Optimization Models for Advanced Cyber-security in the Smart Grid

by

Seyedamirabbas Mousavian

A dissertation submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Auburn, Alabama
August 2, 2014

Keywords: Cyber-security, Risk Mitigation, Phasor Measurement Units, Optimal placement, Mixed Integer Linear Programming, Artificial neural networks

Approved by

Jorge Valenzuela, Chair, Full Professor of Industrial and Systems Engineering
Jianhui Wang, Affiliated Professor of Industrial and Systems Engineering
Saeed Maghsoodloo, Professor Emeritus of Industrial and Systems Engineering
Chase Murray, Assistant Professor of Industrial and Systems Engineering

Acknowledgments

I would first and foremost like to thank my God because without Him, I would not have completed the process of obtaining a Ph.D. Secondly, I am eternally grateful for my advisor, Dr. Jorge Valenzuela, for continuing to guide my dissertation from afar. He continued to encourage, support, criticize and guide me even when it was uncertain where my dissertation was going.

In addition, I would like to especially thank Dr. Jianhui Wang and the Argonne National Laboratory for the research and financial supports throughout my studies. Also, I would like to thank my committee, Dr. Chase Murray and Dr. Allison Jones-Farmer, for their support in the dissertation process.

Last but not the least, I would like to thank my lovely parents and sister, Aliasghar Mousavian and Zahra Jaberansari and Samaneh Mousavian, for being so encouraging and supportive. They continued to push me when I wanted to give up and listened to all of the issues I ran into even when it was not interesting. I am so grateful and thankful for them and would like to dedicate this hard-work to my family who loves regardless.

Table of Contents

List of Figures

List of Tables

Introduction

The power grid is increasingly dependent on information and communication technologies, which puts more emphasis on the importance of power system security as one of the top priorities. Internal and external factors can put the security of the power system at risk. The external factors include cyber-terrorist attacks, sabotage and environmental impacts while the internal factors are inherent to the accuracy of power system applications and their associated input data. As the utility industry becomes more automated and relies more on automated devices, the major threat to the grid is shifting from equipment failures to cyber-security attacks. Hence, improvement of the cyber-security of the power grid along with the reliability of the power system operations are primary focus of the United States government, power industry executives, and the research community.

Cyber-attacks to power systems could cause huge financial losses and substantial damages to the power grid. Hence, the main goal of the research summarized in this dissertation is to highlight the risks associated to the cyber-attacks to power systems and develop algorithms and models to improve the safe operations of the electric power grid. To achieve this goal, a detection algorithm is developed to avoid cyber-attacks to the optimal power flow (OPF) software module of the power systems. Since there is no guarantee that detection models detect all potential cyber-attacks, it is necessary to equip power systems with response models which avoid propagation of the cyber-atacks. In this dissertation, cyber-attacks to a specific network of the power systems, known as the phasor measurement unit (PMU) network, have been discussed, and a risk mitigation model for cyber-attacks to PMU networks is proposed. PMUs provide the system operators with the real-time operating status of the power grid, which can be further utilized for better cyber-security of the power grid. Since PMUs require considerable capital investments, an investment decision model is

developed in this dissertation for the optimal allocation of phasor measurement units. Therefore, this dissertation outlines a research that will consider the OPF and state estimation modules of the electrical power systems and deliver the following outcomes.

- An algorithm for real-time data reassurance in the OPF module
- A probabilistic risk mitigation model for cyber-attacks to PMU networks
- An investment decision model for the optimal allocation of phasor measurement units

The remainder of this dissertation is organized as follows. Chapter 1 explains the cyber-security problem of the OPF module and introduces the real-time data reassurance model to improve the cyber-security of the OPF module. Chapter 2 provides background information about cyber-security of the PMU networks and explains the probabilistic risk mitigation model for cyber-attacks to the PMU networks. Chapter 3 discusses the challenges of the optimal placement of PMUs (OPP) problem and describes the developed investment decision model to allocate PMUs with minimum capital costs.

