. As temporal and spatial features of state variables under attack are subjected to deviations from the distribution of uncorrupted state estimates, a novel cyber-attack detection model using SVD and fast Fourier transform has recently demonstrated a high presence detection accuracy [145]. With the incorporation of image processing techniques, temporal data of state estimates have been recently encoded into 2D colored images. Deep CNNs trained on such datasets have also furnished a higher classification accuracy with a high F_1 score [146]. Such schemes lead to computer vision-based attack detection strategies.

With rapid development in data-driven techniques, identification of FDIA with high accuracy has been portrayed [147, 148]. Machine learning approaches like Bayesian network, Random forest, AdaBoost, SVMs, etc. have been also demonstrated as quick and efficient FDIA identification policies [138, 149–152]. Following the variations in the measurement set due to attack vector intrusions, FDIA identification has been made possible with metrics like Kullback-Leibler distance (KLD) [122]. Dynamic time-varying state estimation models along with Markov chain-based analytical approach leads to the quickest intrusion detection scheme under power grid restructuring and topology reconfiguration [153]. Researchers have also developed advanced graph neural network-based scalable real-time FDIA detectors which undertake the graph topology with spatially temporal correlated measurements of the grid. Such detectors promote a high presence detection accuracy as well [154]. State forecasting-driven FDIA detection schemes for linear and nonlinear state estimation algorithms have also demonstrated an attack detection accuracy of more than 90% [155, 156]. Locational detection schemes of FDIA using machine learning algorithms based on principal component analysis and canonical correlation analysis have also developed advanced attack detection policies [157].

With the rapid progress of machine learning techniques, real-time detection of FDIA can be achieved [106, 107]. Several unsupervised and supervised learning algorithms are also proposed to distinguish between normal and attack operating conditions of the grid

[106]. Machine learning techniques have also been implemented to identify the presence of anomalies on the power system topology database [104]. Conditional deep belief networks based on temporal features of attack have also shown higher accuracy values of nearly 90% for effective detection of FDIA [158]. Several researchers have also showcased effective FDIA detection policies for the dc state estimation algorithm namely time series analysis [159], statistical analysis [160], state forecasting driven detection schemes [161, 162] along with advanced machine learning techniques [106, 163, 164]. A diligent survey portraying the several types of detection policies of FDIA can be seen in [165]. Table 1.2 summarises the current research focus for various types of FDIAs.

Current focus on FDIA research	Classification	Literature reviews
Researches based on theoretical approaches for constructing a perfect FDIA	Construction of FDIA with full knowledge of parameter and topology information of the grid	[42, 166, 166–168] [169–173]
	Construction of FDIA with incomplete topology information of the grid	[49, 51, 174, 175]
	Construction of FDIA with falsified topology	[71, 176–178]
	Construction of FDIA against nonlinear state estimation algorithm	[55, 57, 73, 122, 156, 179–182]
Researches focussing on the several footprints of FDIA	Grid economy and electricity market	[59, 183–188]
	Load redistribution	[50, 69, 189]
Defence strategies	Optimal placement of PMUs	[113–115, 190]
	Machine leaning based FDIA detection	[106, 191–194]
	Deep learning based FDIA detection	[195–201]

Table 1.2: A comprehensive survey pertaining to FDIA research

1.3 Objectives

However, the formulation of stealthy attack vectors is also an important objective of this thesis. Such attack vectors defined on the low-rank subspace of the topology matrix are

capable of bypassing the conventional BDDs under some specific constraints. A comparative analysis of low-rank approximation algorithms under varying noise and outliers has demonstrated the efficacy of the proposed approach. The developed scheme has a small computational burden, hence can be adopted for real-time attack vector formulation on the grid even for large-scale networks.

Additionally, most of the prevailing studies showcase an effective FDIA detection policy when prior information of the grid along with statistical models of the attack vector formulation are present. Recently, rapid developments in data-driven identification strategies have gained renowned importance, hence deep learning techniques can be successfully implemented to effectively detect FDIA. These models can be trained directly on the available raw measurement data without deriving any predefined model of the attack vector and the grid. Furthermore, with rapid advancement in machine learning approaches, an effective state forecasting scheme has been also showcased in this thesis. Such trained state forecasting models demonstrate a minimal RMSE, MSE, and MAE index. Accurate presence detection of FDIA within the set of acquired measurements by deploying such trained deep learning-based state forecasting models followed by two effective anomaly detection schemes within the set of estimated states has also been presented.

Moreover, most of the recent detection algorithms focus on the detection of the presence of FDIA, whereas very little research showcases an exact detection of their intrusion points. To downplay this issue, this thesis portrays a critical comparison between several deep learning architectures and a conventional machine learning model (DT) followed by an MLP model to effectively identify intrusion points of attack vectors into the grid. Such neural networks when appended with the traditional bad data detection strategy based on the Chi-square test can effectively determine the presence along with the respective locations of attack vector intrusions into the grid. Meter failures along with any unstructured FDIAs can be easily detected by determining the quality of the measurements by the conventional bad data detection technique, whereas the deep learning models can be used as a multilabel classifier for detecting the inconsistency and co-occurrence dependency of the raw measurements owing to FDIA. Such an approach does not need any prior modifications of the conventional bad data detection technique based on the Chi-square test, hence can be easily implemented to identify the presence and locations of FDIA in

the grid, thus showcasing a cost-effective approach.

The primary propositions of this thesis can be summarised as follows:

- With knowledge regarding the parameter and topology configuration of the grid, novel data-driven attack vector formulation schemes have been furnished based on the low-rank subspace of the topology matrix which can inherently bypass the BDD.

