A Thesis

entitled

Exploring False Demand Attacks in Power Grids with High PV Penetration

by

Ashish Neupane

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the

Masters of Science Degree in Electrical Engineering

Dr. Weiqing Sun, Committee Chair

Dr. Ahmad Y. Javaid, Committee Member

Dr. Junghwan Kim, Committee Member

Dr. Scott Molitor, Interim Dean
College of Graduate Studies

The University of Toledo
December 2022

An Abstract of

Exploring False Demand Attacks in Power Grids with High PV Penetration

by

Ashish Neupane

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the Masters of Science Degree in Electrical Engineering

The University of Toledo
December 2022

The push for renewable energy has certainly driven the world towards sustainability. However, the incorporation of clean energy into the electric power grid does not come without challenges. When synchronous generators are replaced by inverter based Photovoltaic (PV) generators, the voltage profile of the grid gets considerably degraded. The effect in voltage profile, added with the unpredictable generation capacity, and lack of good reactive power control eases opportunities for sneaky False Data Injection (FDI) attacks that could go undetected. The challenge is to differentiate these two phenomena.

In this thesis work, an attack is exposed in a grid environment with high PV penetration, and challenges associated with designing a detector that accounts for inefficiencies that comes with it is discussed. The detector is a popular Kalman Filter based anomaly detection engine that tracks deviation from the predicted behavior of the system. Chi-squared fitness test is used to check if the current states are within the normal bounds of operation. The work concludes by exposing a vulnerability in using static and dynamic threshold detectors which are directly affected by day-ahead demand prediction algorithms that have not been fully evolved yet. Finally, some of the widely used machine learning

based anomaly detection algorithms is used to overcome the drawbacks of model-based algorithm.

Acknowledgements

This work was the result of great dedication and hard work, and I would first like to thank my advisor Dr. Weiqing Sun for always believing in me and providing his valuable direction and insights. The work would certainly not be possible without his vast knowledge in security and constructive feedback.

I would also like to thank Dr. Junghwan Kim and Dr. Ahmad Y. Javaid for being part of my advisory committee and provide their valuable time to overlook my research work. The Electrical Engineering and Computer Science department has been continuously supporting me throughout my time here, and I am very appreciative of the department's motivation and encouragement. The work would not have been possible without continuous support from my family and friends, I would like to thank everyone who played their part in this – near and far.

Table of Contents

Abstract iii

Acknowledgements v

Table of Contents vi

List of Tables viii

List of Figures ix

List of Abbreviations x

List of Symbols xii

1 Introduction 1

1.1 Background and Motivation 1

1.2 Thesis Objectives 4

1.3 Organization of the Thesis 5

2 Literature Survey 7

2.1 State Estimation 9

2.1.1 Weighted Least Square Estimation 10

2.1.1.1 Maximum Likelihood Estimation 10

2.1.1.2 Weighted Least Square Estimation Algorithm 13

2.2 Detection Algorithms 14

3 Kalman Filter Based Detector 17

3.1 Kalman Filter Estimator 17

3.1.1 Calculation of State Matrix 20
3.1.2 Calculation of State Transition Matrix(F) 20
3.1.3 Calculation of Q and R 21
3.1.4 Calculation of P 22
3.1.5 Calculation of Measurement Function (H) 23
3.1.6 Calculation of K 24
3.1.7 Chi-squared Detector 24
4 Machine Learning based Detectors 26
5 Simulation and Attack setup 29
5.1 Simulation Setup 29
5.2 The Attack 32
6 Results 34
6.1 Detection using Kalman Filter based Detector 34
6.2 Detection using Machine Learning based Detector 37
6.2.1 Accuracy 38
6.2.2 False Positive Rate 38
6.2.3 Precision 38
7 Conclusion and Future Work 41
References 42

List of Tables

6.1 FDIA Detection Under 0% PV Penetration 39

6.2 FDIA Detection Under 40% PV Penetration 40

6.3 FDIA Detection Under 80% PV Penetration 40

List of Figures

2 – 1 Probability density function of a normal distribution 12

3 – 1 Block diagram of Kalman filter based detector 19

3 – 2 State covariance convergence 22

3 – 3 Conversion from state space to measurement space 23

3 – 4 Kalman gain convergence 24

4 – 1 Process of creation of training and test datasets 27

5 – 1 Power demand over a 24-hour period 30

5 – 2 Voltage levels over a 24-hour period on bus 6 31

5 – 3 Reactive capability curve of PV generator 31

5 – 4 False demand injected by the attacker 33

6 – 1 Output of the Chi-squared detector 35

6 – 2 Error in Net-Demand Prediction 36

List of Abbreviations

AKF.....Adaptive Kalman Filter
AVR.....Automatic Voltage Regulation

BTM.....Behind The Meter

CAISO.....California Independent System Operator
CKF.....Curbature Kalman Filter
CVF.....Cooperative Vulnerability Factor

DER.....Distributed Energy Resource
DR.....Detection Rate

EKF.....Extended Kalman Filter

FDIA .....False Data Injection Attack
FN .....False Negative
FP .....False Positive
FPR .....False Positive Rate

IEEE.....Institute of Electrical and Electronics Engineers
InNoVa.....Inflatable Noise Variances

KCL.....Kirchhoff's Current Law
KVL .....Kirchhoff's Voltage Law

MLE.....Maximum Likelihood Estimation
MS.....Matrix Separation
MVAR.....Megavolt Ampere Reactive

OCSVM .....One Class Support Vector Machine

PMU.....Phasor Measurement Unit
PR.....Precision
PV .....Photo-Voltaic

SCADA.....Supervisory Control and Data Acquisition
SVM.....Support Vector Machine

TN .....Total Negative
TP.....Total Positive

WLS .....Weighted Least Square

List of Symbols

$\mathcal{L}$ .....Log-likelihood function
μ .....Angle of incidence
σ .....Angle of distortion
r_i .....residual r_i of the measurement i
W_{ii}.....WLS problem
$G(x^k)$.....Gain Matrix
x^k.....State Vector

$\bar{x}$ .....State mean
P .....State Covariance
F .....Transition Function
Q.....Process Covariance
Re .....Real component
Im .....Imaginary Component
y.....residual
H.....Measurement Function/Matrix
z.....Measurement Mean
R.....Noise Covariance
K.....Kalman Gain

$E[X]$.....State Covariance
χ_c^2 .....Chi-squared Value
$g(t)$.....Chi-squared Function
P .....State Covariance
P .....State Covariance

Chapter 1

Introduction

1.1 Background and Motivation

Electric power is one of the crucial infrastructures that drives the daily human operation. Ever since its invention, humans have found new and improved ways to use it to make life more convenient and make more technological advancements possible. In order to make electricity more easily accessible and scalable, the electric power infrastructure is organized in three components: generation, transmission and distribution. The generation portion of the electric grid infrastructure is associated with generating electric power. Some of the generation techniques include hydro generation, coal fired generation, nuclear power plants, and more recently wind and solar plants. Traditionally, the power generation plants would generate large amounts of power enough for a big city placed scarcely across the country. However, the demand for more clean power like solar and wind have resulted in the concept of Distributed Energy Resources (DER), which are plants that produce less power usually in a few megawatts are renewable [1]. The transmission section transmits large amounts of power across long distances using

transmission lines and terminates at either industry that requires large amounts of power or at a distribution station that distributes power to the end customers.

The modern electric grid has a complex network of transmission and distribution systems, mostly for redundancy and fault tolerance. Hence, it needs to be managed very efficiently. SCADA systems allows centralized control and monitoring of electric equipment in the grid. The system gathers information from various Phasor Measurement Units (PMU) which helps in calculating electrical parameters to make the entire system observable. Along with that, the control system helps run automatic voltage regulation, frequency regulation and generation controls, which is crucial to keeping the system running in the desired state [2]. The ability to remotely gather information and control the electrical infrastructure helps in efficient management of the grid. However, it also makes the grid vulnerable to attacks. The critical nature of the infrastructure demands more security and resiliency. Everything from traffic lights to medical equipment on hospitals work on electric power, and it is very important for the grid to be 100% available.

The electric power grid has seen a lot of changes in recent years. Traditionally, power system comprised of synchronous generators with high power generation capability and a predictable voltage profile that fluctuated slightly throughout the day. These synchronous generators almost exclusively provided the bulk system voltage regulation. However, that is quickly changing, and with the synchronous fossil fuel and nuclear-powered generators being retired slowly but steadily, it has led to the need for renewable generation to contribute more significantly to the power system voltage and reactive regulation [12].

The synchronous generators reliably produce reactive power by controlling the excitation current through the rotors. Although there is a limit to the magnitude of field current that can be given to rotor windings of a generator to produce reactive power, its production has little effect on the terminal voltage of the generator. That helps the synchronous generators achieve a good voltage profile. On the other hand, due to the limited converter current capacity of PV, its reactive power capacity is usually smaller compared with that of a synchronous generator, especially when PV's real power output is close to the rated value. Inverters used for solar PV and wind plants can provide reactive capability at partial output, but any inverter-based reactive capability operating at full power implies that we need a larger converter to handle full active and reactive current [6]. This means one of two things: the PV generators would have to operate significantly lower than their maximum rated output, or they could operate at maximum rated output with a trade-off in the voltage.

The grid is changing substantially with the introduction of Distributed Energy Resources (DER) and the wide adoption of renewables. And, with these ongoing changes in the grid, the traditional definition of grid stability isn't always applicable. Most of today's infrastructure is internet accessible, and false data injection attacks could give an indication that the voltage levels on buses with PV generators are very low, when in reality the generator could be operating normally. Normally, this wouldn't be a problem, because false data injection attacks are easily detectable in power systems with low PV penetration, because these systems have predictable voltage and current levels. Since the injections would have voltage/current levels that vary significantly from the voltage levels at which synchronous generators operate, a Chi-squared detector would easily pick up these

anomalies [3]. The same detector would also detect the injection attacks at systems with high PV penetration, however the system parameters during normal operation at high PV penetration when PV generators are close to maximum power generation limits, and during attacks at low PV penetration would be indistinguishable to the detector. Hence, it is necessary to develop a model which can efficiently detect attacks during high PV penetration.

This research work aims at showing an attack scenario that takes advantage of poor voltage profile during peak loads at a grid with high PV penetration. A comparison between traditionally used model-based algorithms against the machine learning based algorithms is done under same condition. For model-based algorithm, Kalman Filter based detector is used, which is widely researched in state estimation as well as detection of attacks. However, unlike other research, this model is based on day-ahead demand predictions, which defines the normal operation of the system and ultimately thresholds for the states at any given time of the day. The process model in Kalman filter for power system state estimation realistically should not only have Gaussian error. The states are highly dependent on the demand, especially in grids with high PV penetration, and the model takes that into account to get a better prediction. However, the crucial part of this work is showing how model-based algorithms perform poorly in high PV scenarios with high false positives. For machine learning based detection, four of the widely used anomaly detection algorithms is used.