Chapter 1

Real-time Data Reassurance in Electrical Power Systems based on Artificial Neural Networks

1.1 Abstract

Power system security is vulnerable to cyber-attacks that may cause significant damages to the power grid and result in huge financial losses. In this paper, we show the risks associated with cyber-attacks and propose an artificial neural network-based protection approach. The proposed algorithm can monitor the output of power flow calculations and detect data anomalies in real-time. The network observability rules are formulated as a mixed integer linear program (MILP) problem. The results of the MILP problem are used to decrease the amount of data input required by the algorithm while the system stays observable. We run our experiments on the IEEE 24-bus reliability test system. The experimental results show that the developed algorithm is a promising enhancement to ensure data integrity in control centers.

keywords: Power system security, Artificial neural networks, Cyber-security, Network observability

Nomenclature

Sets

Υ_k: Set of lines to/from the bus k

Ω: Set of zero injection buses

Φ_k: Set of lines to/from the zero-injection bus $k \in \Omega$

Ψ: Set of generators

Constants

K: Number of buses

L: Number of lines

L_k: Load at bus k

$\alpha(l)$: From bus of line l

$\beta(l)$: To bus of line l

$H_{k,l}$: Incidence matrix coefficient (-1, 0 or 1) at bus k of line l

S_l: Susceptance of line l (Siemens)

C_g: Energy cost of generator g ($/MWh)

P_g^{min}: Minimum generation of generator g (MW)

P_g^{max}: Maximum generation of generator g (MW)

F_l^{max}: Maximum capacity of line l (MVA)

N_k: Number of transmission lines to/from zero-injection bus k

Variables

p_g: Energy dispatched by generator $g \in \Psi$ (MW)

f_l: Power flow at line $l = 1, , L$ (MVA)

θ_k Voltage angle at bus $k = 1, .., K$ (Degrees)

x_l: Binary variable which equals 1 if line l is chosen

$x_l^{'}$: Binary variable which equals 1 if the flow on line l can be computed

y_k: Binary variable which equals 1 if bus k is chosen

$y_k^{'}$: Binary variable which equals 1 if the voltage on bus k can be computed

ϵ_i: Threshold value i

SSE_t: The mean of the sum of squared errors at time t

F : Power flow matrix

1.2 Introduction

Power system security is one of the top priorities for control center operators. Internal and external factors can put the security of the power system at risk. The external factors include cyber-terrorist attacks, sabotage and environmental impacts [1] while the internal factors are inherent to the accuracy of power system applications and their associated input data. As the utility industry becomes more automated and relies more on automated devices, the major threat to the grid is shifting from equipment failures to cyber-security attacks [2]. According to [3], cyber threats happen when unauthorized users exploit cyber system vulnerabilities. A cyber terrorist could wisely design a malicious data-tampering attack to deliberately inflict major damage on the power grid. The intruder can gain access to the supervisory control of a SCADA system and initiate control actions. Several software modules are used by power system operators to support decision making in the control centers. As a case in point, the state estimation software gives system operators an updated picture of the system status by estimating the actual values of system variables using real-time data. The software estimates the voltage magnitudes and voltage angles at all network buses [4]. The effectiveness of state estimation can be affected by bad data stemming from equipment installation problems, localized equipment failures, communication errors, etc. It has been also pointed out in [5] that the cyber-attackers may take advantage of the bad data for financial arbitrage such as virtual bidding at selected pairs of nodes. Since state estimation procedures already consider that data measurements can be bad, existing procedures have been modified to detect malicious attacks to the data [6]. The weighted least squares (WLS) method, which solves Gauss normal equations iteratively, was initially used in state estimation. And consequently, the Bad Data Detection, Identification and Elimination (BDDIE) method was proposed to detect data attacks [6]. These orthogonal transformation techniques are not widely used in the power system community due to the required high computation efforts in large systems [7]. The bad data suppression (BDS) algorithm, based on a non-quadratic cost function, was proposed to improve the performance of the WLS