- An optimal low-rank subspace is defined using the SVD technique. To reduce the computational burden of FSVD, RSVD is adopted.

- Bilateral random projections based Go-Dec decomposition technique has been undertaken to promote a faster low-rank subspace of the topology matrix in presence of outliers.

- CUR decomposition demonstrates a faster and an effective low-rank structure with the minimal allocation of resources undergoing various noise margins.

- A comprehensive comparison between two different deep learning models followed by a machine learning model like SVM and a statistical forecasting model like ARIMA has been undertaken in this thesis for efficient state forecasting. With an optimal tuning of model hyper-parameters of the developed deep learning structures, a set of minimal error indices have been achieved.

- With the incorporation of noise within the set of acquired measurements, the developed deep learning models demonstrate a robust performance with a minimal variation in the error indices, hence leading to a minimal variation in the attack detection probability.

- The developed anomaly detection algorithms demonstrate superior, real-time, robust FDIA detection schemes.

- A critical comparison between different deep learning architectures along with a traditional machine learning model like DT and an MLP model have been performed to determine the locations of intrusions of FDIA effectively. The developed deep neural network architectures incorporate inherent CNNs which act as multilabel classifiers and can be used effectively to determine the intrusion points of attack.

An effective tuning of hyper-parameters can lead to efficient identification of FDIA under various noise and attack scenarios.

- As the proposed locational FDIA detection policy does not need any substantial modifications of the conventional BDDs, hence it demonstrates a cost-effective approach.

- To enhance model performance along with the extraction of power flow correlation features, the identification strategy of FDIA can be defined as a multilabel classification approach.

- An extensive assessment of the proposed locational detection methodology incorporating variations in parameter sensitivity has been also undertaken. The proposed classifiers are tested on the standard IEEE 118-bus test system showcasing promising results in location and presence detection accuracy. It can be seen that the proposed model is robust with a higher detection accuracy than the other undertaken classifiers.

Furthermore, the key assumptions of this thesis can be furnished as follows:

- A steady state operation of the grid with nearly constant loads is considered and contingency scenarios are kept for future research.

- The attacker with its limited set of resources be it personnel, financial or instrumental can corrupt only a small subset of meters.

- With the minimal set of resources, the attacker is capable of gaining access to the parameter and topological information of the grid.

This thesis primarily demonstrates the effects of FDIAs against the power system state estimators. Protection and control functions that are directly related to the solution of the estimated states may be jeopardised using the proposed attack vector formulation schemes from the control centre like opening the breakers of healthy lines, developing apparent overloading of transmission lines, developing inappropriate control actions etc. It can be seen that most of the literature deals with FDIAs followed by their effects and mitigation strategies when the respective protection devices and the controllers are directly attacked and do not incorporate the solutions of the power system state estimators.

With sufficient offline data for the normal operation of the protection and the control devices, the proposed neural network schemes can be trained effectively. As the trained neural networks have a minimal computational burden, they can be deployed online for the effective detection of such attacks.

1.4 Thesis organization

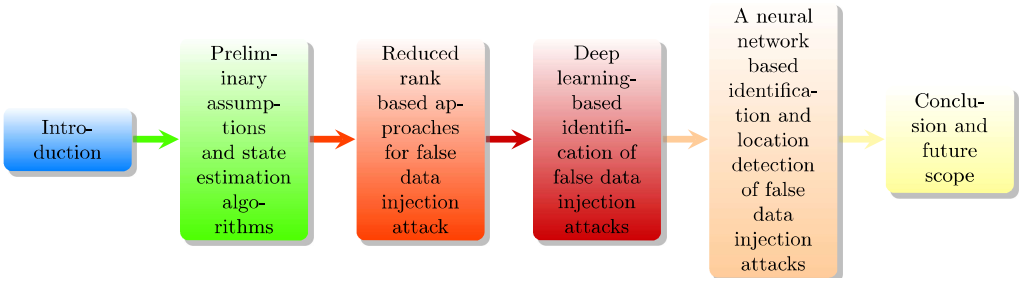

Figure 1.7: Thesis organisation

Primarily, the organization of this thesis can be outlined as follows: chapter II briefly portrays the linear and the nonlinear state estimation strategies along with the modeling of the power grid. Moreover, it also demonstrates the conventional bad data detection strategy based on the chi-square test as adopted by the grid operators along with efficient attack vector formulation schemes that can effectively lead to biased operating states for the linear and the non-linear state estimation algorithms. Chapter III furnishes the stealthy attack vector formulation schemes against the linear state estimation algorithm using the low-rank subspace of the topology matrix using Go-Dec and CUR decomposition which can effectively bypass the conventional χ^2 test-based bad data detection algorithm. With a varying attack strength followed by noise within measurements, the proposed methodologies demonstrate a real-time, robust attack vector formulation. Chapter IV demonstrates an effective state forecasting-based FDIA detection policy incorporating advanced deep neural networks. Anomaly detection schemes undertaking the error between the forecasted and the estimated set of state variables are also developed. Such schemes demonstrate an effective FDIA presence detection policy, but their respective locations of intrusions remain concealed. To overcome this issue, chapter V defines advanced deep learning models working as multilabel classifiers which are capable of detecting not only their presence but also their locations of intrusions effectively. Finally,

Chapter VI denotes the key future works and also furnishes a brief summary of this thesis. An overview of the thesis structure can be seen in Fig. 1.7.