1.2 Thesis Objectives

The objective of this research work is summarized below:

1. Review the literature related to model-based and data-driven FDIA detectors

2. Develop a Kalman filter model for state estimation of grid state
3. Develop a Chi-squared detector that uses measurement co-variance matrix and reside from Kalman filter model
4. Gather simulation data for load flow analysis under low and high PV penetration
5. Test the performance of Kalman filter and Machine Learning based detectors under attacks in different levels of PV penetration.

1.3 Organization of the Thesis

Chapter 1 – Introduction

The first chapter gives a brief introduction to the electric grid infrastructure, highlighting the importance of security. It explains how the advancement in grid is making it vulnerable to attacks, and various detection techniques that have been developed to prevent it.

Chapter 2 – Literature Review

This chapter discusses various approaches to detecting False Data Injection Attacks. Both traditional model-based and the new data-driven approach has been discussed.

Chapter 3 – Kalman Filter Estimator

Kalman filter-based state estimator has been presented in this chapter. Along with presenting the theoretical basis of a Kalman filter model, the chapter discusses how this model is used to estimate grid state like voltage. The chapter also shows the use of Chi-squared detector in conjunction with the Kalman filter model to detect FDIA. A crucial

portion in the chapter is how the state residual and measurement covariance are propagated to Chi-squared detector to get a real time detection.

Chapter 4 – Attack Model

The chapter gives an insight into the attack model used in the research work as well as explain the attack scenario in during low and high PV penetration. The ability of the attack to obfuscate as a diminishing performance during high PV penetration is also discussed.

Chapter 5 – Machine Learning Based Anomaly Detector

The implementation of four of the most widely used Machine Learning algorithms in anomaly detection is presented in the chapter. A detailed explanation of training and testing models has also been explained.

Chapter 6 – Results

The result of the data-driven model is compared with the model-based detection in both low PV and high PV penetration. Accuracy and false positives two of the main focus of the results section.

Chapter 7 – Conclusion and Future Work

Finally, this chapter makes some concluding remarks on the research work, as well as suggests some modifications which could give new direction for continuing this research work.

Chapter 2

Literature Survey

Power systems employ state estimation techniques for synchronizing its generation, transmission and distribution operation [2]. The technique models the states of the system using process covariance, which represents the change in states with respect to time using statistical covariance, and measurement co-variance which depicts the change in measurement. It is crucial that the state and measurement covariances are correctly modelled, because an incorrect value will give a false representation of the system. State estimation allows 100% observability of the system using direct measurements and pseudo measurements. Pseudo measurements are measurements which are calculated using mathematical relations if enough parameters about bus and line are known [4].

A wide variety of state estimation techniques have been developed throughout the years. The most notable is Weighted Least Square method, which uses weights to show belief in a particular state. Although WLS method is widely used, it has a drawback of being iterative in nature [2]. This makes it very slow, and researchers are looking for fast and non-iterative way of state estimation in recent times where the grid has not only gotten more complicated, but also very unpredictable with the introduction of more renewable energy sources.

Kalman filter has recently got more attention in state estimation because of its success in modelling systems with large amounts of errors. It is however not without its drawbacks. Although it is fast and non-iterative, it has strict requirements on the nature of the states it tries to model. More specifically, the states should follow a normal distribution in order to be correctly modelled using a Kalman filter [5]. A lot of the research in Kalman filter based state estimation has been done without explaining the intricacies of the scope of normal distribution and boundary conditions where the estimation is relevant.

The detection algorithms use state estimation to get the required information and draw a conclusion regarding the validity and integrity of the data. The main challenge associated with these algorithms is deciding on a threshold which ideally differentiates legit states with falsely injected states. If the threshold is too high, the detector will likely not detect all attacks resulting in too many false negatives, and if it is too low, the detector will have a high false positive. Getting the right amount of balance is the key.

On the detection side, Kalman filter is usually paired with a Chi-squared detector, or a Euclidean detector to detect FDIA. This set up works perfectly on traditional grid which is very predictable, and the behavior of the grid is very stable. However, modern grid increasingly uses renewable energy like solar and wind, the output of which is very unpredictable. More recently, BTM PV supply resources residing in customer end has added more uncertainty on energy generation and demand [6]. Hence, it has become very difficult to model the behavior of the grid to account for new changes. Hence, Machine Learning algorithms have been widely explored in both state estimation and FDIA detection.

The scope of the research work is very specific. The work shows drawbacks associated with model-based algorithms in a very high PV penetration environment where, at peak demands, the grid shows behavior which mimics an attack. The grid supposedly needs to know the context to a wide number of variables to predict accurately in such scenario.

2.1 State Estimation

State estimation in power system was first recognized by Fred Schweppe [13, 14, 15]. Since its introduction, state estimation has widened the capabilities of the SCADA systems. State estimation has 5 main functions [2], which is explained below:

1. Topology processor: The topology processor helps gather information about the interconnection between components of grid infrastructure. The grid changes its topology every so often due to faults, or economic constraints and topology processor receives current status of switches and circuit breakers to build the one-line diagram of the system.
2. Observability analysis: The system or portion of it is observable if all the parameters of it are known directly or can be calculated using mathematical relations. Observability analysis determines if all bus voltages and line currents of the grid can be calculated using the given PMU measurements. It also checks if the system has any unobservable branches.
3. State estimation solution: The solution provides optimal estimate for the system state based on the given measurements and the estimation model. The solution includes l2ine flows, loads, transformer taps and power injections.

4. Bad data processing: The parameters measured on the grid can be altered by a faulty device, or its integrity can be violated in transit. Such data can heavily impact the performance of state estimation. Hence, it is necessary to eliminate such data and correct it using redundant measurements.
5. Parameter and structural error processing: Estimations are done on various parameters like transmission line model parameters, and shunt capacitor or reactor parameters. The main function is to detect errors in network configuration provided enough redundancy exists in the system.

2.1.1 Weighted Least Square Estimation

2.1.1.1 Maximum Likelihood Estimation

The main objective of state estimation is to calculate the most likely state of the system among all the possible states by using the measured parameters. One of the most popular technique to determine the likelihood of a given state is the maximum likelihood estimation (MLE) [7]. The measurement errors on various measured parameters on the grid are very predictable, and hence a joint probability density function can be drawn in terms of unknown parameters. This is called the likelihood function which has a peak value when the unknown parameters are close to the actual values. The MLE method can be used to solve an optimization problem which can be used to provide the maximum likelihood estimates of the unknown parameters.

The measurement errors on the measurement units or PMUs are supposed to follow a normal distribution. This is also commonly known as a bell curve, which is shaped like a bell. Two of the important parameters of the distribution are mean μ and standard

deviation σ, which defines the shape of the curve. Any random variable has a high probability of being close to the mean, and the probability of a random variable tapers away as it goes further away from the mean [2]. For a random variable *z*, the normal probability density function (pdf) is defined as:

$$f(z) = \frac{1}{\sqrt{2\pi}\sigma} e^{-1/2\{\frac{z-\mu}{\sigma}\}^2} \tag{2.1}$$

where,

μ = expected value of z = E(z)

σ = standard deviation of z

After standardization, the function becomes,

$$\phi(u) = \frac{1}{\sqrt{2\pi}} e^{u^2/2} \tag{2.2}$$

where,

$$u = \frac{z-\mu}{\sigma}$$

The plot of ϕ(u) is shown in fig 2-1.

The next step in the process is calculating the likelihood function. The probability of measuring *m* independent variables or measurements is represented by a joint distribution function, which is the product of probability distribution function of each individual measurements. It is given by:

$$f_m(z) = f(z_1)f(z_2)\ldots f(z_m) \tag{2.3}$$

where, z_i = i^{th} measurement

This function is the likelihood function for random variable *z*. The aim of the MLE is to maximize this function by varying its mean μ and standard deviation σ. The calculations

can by simplified by replacing the function in terms of its logarithm. The resulting function is called the Log-likelihood function given by:

$$\mathcal{L} = logf_m(z) = \sum_{i=1}^{m} logf(z_i)$$

$$= -\frac{1}{2}\sum_{i=1}^{m}\left(\frac{z_i-\mu_i}{\sigma_i}\right)^2 - \frac{m}{2}\, log2\pi - \sum_{i=1}^{m} log\,\sigma_i \qquad (2.4)$$

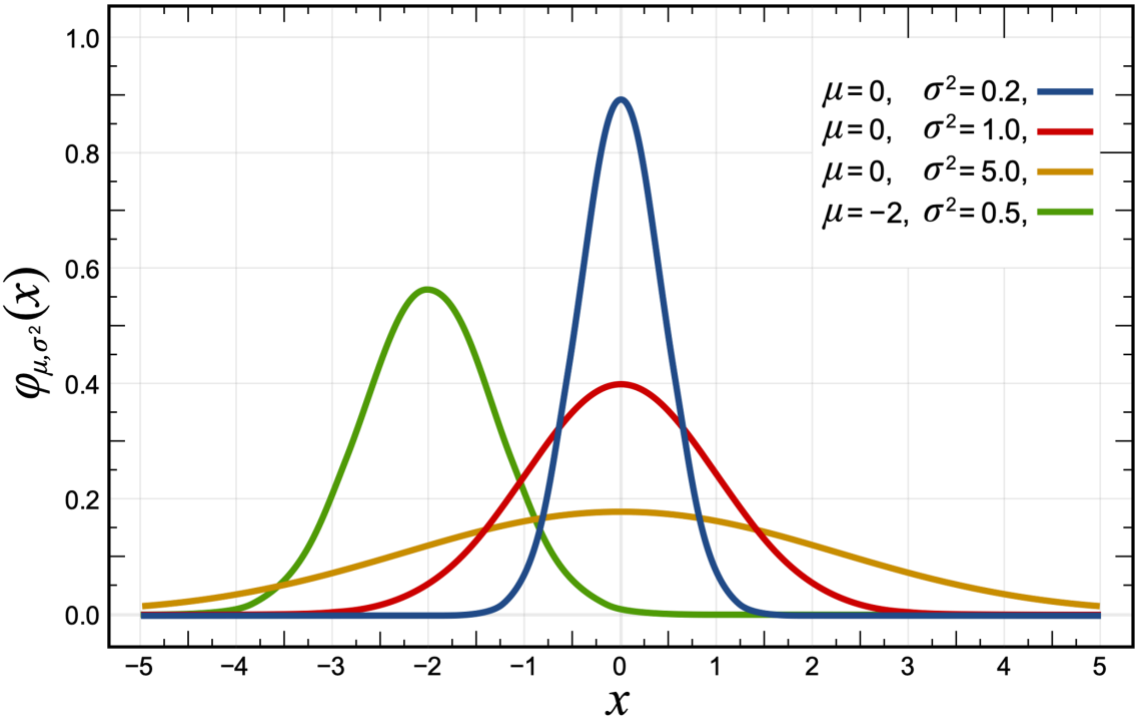

Fig 2-1: Probability density function of a normal distribution

The solution to maximizing the likelihood can be obtained in two ways:

1. maximize $logf_m(z)$
2. minimize $\sum_{i=1}^{m}\left(\frac{z_i-\mu_i}{\sigma_i}\right)^2$

The residual r_i of the measurement i is defined as:

$$r_i = z_i - \mu_i = z_i - E(z_i) \qquad (2.5)$$

A new function called $h_i(x)$ is introduced which is non-linear in nature and relates the states of the system to the measurements. The standard deviation of the measurement variables not only shows how the variables are distributed, but also helps achieve a set level of confidence in predicting its likely value. Hence, the WLS problem is introduced by placing a weight $W_{ii} = \sigma_i^{-2}$. This expression puts more weight on measurements that can be trusted, or in other words, measurements which have less standard deviation. Finally, the minimization problem becomes,

Minimize:

$$\sum_{i=1}^{m} W_{ii} r_i^2 \tag{2.6}$$

Given:

$$z_i = h_i(x) + r_i \text{ , i = 1, 2 . . , m}$$

The Weighted Least Square (WLS) estimator for x is the solution to the optimization problem above.