technique in the presence of bad data [7]. In this technique, the least normalized residuals (LNR) are used in detection and elimination of bad data. This use of residual analysis and non-quadratic estimation criteria laid the groundwork for the concept of interacting vs. non-interacting bad data and the ability to probabilistically predict false alarms [8]. Valenzuela et al. [9] considered another important software module used by the control centers, the Optimal Power Flow (OPF), that can be a target for a data attack. OPF determines the steady-state operation point which ensures the minimum generation cost while maintaining system constraints on real and reactive power, generator outputs, transmission line flows, bus voltages, etc. The authors pointed out that an undetected cyber-attack on the input data to the OPF module could cause power to be dispatched erroneously, overloading transmission lines and possibly resulting in cascading power outages. Traditional state estimation can detect differences in database parameters and estimated parameters during the bad data detection process; however, cyber terrorists could carefully design an attack after the most recent state estimation program has run that is undetectable and intentionally designed to hamper the grid. In [10], it was shown that false data injection attacks cannot be avoided in todays SCADA systems. The notion of a false data injection attack was first introduced in 2009 [11]. Besides, it is discussed in [12] that current bad data detection schemes would not detect all types of parameter changes, especially when branch power flows and power injections at both ends of a branch are critical to estimate the conventional state vector. Hence, it can be inferred that data manipulations would remain undetected and the incorrect database parameters would be used for later decisions. It has been pointed out also in [13] that there is a crucial need for SCADA real-time intrusion detection algorithms to mitigate the risk of cyber threats. To our knowledge, the data supplied to the OPF module is not well-protected against these kinds of attacks and could be an attractive target for cyber-attackers. In a similar research to this paper, Valenzuela et al. [9] proposed a bad data detection algorithm that monitors the AC power flow results of the OPF. The algorithm uses Principal Component Analysis (PCA) to determine whether the power system input data has been

compromised. In this paper, we address the same problem as in [9], but we use a different approach which allows for several enhancements to our algorithm. Our approach is based on a forecasting technique while the other paper uses a variability monitoring technique. The advantage of our technique is that the threshold value can be computed statistically. The threshold value in [9] is obtained by experimentation. Another difference is that [9] considers just the AC OPF software while we consider both the AC and DC OPF. Lastly, we show by an example how a cyber-attack to the network data can endanger the physical power system, which is not discussed in [9]. We use artificial neural network (ANN) to verify the trustworthiness of the results from the OPF. ANN has been used extensively in nonlinear systems such as the single-ended fault location of transmission lines [14], short term load forecasting [15] and power transformer fault diagnosis [16]. However, to the best of our knowledge, it has not been used in detecting data anomalies in power system applications. We also model network observability rules as a mixed integer linear programming (MILP) problem to reduce the dimensionality of the problem while still maintaining the critical variables.

The rest of this chapter is organized as follows: Section 1.3 describes the optimal power flow model. Section 1.4 analyzes the cyber-attacks to the network data. Section 1.5 discusses the anomaly detection model and the ANN algorithm. Section 1.6 provides experimental results and Section 1.7 reports our conclusions.

1.3 Optimal power flow model

Modern power system control centers run a sophisticated collection of computer applications and maintain huge databases that ensure the economical operations of the power system. The input data to various application modules is cleansed and sampled for computation, storage and further analysis. In this paper we model a system where a cyber terrorist has compromised the integrity of the data supplied to the OPF module. We focus on the OPF module because it plays a significant role in power generation and transmission, and an

undetected attack to the input data to the OPF could be disastrous to the power grid. OPF is an optimization-based module which minimizes the total generation cost of the system. For simplicity, a simplified DC OPF is presented in this section. However, in Section 1.5, we provide the results for both the DC and AC models.

$$z = \min \sum_{g \in \Psi} C_g p_g \tag{1.1}$$

Subject to

$$\sum_{l=1}^{L} H_{k,l} f_l + p_k = L_k \qquad k = 1, \ldots, K \tag{1.2}$$

$$f_l - S_l(\theta_{\alpha(l)} - \theta_{\beta(l)}) = 0 \qquad l = 1, \ldots, L \tag{1.3}$$

$$-F_l^{max} \leq f_l \leq F_l^{max} \qquad l = 1, \ldots, L \tag{1.4}$$

$$P_g^{min} \leq p_g \leq P_g^{max} \qquad \forall g \in \Psi \tag{1.5}$$

The objective function in equation (1.1) is subject to power balance constraints at each bus k given in equation (1.2). The power flow on each line l is shown in equation (1.3). Constraints in equation (1.4) represent thermal flow limits for all lines, and constraints in equation (1.5) are generation capacities for each generator. The variables θ_k are unrestricted.

1.4 Analysis of cyber-attacks to the network data

The main goal of this research is to provide the system operators with an approach to protect the power system from attacks against the network model used in the OPF calculation. The network model represents the physical parameters of the network and is stored in a database. We use a 6-bus test system given in [17] to show how a cyber-attack to the network data can endanger the physical power system. The 6-bus test system is shown in Figure 1.1. This test system includes six buses, three generators and eleven transmission lines. TABLE 1.1 shows the load at each bus.

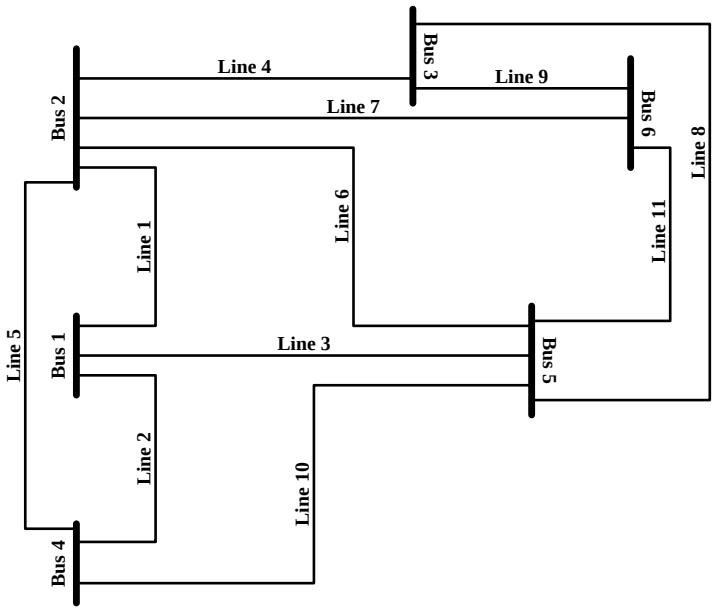


Figure 1.1: The 6-bus Test System

Table 1.1: Load in MW

Bus	1	2	3	4	5	6
Load (MW)	0	0	0	80	80	80

First, we run the DC version of the OPF software to obtain power generation outputs and flows in the transmission lines assuming that there is no contaminated data. We use MatPower [18] in this paper for the OPF calculations. The power generation results are given in TABLE 1.2, and TABLE 1.3 shows the flows on transmission lines. The last column of TABLE 1.3 shows the percentage of transmission line capacity used for dispatching.

Table 1.2: Power generation output with no cyber-attack

Generator	1	2	3	Total
p_g (MW)	46.77	103.18	90.05	240

Next, we assume that intruders attack the database by getting access to the physical parameters of the network and carefully making changes to hamper the power grid. In addition, we assume that the system operator is unaware of these changes and operates the