2.1.1.2 Weighted Least Square Estimation Algorithm

The precursor to WLS estimation has been explained in the previous section. The WLS estimation is not just a single step but a series of steps which has to be followed precariously to obtain effective results. The algorithm for WLS estimation is given in following steps [2].

1. Set the iteration index k = 0
2. Do a flat start initialization of the state vector x^k
3. Compute gain matrix $G(x^k)$
4. Calculate R.H.S of $t^k = H(x^k)^T R^{-1}(z - h(x^k))$
5. Decompose $G(x^k)$ and solve Δx^k

6. Test if the solution converges, max $| \Delta x^k | \leq \varepsilon$?
7. If the solution converges, stop. If not, update $x^{k+1} = x^k + \Delta x^k$, $k = k + 1$

2.2 Detection Algorithms

Detection methods for False Data Injection Attacks have been researched for a few decades. These algorithms are broadly categorized as model-based detection algorithms and data-driven detection algorithms [11]. Weighted Least Squares (WLS) were realized in [16, 17, 18, 19]. These first detectors were static and iterative in nature, which did not use the last state to update the new state. That made them slow and processor intensive. Kalman filters and some of its variations were used in [20, 21]. In [22, 23] specifically, Extended Kalman Filters were used which was able to address non-linearity in the system and yielded more precise estimate. Unlike WLS, these detectors are dynamic in nature and use the last state to update the current state.

Some detection algorithms are however estimation-free. Cooperative Vulnerability Factor (CVF) employs secondary output of voltage controllers that converges to zero if the system is under the FDI attack (FDIA) [24]. This technique was used in microgrids environment. Another technique called Matrix Separation (MS) exploits the sparse nature of FDIA by separating nominal states of power grid and anomaly matrices [25, 26]. Some similar techniques are presented in [27, 28]. Data-driven detection algorithms are popular class of algorithms broadly classified as Machine Learning, Data Mining and other miscellaneous algorithms. Supervised learning technique use datasets that have labelled data to separate attacks from the normal flow. They have high accuracy but cannot detect new variation of attacks. Unsupervised learning does not need labelled data but is extremely difficult to model. Support Vector Machine (SVM), which is a type of

supervised learning is the most utilized in FDIA. These have been presented in [29, 30, 31]. In the unsupervised category, K-means clustering is very popular and have been researched in [32, 33].

A wide variety of Kalman Filter has been used in the detection of False Data Injection Attacks. One of the challenges faced in the research is modelling non-linear relationship of power and voltages in the grid. In [34], the authors presented dynamic state estimation that does not require calculation of Jacobian matrix, which decreases the processing time. Similarly, Qi et.al [35] introduced Cubature Kalman Filter (CKF) that has a non-linear observer. These were then tested on a 68-bus system under various uncertainties in a realistic scenario. The authors showed that the model was comparatively more robust to uncertainties in the systems including cyber-attacks.

A risk mitigation strategy was presented in [36] that addresses dynamics in the system for higher order depictions by utilizing a dynamic state estimator. The estimator is followed by a detection algorithm that checks for unknown inputs. [37] proposed a unique approach to dynamic state estimation. The algorithm employs a fully distributed approach where the estimation has an innovation design element for attack detection which reduces the overhead in communication. [38] designed an Adaptive Kalman Filter with Inflatable Noise Variances (AKF with InNoVa) algorithm that uses a 2-stage system that estimates static states like voltage magnitudes as well as dynamic states like generator rotor angles. The first stage of the system filters out the impact of incorrect system modelling and bad PMU measurements using AKF with InNoVa. The result in the first stage is served as a measurement to the second stage which has an Extended Kalman Filter (EKF). Kebina et. al. [39] used Chi-squared detector to detect anomalies in the system. The residuals from

Kalman filter were fed to a Euclidean detector which has the parameters for normal level of the system and detects if there is any deviation from the normal operation.

Chapter 3

Kalman Filter Based Detector

3.1 Kalman Filter Estimator

The Kalman Filter has been extensively used in various applications in mathematics, engineering and economics. The filter is robust and provides good estimation of systems. At its core, Kalman filter balances the prediction of states and measurements of the states. Based on which of the two has higher beliefs, process or measurements, the filter calculates its estimation [5]. It assumes that the measurement error variance and process covariance is already known.

The prediction equation is given below.

$$\bar{x} = Fx + Bu \tag{3.1}$$

$$\bar{P} = FPF^T + Q \tag{3.2}$$

where,

x and P are the state mean and covariance

F is the state transition function

Q is the process co-variance

B and u are the control inputs which is 0 here

The first equation calculates the current state based on the last state and the state transition matrix. The states in the equation are vectors of real and imaginary currents and voltages given by equation (3) [8].

$$\begin{bmatrix} Re(z) \\ Im(z) \end{bmatrix} = \begin{bmatrix} Re(H) & -Im(H) \\ Im(H) & Re(H) \end{bmatrix} \begin{bmatrix} Re(x) \\ Im(x) \end{bmatrix} + \begin{bmatrix} Re(v) \\ Im(v) \end{bmatrix} \tag{3.3}$$

Unlike most of the research, where state transition matrix is taken as identity matrix because it is assumed that the next state is the mean of the stable state and some process error, this research uses pre-computed factors obtained from the demand forecast computer. The prediction step always lessens the belief that the estimator has towards the system. In other words, instead of having high probability in a small range of states, the estimates get dispersed to a slightly wider range of values with lesser probabilities. That is corrected by the update state. The measurement equation is given below.

$$y = z - Hx \tag{3.4}$$

$$K = PH^T \left(HPH^T + R\right)^1 \tag{3.5}$$

$$x = \bar{x} + Ky \tag{3.6}$$

$$P = (I - KH)P \tag{3.7}$$

where,

y is the residual

H is the measurement function/matrix

z and R are the measurement mean and noise covariance

P and K are the state covariance and Kalman gain

The residual y is the difference between measured values and predicted measurements which have been derived from the predicted states using H. The variables K

and *P* converges to some stable values. The measurement matrix converts the states from the state space to its corresponding measurements in the measurements space. The calculation of *H* matrix has been explained in [40]. The conversion of states to the measurement space however also changes the covariance. Hence, it needs to be recalculated in each iteration which is given by the relation in equation (7). It should also be noted that although the Kalman gain remains fairly stable after getting converged, the value should also be calculated in each state for a more accurate prediction and to avoid propagation of error.

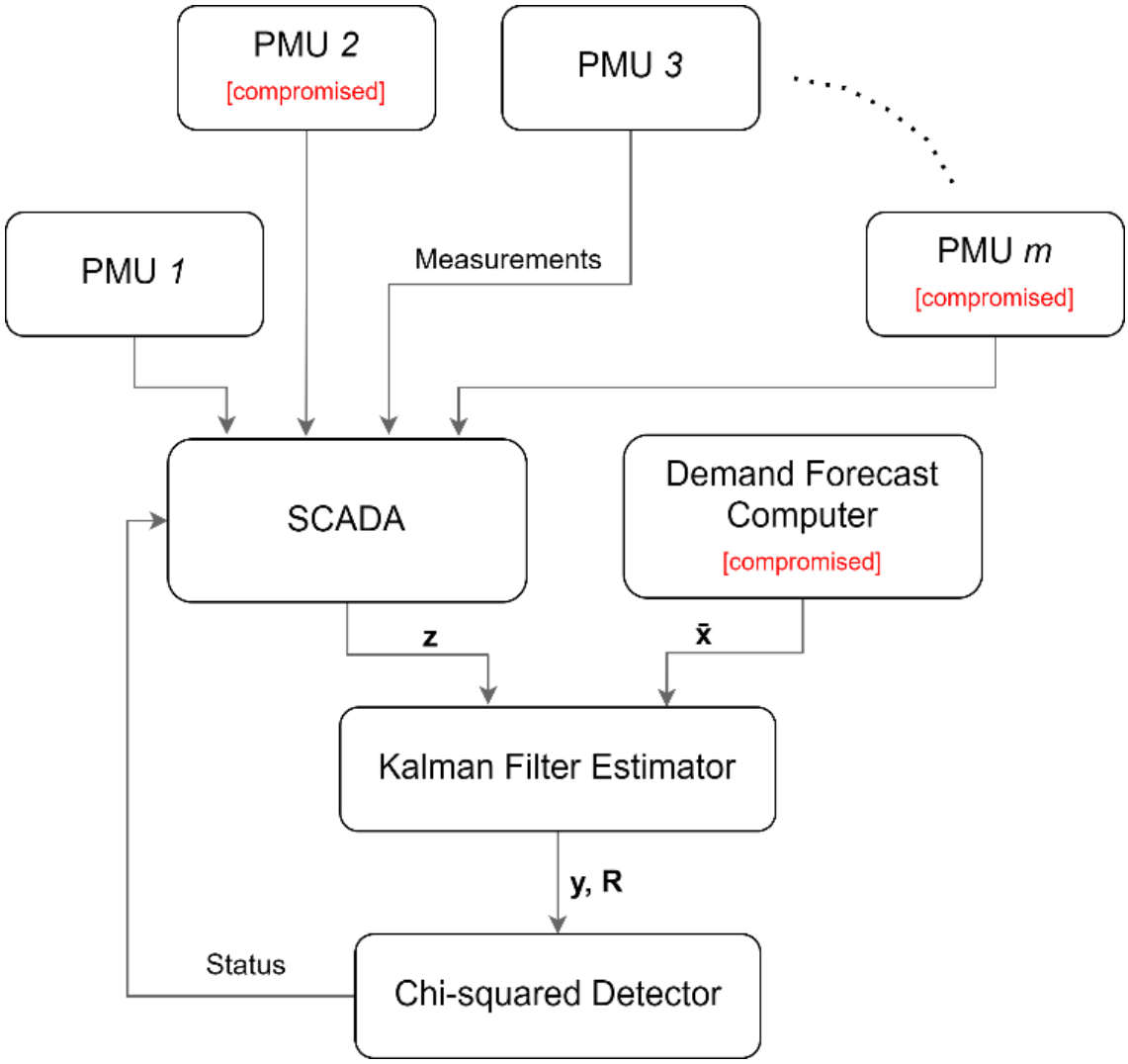

Fig 3-1: Block diagram of Kalman filter based detector

3.1.1 Calculation of State Matrix

The states in Kalman filter are the parameters whose estimations are done by balancing the value between its measured and predicted versions. The states in this work are all the real and imaginary voltages in a 14-bus setup. The following expression shows the states of the setup.

$$x = [Re(V1) \quad Re(V2) \ldots Im(V1) \quad Im(V2) \ldots Im(V14)]^T$$

There are *n* states in the system. Hence, the size of x is *nx1*. When the simulation starts, the states have to be initially set to a certain stating condition. Usually, the rule of thumb is to start the states with a flat start condition. The states are initialized by setting all the real voltages to 1 and all the imaginary voltages to 0. However, the states of the grid are tentatively known and hence, the grid configuration is pre-simulated to get the stable values of the states, which results in faster convergence.

But because all the states are not directly measured,

3.1.2 Calculation of State Transition Matrix (F)

The state transition matrix defines the transition of states from current state to next state [5]. The grid is a very dynamic infrastructure, and hence it is extremely difficult to accurately predict the next state of the system based on the current state. However, in this case, because the states are voltages, the Automatic Voltage Regulation (AVR) system always tries to stabilize the voltage between ±5% of the nominal voltage of 1 P.U, and hence, it is easier to compute the state transition matrix.

This research work uses a different approach in calculating F based on the real-world scenario. Unlike other research where states are modelled to vary randomly between certain ranges, the work takes into account that the grid has a dynamic active and reactive power demand that varies throughout the day, and it affects the states of the system based on whether majority of its power comes from synchronous generators or PV generators. The day-ahead demands throughout the day is download from California Independent System Operator (CAISO) [9], simulated on an IEEE 14 bus configuration and the matrix F is calculated for each time step. However, the research work would be of no use if F was made to be 100% accurate. Instead of using hour-ahead demands for F, day-ahead demands

are used. And because day-ahead demands are slightly inaccurate than hour-ahead demands, there is a need for accurately predicting the next state by using measurements. For instance, the next state from the current state is calculated as follows:

$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

$$\bar{x} = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

State transition matrix is a *nxn* matrix. Here, the second equation predicts the next state using F. The state x_1 changes by a factor of A and x_2 changes by a factor of B. It is assumed that the states transition only depend the state itself and not on other states, the off-diagonal elements of F are 0. However, in a grid, the states do depend on the values of other states which has to be taken into account. That is done by incorporating state co-variance P and process covariance Q.

3.1.3 Calculation of Q and R

As discussed earlier, the state transition matrix takes time-dependent state transitions into account which is part of the process. Kalman filter also has *B* and *u* that considers any known external forces or variables, which is ignored in this work. However, the possibility of any unknown variables changing the predictions is huge. The filter should be designed in a way that expects some unaccounted variables and models uncertainty using it as a variable in the equation. The process covariance Q helps the filter account for those uncertainties.

The modelling of Q matrix is very crucial and one of the most difficult tasks of a Kalman filter and it is important to model Q accurately. If Q is too low, the filter will have more confidence in the prediction model and ignore noises in the system. If it is too high, the filter becomes inaccurate because its prediction will be largely influenced by the noise [5]. While there are various approaches to calculating Q, the appropriate Q matrix was obtained in this work by simulating the IEEE bus under various load conditions and evaluating the errors obtained in the simulation. When following this method, the simulation should be iterated numerous times to account for various load conditions and uncertainties in the grid.

The measurement covariance R represents the predicted observation errors. This is sometimes referred as sensor noise and can be estimated easily by comparing the expected results with the sensor measurements [5].

3.1.4 Calculation of P

The state covariance matrix P shows the relation between all the system states. Mathematically, it is a measure of joint probability of two random variables. The covariance is defined as:

$$\text{cov}(X, Y)=E[(X-E[X])(Y-E[Y])] \tag{3.8}$$

where, E[X] is the expected value of random variable X.

A positive value of covariance between two variables, or state in this case shows a direct relation between those state and a negative value indicates inverse relationship. The matrix P is initialized in a similar way to the states. It doesn't have a strict requirement like Q because P is optimized in each time step of Kalman filter equations, and ultimately converges to a stable value [5]. The state covariance matrix P is a symmetric matrix of size *nxn* where the element P_{ij} shows the relationship between states *i* and *j*. The following graph shows how the covariance converges in less than 200 iterations.

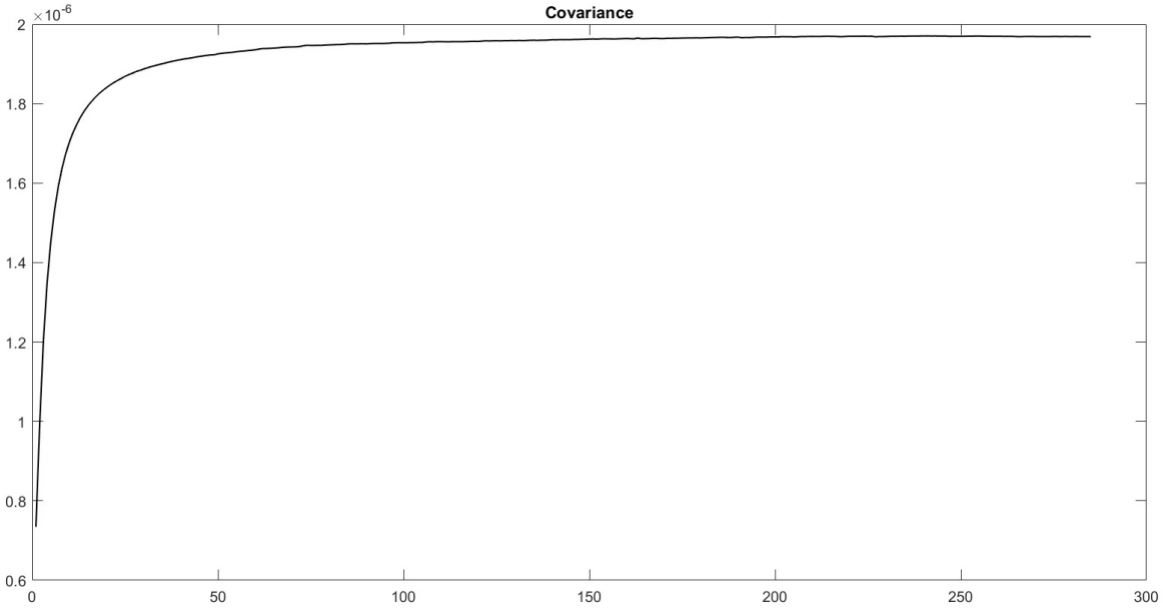

Fig 3-2: State covariance convergence

3.1.5 Calculation of measurement function H

The Kalman filter equations have *n* states and *m* measurements. The measurements done on the system can be different from the states. Therefore, in order to get a residual value between the predicted states and measurement, all the states have to be converted to the measurement space to make mathematics compatible to the same operands. The following figure illustrates this concept where the data points on the state space are converted to datapoints in measurement space using the measurement function *H* [5].

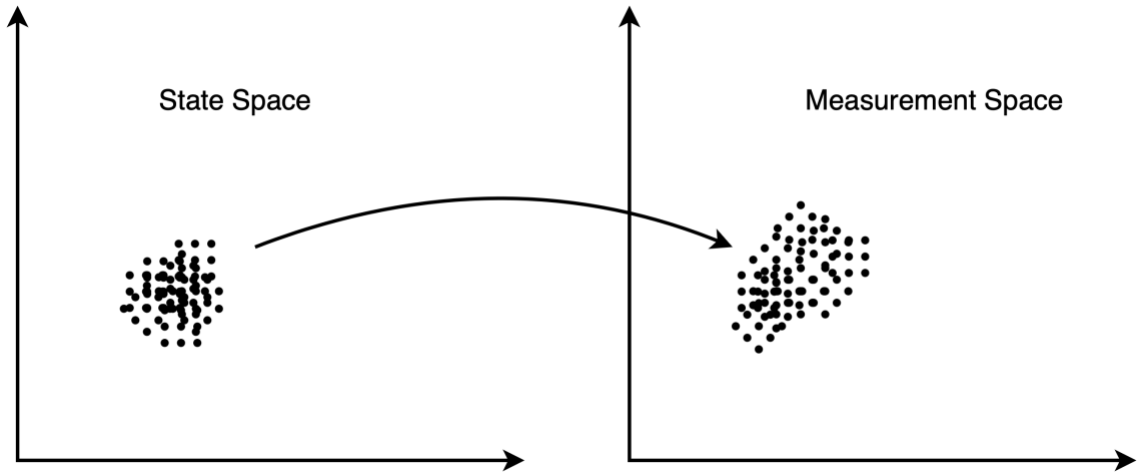

Fig 3-3: Conversion from state space to measurement space

$$y = z - Hx$$

$$y = \begin{bmatrix} V_1 \\ V_5 \\ V_8 \end{bmatrix} - H \begin{bmatrix} V_1 \\ V_2 \\ V_3 \end{bmatrix}$$

In order to convert states *x* to its measurement counterparts *z*, the *mxn* matrix *H* should be chosen such that the resulting operation *H.x* gets converted to measurements with elements V_1, V_5 and V_8. Hence, it is necessary to first come up with a relationship between different voltages. Consider for example, the network is configured such that the following relationship holds true:

$$V_5 = V_2 + V_3$$

$$V_8 = V_1 - V_2$$

Then, the H matrix is chosen such that *Hx* results in $[V_1\ V_5\ V_8]^T$. The final H matrix for this example is given below:

$$H=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 1 & -1 & 0\end{bmatrix}$$

3.1.6 Calculation of K

The Kalman gain is the most crucial parameter of any Kalman filter. The Kalman gain decides whether the estimation should lean towards predicted values or measured values based on which value the filter has higher confidence in [5]. In matrix form, the Kalman gain is a *nxm* matrix which sums each product between Kalman gains and measurements for a particular state. Like state covariance, Kalman gain also converges to a stable value after a few iterations. One of the Kalman gains used in this work has been graphed in the figure below.