Table 1.3: Flows with no cyber-attack

Line	F_l^{max}	$f_l(MVA)$	% Line Capacity Used
1	40	-1.37	3.4
2	60	26.67	44.5
3	40	21.46	53.6
4	40	-2.71	6.8
5	60	56.08	93.5
6	30	22.37	74.6
7	90	26.07	29.0
8	70	28.42	40.6
9	80	58.92	73.6
10	20	2.76	13.8
11	40	-4.99	12.5

system using the tampered data. The attacks consist of changing the network topology by modifying the origin and destination buses of some transmission lines. Mathematically, the network topology is represented by $H_{k,l}$ in equation (1.2) of the OPF model. In the 6-bus test system, line 1 distributes the power from bus 1 to bus 2. Line 5 goes from bus 2 to bus 4. We assume that the attack aims at changing the destination of line 1 to bus 3 and the destination of line 5 to bus 3. Notice that these cyber-attacks will change only the network topology and there will be no change in the physical parameters of the network. Figure 1.2 shows the network model under attack. The dashed lines are the actual lines in the physical network which the attacker modifies. As a result, the network topology stored in the database no longer maps to the real system. Because the network model does not match the physical network, the physical flows will be different from the flows obtained by the OPF software. To compute the physical flows after the cyber-attack, we used MatPower [18], set the input voltage angles at all buses and obtained physical power flows. TABLE 1.4 shows the physical power flows on each line when the system is under cyber-attack.

As shown in TABLE 1.4, line 9 is obviously overloaded. Overloaded transmission lines are highly undesirable to the grid stability since the overloaded transmission lines may lead to cascading outages and blackouts. In addition to possible overloaded lines, an attack can affect the economics of power systems by using more expensive generating units or taking

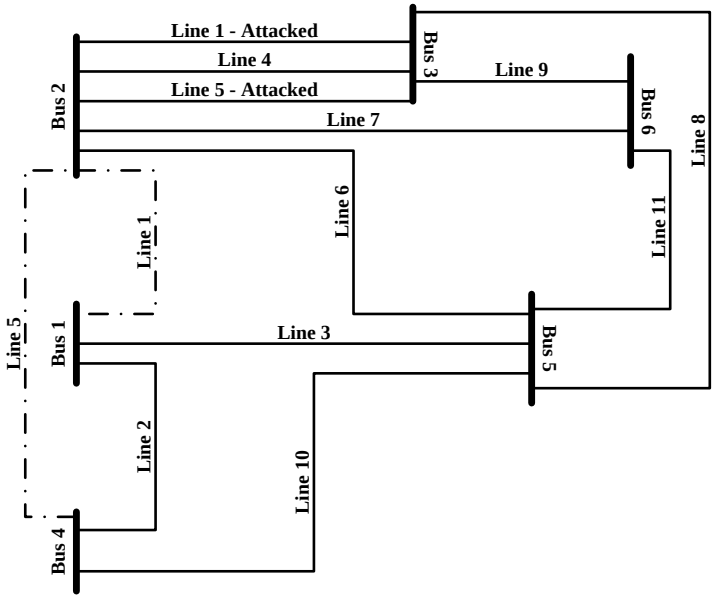


Figure 1.2: The network model under attack

Table 1.4: Flows after the cyber-attack

Line	Power Flow	% Line Capacity Used
1	0.34	0.8
2	25.58	42.6
3	11.78	29.4
4	-37.00	92.5
5	50.47	84.1
6	11.55	38.5
7	-0.26	0.29
8	48.91	69.9
9	91.98	115.0
10	-3.96	19.9
11	-11.72	29.3

advantage of financial arbitrage in virtual bidding at different nodes [19]. Therefore, it is extremely important to detect this type of cyber-attack to the system.

1.5 Detection model

In this section, we describe a model that allows the system operators to detect whether the network model has been compromised. The detection model is based on ANN, which

has been used extensively in the area of power systems. In particular, ANN has broad applications in fault diagnosis methods because of its ability to deal with noisy inputs, non-linear function approximation, and adaptive learning.

1.5.1 Artificial Neural Network Model

ANNs are usually trained offline and then used to detect faults online. As shown in Figure 1.3, an ANN is composed of interconnected layers of artificial neurons. ANN is a powerful computational model which can adjust the values of the connections, namely the weights, to approximate almost any nonlinear function [20].