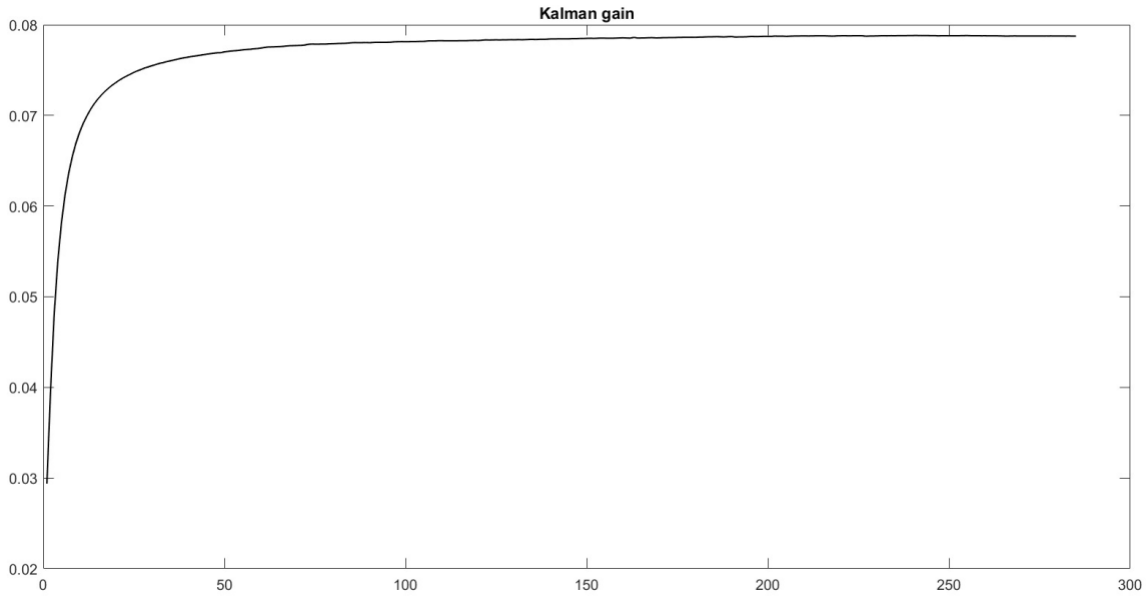

Fig 3-4: Kalman gain convergence

3.1.7 Chi-squared Detector

Kalman filter is very efficient is filtering out errors and providing true estimate of the system. However, it cannot be used to give an indication of deviation of states from normal operation. In order to do that, the Kalman filter is used in conjunction with a Chi-squared detector in this research. The mathematical expression for chi-squared test is given below [11].

$$\chi_c^2 = \sum \frac{(O_i - E_i)^2}{E_i} \tag{3.9}$$

The Chi-squared detector is widely used for goodness of fit tests. That makes it practical for use in detecting false data injections where the normal states of the system can be plugged in, and with the knowledge of co-variance in the states, the Chi-squared values can be obtained. The expression above is not suitable for working with matrices and large number of states and measurements. Hence, as shown in [41], the following expression can be used for computing chi-squared value using the residual *y* and measurement co-variance *R*.

$$g(t) = y^{-1}Ry \tag{3.10}$$

The measurement covariance matrix R is crucial in the above equation. If the residual deviates from expected values, the Chi-squared value goes higher, indicating an inconsistency between the expected and real value. Chi-squared detector is a hypothesis test that uses a table based on degrees of freedom and level of confidence to build a threshold. This research work uses 95% confidence level, which translates to $\alpha = 0.05$. The measurement covariance R gives an indication of normal operation, and if the residual, which is the difference between measured and predicted value, is high, then the chi-squared value increases past the threshold indicating a deviation from normal operation has occurred. The two suspected causes of this inconsistency are false data injection attacks, and a switch from synchronous generators to PV generators, which has a poor voltage profile. The challenge, and the main focus of research is to differentiate the two.

Chapter 4

Machine Learning based Detectors

The electric is composed of complex network of electric infrastructure that spans from generation stations to transmission and distribution stations. While model-based algorithms can perform efficiently under ideal conditions when all the measurements are received timely and topological information about the network is known. However, the grid is unpredictable in nature because of occasional faults and equipment failures. It has become even more complicated in recent years with the introduction of Distributed Energy Resources (DER). The load flow analysis and state estimation become quickly overwhelmed if there are too many variables, and its performance is impacted when the entire system is not observable.

On traditional electric grid, the parameters like voltages, currents and power injection would be relatively stable because synchronous generators are efficiently in handling reactive power demand. However, with the introduction of DERs in the grid, the PV based generators and inverters have limited reactive generation capability [6]. Due to this, the voltage gets fluctuated, and the grid states become unpredictable. Moreover, the renewable generation is unpredictable in nature with generations fluctuating throughout the day as well as the Behind the Meter (BTM) generation equipment adds more

uncertainly on whether the customers would be adding power to the grid or drawing from it. It has also been recently shown in [6] that the high PV penetration negatively impacts the grid if the generators reach close to their reactive generation limit. Due to these various reasons, the number of variables affecting the state of the grid like voltage, currents and power injections have increased significantly. Modelling all those variables like power demands and BTM generation mathematically is extremely difficult. Hence, detecting anomalies from the normal operation of the grid accurately using model-based algorithms is very difficult, and if all the variables are not accounted for, it will produce large errors.

Machine learning algorithms have been explored extensively in the detection of false data injection attacks [12]. The idea is to first train the model with normal operation of the system under varying conditions of PV penetration and load demand. This training approach helps the ML model to help define normal operation under varying load conditions and different percentages of PV penetration. An attack scenario is generated by modifying the measurements during lower PV penetration and normal demand by replacing the measurements with measurements generated during high PV penetration and high demand. The block diagram for the training and test dataset is shown below.

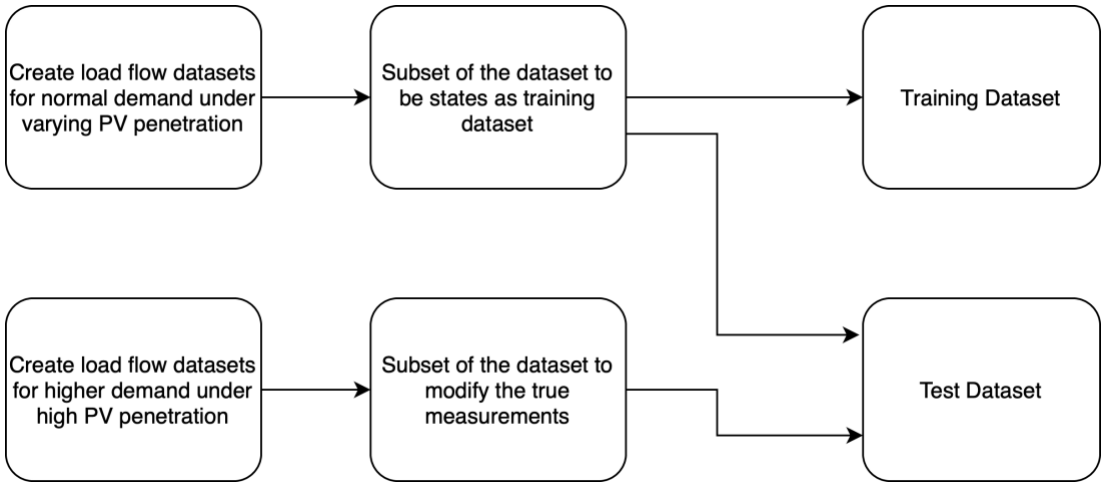

Fig 4-1: Process of creation of training and test datasets

The works uses 4 ML algorithms for anomaly detection which includes

1. Isolation forest
2. Local Outlier Factor
3. One-class Support Vector Machine (OCSVM)
4. Mahalanobis Distance

Chapter 5

Simulation and Attack Setup

5.1 Simulation setup

The research work consists of IEEE 14 bus with the standard load profile. A 24-hour demand curve is extracted from CAISO's website as shown in Fig. 3 that drives the real and reactive power demands on each bus. The load flow is solved for each demand, and the corresponding states are obtained.

In this setup, an IEEE 14 bus is simulated using Power World Simulator. The simulator runs 24-hour load demands and calculates the corresponding states and measurements. The load demand is obtained from CAISO every 5 minutes totaling 289 demand points. These data points are interpolated to obtain 5,000 data points which is imported into MATLAB where Kalman filter predicts and estimates the real and imaginary voltages on each bus. The per-unit real voltage on bus 6 during a 24-hour period is shown in Fig. 4.

The load flow is solved using the MATPOWER package. The Newton's method is used to solve non-linear load flow equations. The Kalman filter estimator gets measurement data from the load flow solution and makes estimates using the day-ahead predictions and measurements.

The reactive power generation in any power system is restricted by the reactive capability curve. The general idea behind reactive capability curve is that, for any given amount of active power generation, there is a limit on the amount of reactive power that can be generated. The limit is determined by the capability curve. Fig. 5 shows the

operating area of the PV inverters which are highly restricted by the power factor requirements and internal limits. The reactive power generation is limited in PV inverters, and although they can have D-shaped curve, this is not an industrial standard [12].

There is a special STATCOM mode which allows the PV inverters to generate reactive power without producing any active power and use that for voltage regulation. However, this mode is not always available due to restrictions. The reactive capability curve of the operating range was inserted into the Power World Simulator using a piecewise linear model. The PV control model, while being a crucial part of the system, has limited scope in this research and its intricacies are almost independent on how the attacks are carried out. Hence, it is excluded.

The simulation setup for machine learning based detector is highly rigorous because unlike model-based algorithms where the states would be calculated using an equation, machine learning algorithms rely on pre-simulation of all the load flow condition that the model may encounter in real-life.

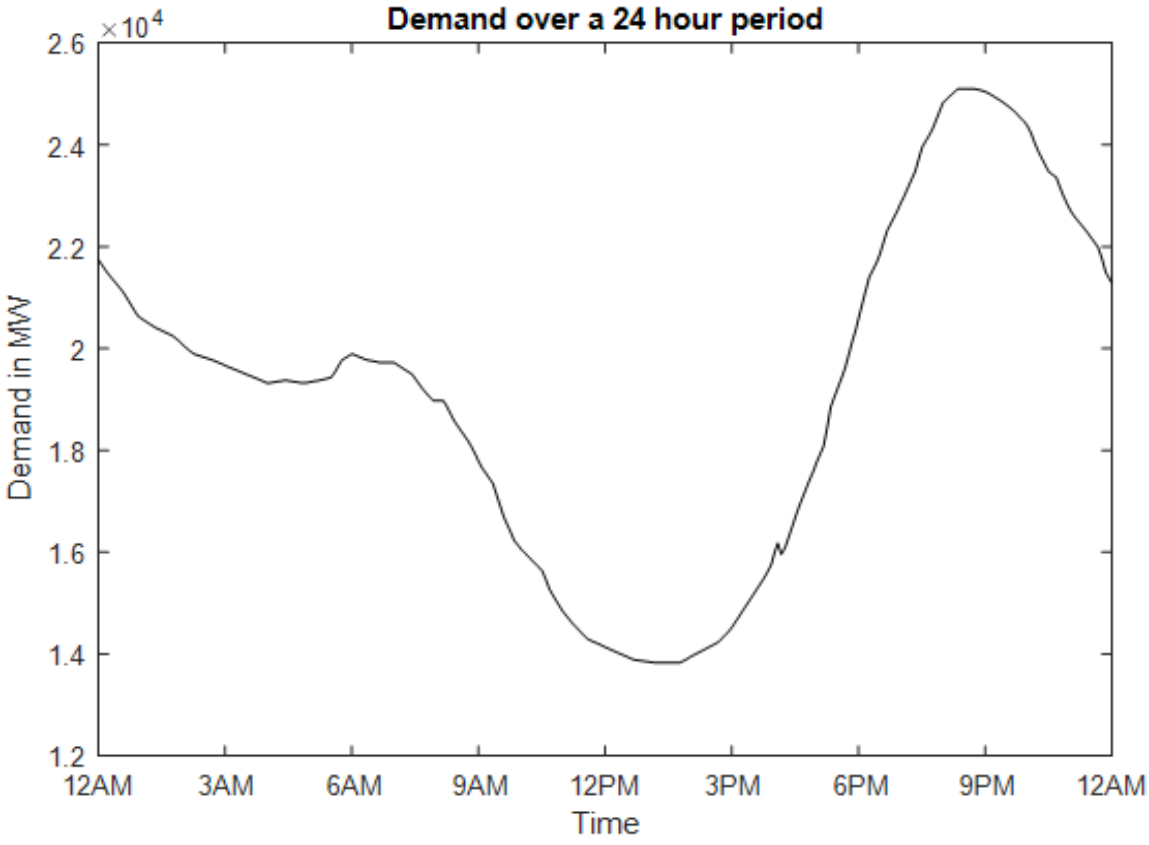

Fig 5-1: Power demand over a 24 hour period

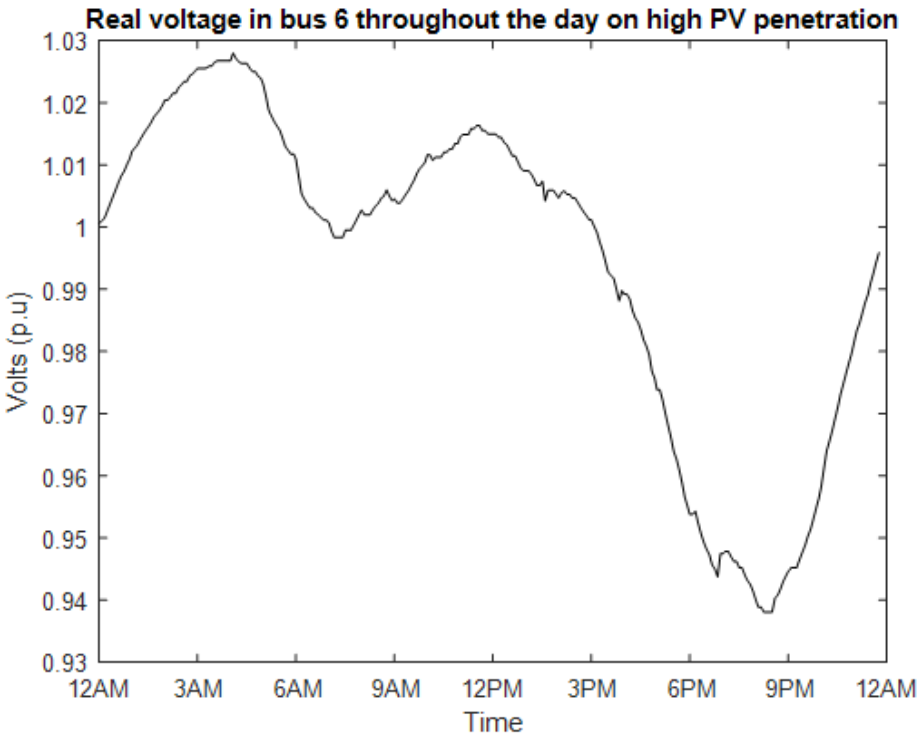

Fig 5-2: Voltage levels over a 24-hour period on bus 6

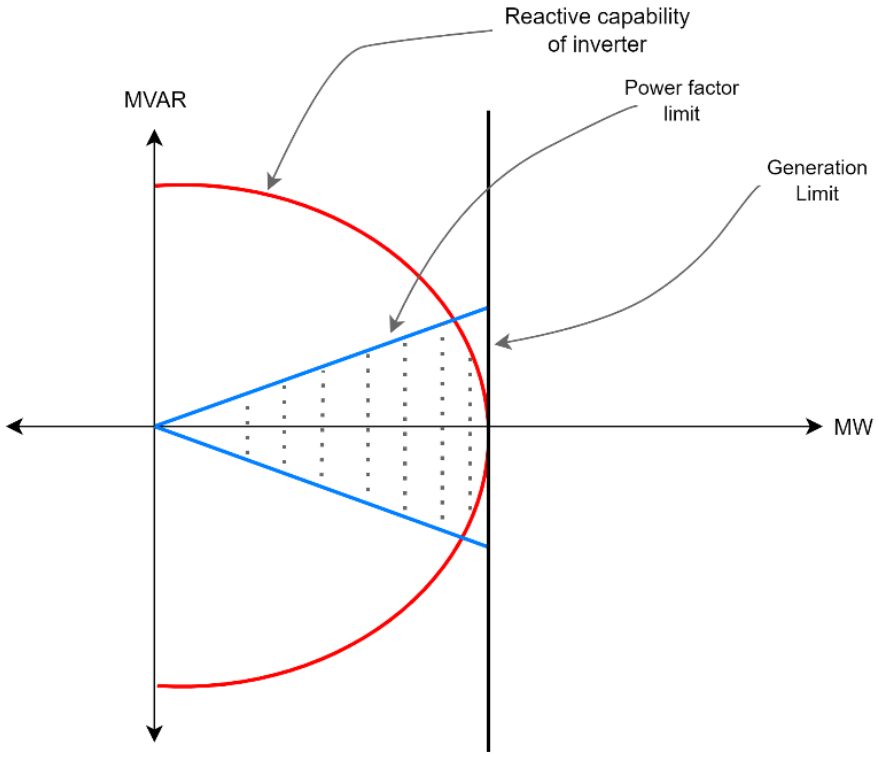

Fig 5-3: Reactive capability curve of PV generator

5.2 The Attack

The false data injection attack is carried out by changing the measurements on a PMU unit. This research work assumes that the attacker has access to a limited number of PMUs in the grid and is able to manipulate bus voltages and line current measurements on that PMU. As mentioned in [42], any unsophisticated attack can be easily detected using plausibility tests. Some red flags include voltage magnitudes that are negative or considerably higher or lower than the operating range of the bus, failed KVL and KCL tests and power equations.

Any sophisticated attack would easily pass those tests. Hence, a difficult-to-detect attack is exposed, which makes the detection extremely hard. The attack impersonates a drop in voltage due to poor reactive performance that results in a less ideal voltage profile of PV generators. This attack is specifically targeted at a system that has higher PV penetration. The research in [6] shows how the increase in penetration of PV generators results in a poor voltage performance.

In this attack, the attacker can get the bad voltage profile measurements and inject it during the time when the grid is performing normally. The detector will have difficulty in differentiating if the anomaly is caused by an attack or the high PV penetration. The challenge with this kind of attacks is that there should be no visible transition between a normal operation and the attack. A sudden drop in voltage, or a sudden loss in a portion of the grid is a major red flag that will draw immediate attention. It is assumed that the attacker can access demand forecasts on a generator bus which is being attacked. The access can be obtained by compromising a computer which stores demand forecasting information. The

attacker can even go a step further and run their own demand forecast algorithm using the historical data and the freely available machine learning tool.

The PV generators' voltage drops quickly when approaching active and especially reactive power generation limit [6]. The data in the demand forecast could be compromised and give a false impression that the demand is increasing, as shown in Fig. 6. This helps justify the voltage drop across busses. The reason that helps make the attack successful is that it blends in with the poor voltage control of PV generators. The timing of the attack during peak summer hours could even make it go unnoticeable.

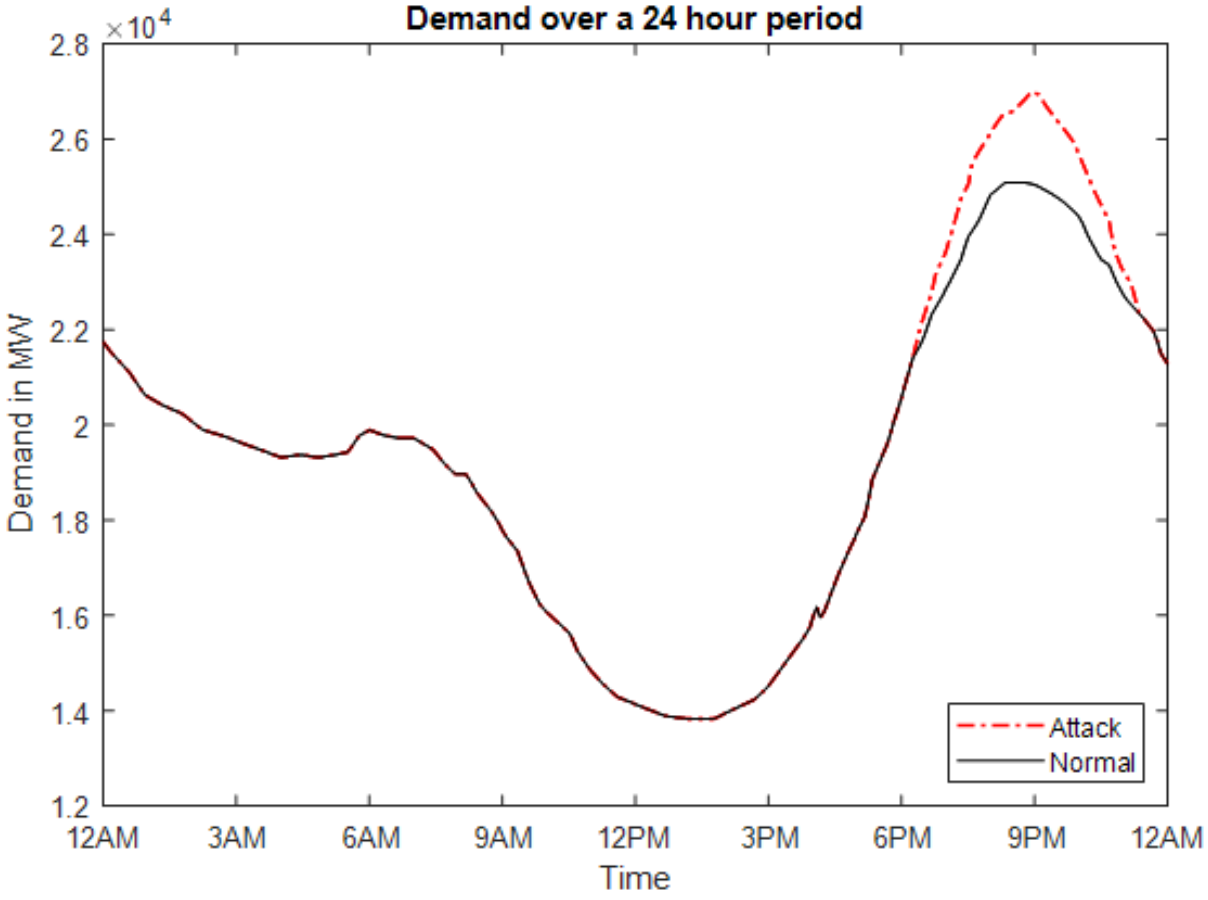

Fig 5-4: False demand injected by the attacker

Chapter 6

Results

The results of the simulation are categorized based on the algorithms being used. The performance is presented in terms of accuracy, false positive and false negative.

6.1 Detection using Kalman Filter based Detector

The attack model was simulated on Power World Simulator and MATLAB. During the period of the attack between 6 PM and 11 PM, a false demand is injected by the attacker where the demands are made to go higher than expected. The detector has a static threshold level that determines the normal operation. Any voltage levels above or below the normal operating ranges will be picked up by the detector and the Chi-squared value goes higher as the difference between expected values and measured values goes high. As Fig. 6-1 shows, the Chi-squared values kept rising and ultimately exceeded the threshold during the attack.