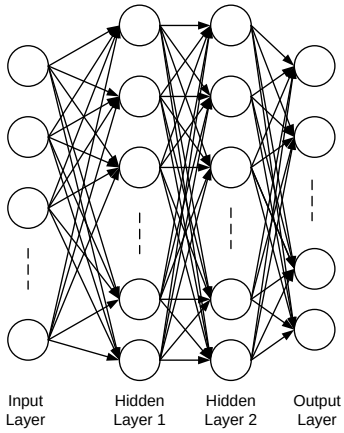


Figure 1.3: Multi-layer ANN with two hidden layers

In our detection model, ANN is used to estimate the power flows at period t given the load and the power flows at the previous period $t-1$. To detect anomalies the estimated power flows are then compared to the power flow output from the OPF module in the same period to determine whether an anomaly exists. The flows and the load at the previous period are the input data to the ANN model. The load is included to eliminate the variations stemming from load variability. Figure 1.4 shows a block diagram of the inputs/outputs of the algorithm. The MATLAB Neural Network Toolbox described in [20] is used to train the ANN module of the detection algorithm.

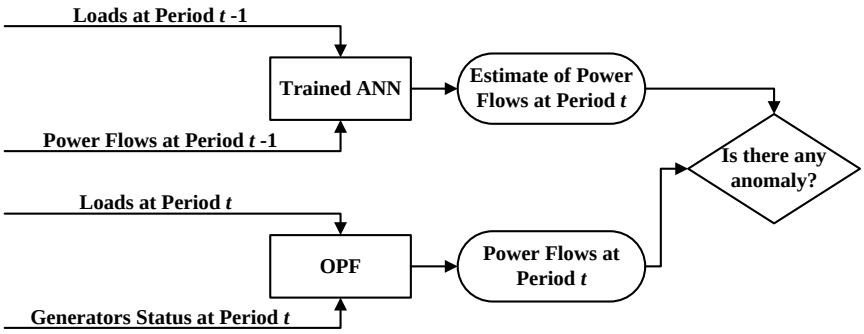


Figure 1.4: Block diagram of the inputs/outputs of the algorithm

1.5.2 ANN Reduction

The number of input vector entries to the ANN model is determined by the number of transmission lines plus the number of buses where loads are present. Since one of the factors affecting the computational efficiency of the detection algorithm is the size of the input vector, we use the concept of network observability defined in [21] to reduce the size of ANN. The network observability is a measure for how well to infer the state of a system by knowledge of a subset of its external outputs. Hence, we can just select a subset of transmission flows and buses such that the power system can still remain observable with less data. The problem of finding these subsets is formulated as a MILP model where the constraints assure the observability of the power network. The MILP model is formulated as follows:

$$\min \sum_{l=1}^{L} x_l + \sum_{k=1}^{K} y_k \tag{1.6}$$

Subject to

$$y^{'}_{\beta(l)} = y_{\alpha(l)} x_l \qquad \forall l \; such \; that \; \beta(l) \notin \Omega \tag{1.7}$$

$$x^{'}_{l} = y_{\alpha(l)} y_{\beta(l)} \qquad \forall l \; such \; that \; \beta(l) \; or \; \alpha(l) \notin \Omega \tag{1.8}$$

$$\left(\sum_{l \in \Phi_k} x_l \right) - x^{'}_{l'} \leq N_k - 2 \qquad \forall k \in \Omega \; and \; \forall l^{'} \in \Phi_k \tag{1.9}$$

$$x_l + x^{'}_{l} \geq 1 \qquad l = 1, \ldots, L \tag{1.10}$$

$$y_k + y_k^{'} \geq 1 \qquad \forall k \notin \Omega \tag{1.11}$$

$$\sum_{l \in \Upsilon_k} x_l \geq 1 \qquad k = 1, \ldots, K \tag{1.12}$$

$$x_l, x_l^{'}, y_k, y_k^{'} \in \{0, 1\} \qquad l = 1, \ldots, L \; and \; \forall k \notin \Omega \tag{1.13}$$