This was an expected behavior. However, running a separate simulation with high PV penetration during the interval of the attack, the graph was similar and indistinguishable. This gives the realization that under high PV penetration grid environment, a Chi-squared detector alone cannot be used as a detector because it will give

a large number of false positives. As the system continuously switches from solar to synchronous depending on the generation capabilities, more false detection alarms will be generated. The results show that the detector is not able to differentiate an attack from the poor voltage profile of the PV generator. The top graph is simulated with an attack, and the bottom graph is simulated with the generator switched from synchronous to PV. Hence, a traditional Chi-squared based detectors will raise a large number of false positives if deployed in grids with high PV penetration.

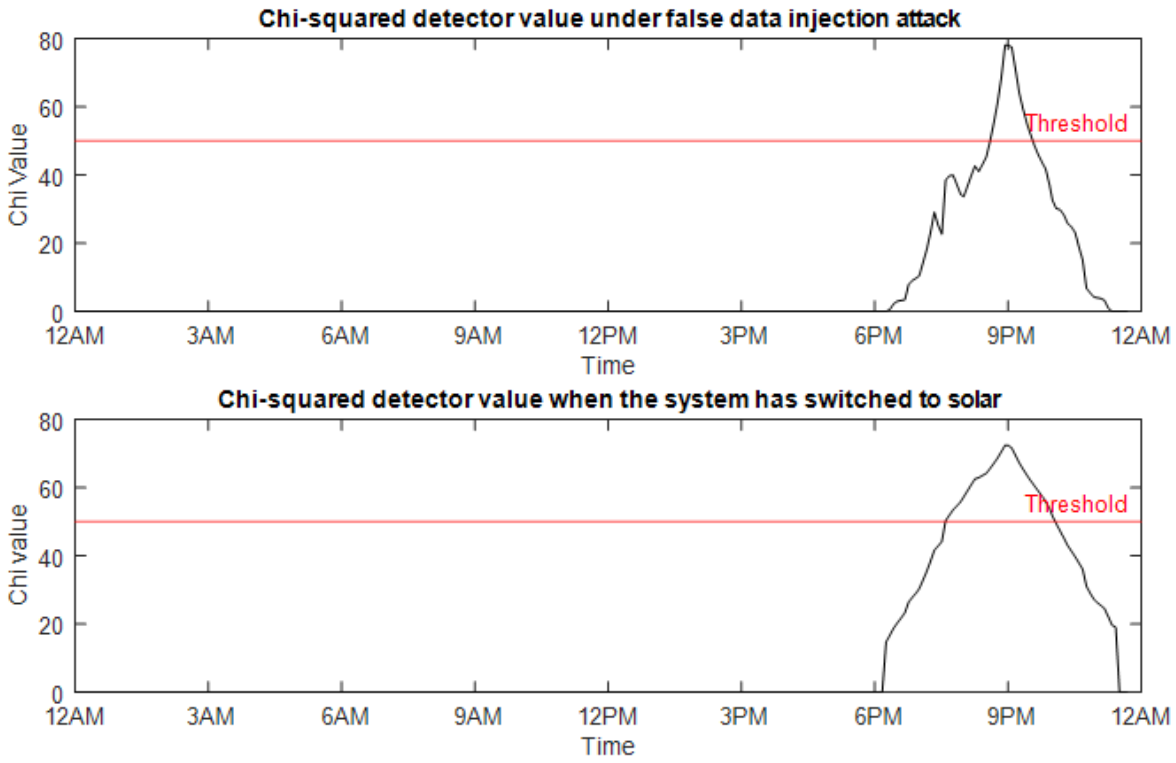

Fig 6-1: Output of the Chi-squared detector

A simple solution would be modifying the Kalman filter model to expect voltage degradation due to the switch to PV. However, the problem with this approach is that the attacker now has more flexibility for attacks even when PV penetration is low and can easily carry out attacks without the detector even noticing it. Another solution could be changing the Kalman filter model dynamically depending on the % of PV penetration in

the system. While this solution can accurately detect attacks, the switch to PV in most of the plants is unpredictable, and if the SCADA is compromised, the detector is useless.

A slightly different approach was taken in [43]. Dynamic threshold is used based on the false alarm rate allowed at the current moment instead of the static threshold. This allows adjusting the false alarm rate during periods where solar penetration is high. However, solar generations and net-demand is difficult to predict accurately. Fig 6-2 shows maximum errors in net-demand prediction over 10 days between June 16 and 25, 2022 in the data published by CAISO [9].

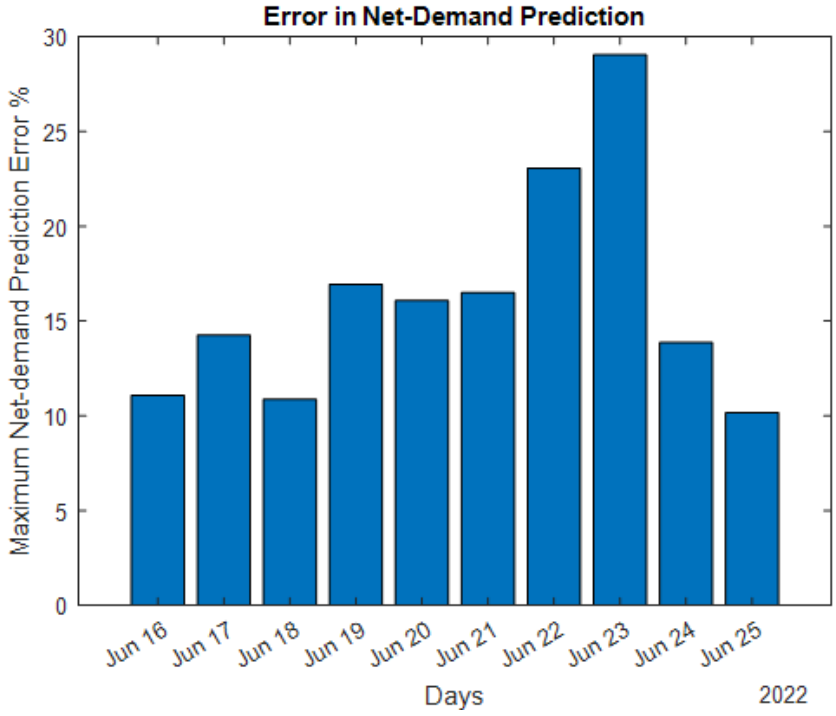

Fig 6-2: Error in Net-Demand Prediction

As [43] mentions, the yin-yang effect of Behind the Meter (BTM) PV adversely affects the net-demand prediction. Whatever BTM PV supply does not get produced (i.e., due to weather), will likely result in an increase in demand/load approximately equal to the missing BTM supply. Hence, the load forecasting algorithm continuously misses its day-

ahead net demand forecast. With the increasing number of customers using BTM solar plants, the algorithm needs access to data from these plants in real time to predict accurately. This is currently not feasible. As shown in the figure, on 23rd of June, the maximum error was close to 30%, which only backs our concern that dynamic threshold-based detectors cannot be relied on to make estimations, which makes them equally, if not more vulnerable than static threshold-based detectors.

6.2 Detection using Machine Learning based Detectors

The research work explores four of the widely used anomaly detection algorithms based on Machine Learning to learn the behavior of the grid under varying load condition and % PV penetration. The training dataset includes 12 load demands from all months of the year derived from California Independent System Operator. Each 24-hour demand is then divided into 5000 loads, and each load on the grid changes proportional to that load demand. The crucial part of this simulation is that the same simulation is done multiple times from 0%-100% PV penetration. The load flow data used for simulation are per unit voltages and MVAR generation and demand. Hence, the grid not only knows how to correlate the grid parameters, but any attempt to inject portions of parameters like voltages and power demands is detected by the anomaly detection model. The result of the work is compared using 3 performance metrics: detection rate, false positive rate and precision. Before explaining those metrics, there are 4 other terms that need to be defined, which are true positive (TP), true negative (TN), false positive (FP) and false negative (FN). True positive is the number of attacks which are successfully detected by the detector. True negative is the number successfully detected to not be an attack. False positive is the

number of non-attack instances which are incorrectly labelled attacks. False negative is the number of attacks which are incorrectly labelled as normal.

6.2.1 Accuracy (AR)

The accuracy is the ratio between the number of correctly detected attacks to the total number of attacks. Accuracy might not be the ideal metrics for giving a good picture of the detection because it can be misleading if used in a dataset which have more normal instances than attacks. Hence, precision should be used.

$$AR = \frac{Total\ correct\ predictions}{Total\ predictions}$$

$$AR = \frac{TP + TN}{TP+FP+TN+FN}$$

6.2.2 False Positive Rate (FPR)

FPR is defined as the ratio between the number of non-attack instances incorrectly detected as attack and the total number of instances.

$$FPR = \frac{Normal\ instances\ detected\ as\ attack}{Total\ number\ of\ instances}$$

$$FPR = \frac{FP}{FP+TN}$$

6.2.3 Precision (PR)

The precision is the fraction of instances predicted to be positive, which are truly positive.

$$PR = \frac{TP}{TP+FP}$$

Table I compares the FDIA detection capabilities of machine learning and Kalman filter algorithms under 0% PV penetration, while table II compares the algorithms when

there is FDI attack, and the grid is operating under 80% PV penetration. A crucial part of this work is exploring the behavior of machine learning algorithms when the grid is switched to solar. Specifically, the topic of interest is observing if the algorithm can differentiate higher PV penetration and false data injection attacks, which the Kalman Filter based algorithm failed to do.

As seen in Table I and II, One-class Support Vector Machine (OCSVM) algorithm has the best accuracy among all the machine learning algorithms, but also gives higher amounts of false positives. As the Table II shows, the machine learning algorithms have substantially lower false positive rate than Kalman Filter which indicates that the poor voltage profile during high PV penetration condition is ruled not as attack but to higher solar penetration. The machine learning algorithms are however not 100% efficient because the difference between the characteristics of states during lower PV penetration and mild false data injection attack is very subtle, and the result is expected to improve with additional training of the algorithms.

Table 6.1: FDIA Detection Under 0% PV Penetration

Algorithm	***Precision***	***False Positive Rate***	***Accuracy***
Isolation Forest	93.39%	1.41%	97.24%
Local Outlier Factor	93.16%	1.46%	97.16%
OCSVM	96.05%	0.82%	97.88%
Mahalanobis Distance	93.27%	1.41%	96.94%
Kalman Filter	98.06%	0.41%	98.86%

Table 6.2: FDIA Detection Under 40% PV Penetration

Algorithm	***Precision***	***False Positive Rate***	***Accuracy***
Isolation Forest	92.73%	1.56%	97.06%
Local Outlier Factor	92.61%	1.58%	97%%
OCSVM	95.69%	0.90%	97.72%
Mahalanobis Distance	92.12%	1.65%	96.54%
Kalman Filter	96.58%	0.73%	98.38%

Table 6.3: FDIA Detection Under 80% PV Penetration

Algorithm	***Precision***	***False Positive Rate***	***Accuracy***
Isolation Forest	90.92%	1.97%	96.62%
Local Outlier Factor	90.88%	1.97%	96.54%
OCSVM	94.80%	1.09%	97.52%
Mahalanobis Distance	90.73%	1.97%	96.24%
Kalman Filter	67.22%	10.04%	90.66%

Chapter 7

Conclusion and Future Work

In this thesis work, a vulnerability associated with model-based detectors is exposed, and the performance of machine learning based algorithms in the same scenario is exposed. It was concluded that the model-based detector works best only on a grid environment with little to no PV penetration. While dynamic thresholds can be used to overcome this problem, it has been shown that the grid's behavior cannot be predicted accurately well ahead of time. To attempt to do it accurately, massive amounts of data from large number BTM devices would have to be taken, which is not feasible now. Finally, it was observed that, if trained substantially, machine learning algorithms have the awareness to understand if a degrading voltage profile is due to a false data injection attack or a switch to PV generators.

The thesis used 5000 data points and 14 bus IEEE setup for simulation. However, more accurate data could be obtained if the simulation was done over more load points that spanned a few days or even weeks. Similarly, instead of using 14-bus, a larger grid setup would have given a more realistic scenario. These tasks could certainly be a done as future work for the research. Additionally, new algorithms like Artificial Neural Networks could be explored for this research work.

References

[1] Horowitz, Kelsey A, Peterson, Zachary, Coddington, Michael H, Ding, Fei, Sigrin, Benjamin O, Saleem, Danish, Baldwin, Sara E, Lydic, Brian, Stanfield, Sky C, Enbar, Nadav, Coley, Steven, Sundararajan, Aditya, and Schroeder, Chris. An Overview of Distributed Energy Resource (DER) Interconnection: Current Practices and Emerging Solutions. United States: N. p., 2019. Web. doi:10.2172/1508510.

[2] Abur, A. & Gomez-Exposito, Antonio. (2004). *Power System State Estimation: Theory and Implementation*. 10.1201/9780203913673.

[3] K. Manandhar, X. Cao, F. Hu and Y. Liu, "*Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter*," in IEEE Transactions on Control of Network Systems, vol. 1, no. 4, pp. 370-379, Dec. 2014, doi: 10.1109/TCNS.2014.2357531.

[4] Deebiga, K. & Hussain, Raqib. (2015). *Optimal Placement of Phasor Measurement Unit for Better Power System Observability*. TELKOMNIKA Indonesian Journal of Electrical Engineering. 14. 10.11591/telkomnika.v14i2.7605.

[5] Labbe, R. R. (2020). *Kalman and Bayesian Filters in Python*.

[6] J. Till, S. You, Y. Liu and P. Du, "*Impact of High PV Penetration on Voltage Stability*," 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), 2020, pp. 1-5, doi: 10.1109/TD39804.2020.9299973.

[7] Norden, R. H. "*A Survey of Maximum Likelihood Estimation.*" International Statistical Review / Revue Internationale de Statistique, vol. 40, no. 3, 1972, pp. 329–54. JSTOR, https://doi.org/10.2307/1402471. Accessed 1 Dec. 2022.

[8] J. Zhang, G. Welch, G. Bishop and Z. Huang, "*A Two-Stage Kalman Filter Approach for Robust and Real-Time Power System State Estimation*," in IEEE Transactions on Sustainable Energy, vol. 5, no. 2, pp. 629-636, April 2014, doi: 10.1109/TSTE.2013.2280246.

[9] California ISO. Available at: http://www.caiso.com/ (Accessed: November 1, 2022).

[10] McHugh ML. *The chi-square test of independence*. Biochem Med (Zagreb). 2013;23(2):143-9. doi: 10.11613/bm.2013.018. PMID: 23894860; PMCID: PMC3900058.

[11] A. S. Musleh, G. Chen and Z. Y. Dong, "*A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids*," in IEEE Transactions on Smart Grid, vol. 11, no. 3, pp. 2218-2234, May 2020, doi: 10.1109/TSG.2019.2949998.

[12] McDowell, Jason et al. "Reactive Power Interconnection Requirements for PV and Wind Plants - Recommendations to NERC." (2012).

[13] Schweppe F.C. and Wildes J., "Power System Static-State Estimation, Part I: Exact Model", IEEE Transactions on Power Apparatus and Systems, Vol.PAS-89, January 1970, pp. 120-125.

[14] Schweppe and Rom D.B., "Power System Static-State Estimation, Part II: Approximate Model", IEEE Transactions on Power Apparatus and Systems, Vol.PAS-89, January 1970, pp.125-130.

[15] Schweppe F.C., "Power System Static-State Estimation, Part III: Implementation", IEEE Transactions on Power Apparatus and Systems, Vol.PAS-89, January 1970, pp.130-13

[16] J. Duan, W. Zeng and M.-Y. Chow, “Resilient Distributed DC Optimal Power Flow Against Data Integrity Attack,” IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 3543 - 3552, 2018.

[17] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung and C.-K. Wen, “Local cyber-physical attack with leveraging detection in smart grid,” in IEEE International Conference on Smart Grid Communications (SmartGridComm), 2017.

[18] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung and C.-K. Wen, “Local cyber-physical attack with leveraging detection in smart grid,” in IEEE International Conference on Smart Grid Communications (SmartGridComm), 2017.

[19] Q. Jiang, H. Chen, L. Xie and K. Wang, “Real-time detection of false data injection attack using residual prewhitening in smart grid network,” in IEEE International Conference on Smart Grid Communications (SmartGridComm), 2017.

[20] M. N. Kurt, Y. Yılmaz and X. Wang, “Distributed Quickest Detection of Cyber-Attacks in Smart Grid,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2015 - 2030, 2018.

[21] X. Wang, X. Luo, M. Zhang and X. Guan, “Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers,” International Journal of Electrical Power & Energy Systems, vol. 110, pp. 208-222, 2019.

[22] H. Karimipour and V. Dinavahi, “Robust Massively Parallel Dynamic State Estimation of Power Systems Against Cyber-Attack,” IEEE Access, vol. 6, pp. 2984 - 2995, 2018.

[23] H. Karimipour and V. Dinavahi, “On false data injection attack against dynamic state estimation on smart power grids,” in IEEE International Conference on Smart Energy Grid Engineering (SEGE), 2017.

[24] S. Sahoo, S. Mishra, J. C.-H. Peng and T. Dragicevic, “A Stealth Cyber Attack Detection Strategy for DC Microgrids,” IEEE Transactions on Power Electronics, p. in press, 2018.

[25] B. Li, T. Ding, C. Huang, J. Zhao, Y. Yang and Y. Chen, “Detecting False Data Injection Attacks Against Power System State Estimation with Fast Go-Decomposition (GoDec) Approach,” IEEE Transactions on Industrial Informatics, vol. 15, no. 5, pp. 2892 - 2904, 2019.

[26] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih and Z. Han, “Detecting False Data Injection Attacks on Power Grid by Sparse Optimization,” IEEE Transactions on Smart Grid, vol. 5, no. 2, pp. 612 - 621, 2014.

[27] A. Ameli, A. Hooshyar and E. F. El-Saadany, “Development of a Cyber-Resilient Line Current Differential Relay,” IEEE Transactions on Industrial Informatics, vol. 15, no. 1, pp. 305 - 318, 2019.

[28] A. Ashok, M. Govindarasu and V. Ajjarapu, “Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation,” IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 1636 - 1646, 2018.

[29] S. Binna, S. R. Kuppannagari, D. Engel and V. K. Prasanna, “Subset Level Detection of False Data Injection Attacks in Smart Grids,” in IEEE Conference on Technologies for Sustainability (SusTech), 2018.

[30] S. A. Foroutan and F. R. Salmasi, “Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method,” IET Cyber-Physical Systems: Theory & Applications, vol. 2, no. 4, pp. 161 - 171, 2017.

[31] D. Wang, X. Wang, Y. Zhang and L. Jin, “Detection of power grid disturbances and cyber-attacks based on machine learning,” Journal of Information Security and Applications, vol. 46, pp. 42-52, 2019.

[32] M. Zanetti, E. Jamhour, M. Pellenz, M. Penna, V. Zambenedetti and I. Chueiri, “A Tunable Fraud Detection System for Advanced Metering Infrastructure Using Short-Lived Patterns,” IEEE Transactions on Smart Grid, vol. 10, no. 1, pp. 830 - 840, 2019.

[33] J. L. Viegas and S. M. Vieira, “Clustering-based novelty detection to uncover electricity theft,” in IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2017.

[34] Farsadi, Murtaza & Mohammadzadeh Shahir, Farzad & Babaei, Ebrahim. (2017). Power System States Estimations Using Kalman Filter.

[35] J. Qi, A. F. Taha and J. Wang, "Comparing Kalman Filters and Observers for Power System Dynamic State Estimation With Model Uncertainty and Malicious Cyber Attacks," in IEEE Access, vol. 6, pp. 77155-77168, 2018, doi: 10.1109/ACCESS.2018.2876883.

[36] A. F. Taha, J. Qi, J. Wang and J. H. Panchal, "Risk Mitigation for Dynamic State Estimation Against Cyber Attacks and Unknown Inputs," in IEEE Transactions on Smart Grid, vol. 9, no. 2, pp. 886-899, March 2018, doi: 10.1109/TSG.2016.2570546.

[37] A. Minot, H. Sun, D. Nikovski and J. Zhang, "Distributed Estimation and Detection of Cyber-Physical Attacks in Power Systems," 2019 IEEE International Conference on Communications Workshops (ICC Workshops), 2019, pp. 1-6, doi: 10.1109/ICCW.2019.8756653.

[38] J. Zhang, G. Welch, G. Bishop and Z. Huang, "A Two-Stage Kalman Filter Approach for Robust and Real-Time Power System State Estimation," in IEEE Transactions on Sustainable Energy, vol. 5, no. 2, pp. 629-636, April 2014, doi: 10.1109/TSTE.2013.2280246.

[39] K. Manandhar, X. Cao, F. Hu and Y. Liu, "Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter," in IEEE Transactions on Control of Network Systems, vol. 1, no. 4, pp. 370-379, Dec. 2014, doi: 10.1109/TCNS.2014.2357531.

[40] J. Zhang, G. Welch and G. Bishop, "Observability and estimation uncertainty analysis for PMU placement alternatives," North American Power Symposium 2010, 2010, pp. 1-8, doi: 10.1109/NAPS.2010.5618970.

[41] Mo, Yilin & Sinopoli, Bruno. (2010). False data injection attacks in control systems. Preprints of the 1st Workshop on Secure Control Systems.

[42] Abur, A. & Gomez-Exposito, Antonio. (2004). Power System State Estimation: Theory and Implementation. 10.1201/9780203913673.

[43] Y. Wang, Z. Zhang, J. Ma and Q. Jin, "KFRNN: An Effective False Data Injection Attack Detection in Smart Grid Based on Kalman Filter and Recurrent Neural Network," in IEEE Internet of Things Journal, vol. 9, no. 9, pp. 6893-6904, 1 May1, 2022, doi: 10.1109/JIOT.2021.3113900.