In the objective function, equation (1.6), the first term is the total number of selected transmission lines while the second term is the total number of chosen buses. Constraints equation (1.7) assure that if we know the flow of a branch and the bus voltage on one end, then the bus voltage on the other end can be calculated via the power flow equations. Since the term $y_{\alpha(l)}x_l$ is the product of two binary variables, these constraints are nonlinear. These constraints can be represented by a group of linear constraints as follows:

$$2y_{\beta(l)}^{'} - y_{\alpha(l)} - x_l \leq 0 \tag{1.14}$$

$$y_{\beta(l)}^{'} - y_{\alpha(l)} - x_l \geq -1 \tag{1.15}$$

These two constraints set the binary variable $y_{\beta(l)}^{'}$ to be the product of $y_{\alpha(l)}$ and x_l. This is if $y_{\alpha(l)} = 0$ or $x_l = 0$, then $y_{\beta(l)}^{'} = 0$. The value of $y_{\beta(l)}^{'}$ is 1 only if $y_{\alpha(l)} = 1$ and $x_l = 1$.

Equation (1.8) assures that if we know the voltages at both buses of a transmission line, the line flow can be calculated. Again, the term $y_{\alpha(l)}y_{\beta(l)}$ is a nonlinear term. Similarly, these constraints can be represented by two linear constraints as follows:

$$2x_l^{'} - y_{\alpha(l)} - y_{\beta(l)} \leq 0 \tag{1.16}$$

$$x_l^{'} - y_{\alpha(l)} - y_{\beta(l)} \geq -1 \tag{1.17}$$

Equation (1.9) assures that for a zero-injection node, if just one of the incidence transmission line flows is unknown, then it can be calculated by Kirchhoffs law. Equation (1.10) and equation (1.11) assure that all bus voltages and transmission flows are either directly or

indirectly computed. Since the ANN predicts power flows, equation (1.12) assures that at least one transmission line from each bus is included in the reduced set of inputs.

1.5.3 Detection Algorithm

The detection algorithm is theoretically grounded on forecasting the power flows of the current hour t based on the power flows of the previous hour $t-1$. Forecasted power flows at hour t are compared to the power flows generated by the OPF module at hour t. The difference is computed by the sum of squared errors (SSE) of the forecasted flows and the flows from the OPF. If the SSE is greater than a threshold value, the alarm informs the system operator that the power system may have been compromised. We use ANN as the forecasting tool since it has been shown in other applications [14–16] to have excellent multivariate forecasting capabilities. We describe our methodology by the following pseudo code:

Step 0. Simulate the generators status

Simulate the generators status (on/off) from a continuous-time Markov chain

Step 1. Generate historical power flows

$tSim$ = Simulation Time

for $t = 1$ to $2 \times tSim + 1$ do

Sample generator status

Solve the OPF using the load at time t

Compute the t^{th} row of the power flow matrix F

end for

Step 2. Create and Train the Neural Network

Create the matrix Training-Input by using the entries 1 to $tSim - 1$ of the flow matrix F as the input to the training function of the neural network

Create the Matrix Training-Target by using the entries 2 to $tSim$ of the flow matrix F as the target of the training function of the neural network

Create the neural network object

Train the ANN using the matrices Training-Input and Training-Target

Step 3. Statistically compute the threshold value

for $t = tSim + 1$ to $2 \times tSim + 1$ do

Obtain an estimate for the flows at time t, $\hat{P}$, by using the load and the flows at time $t - 1$ as input to the neural network

Compute the vector $\hat{U}$ by dividing $\hat{P}$ by the maximum emergency capacity of the transmission lines

Compute the t^{th} row of the used-capacity matrix U by dividing the t^{th} row of the actual power flow matrix F by the maximum emergency capacity of the transmission lines

Compute the sum of squared error SSE_t between the t^{th} row of U and $\hat{U}$

end for

Compute a threshold value ϵ based on fitting a Weibull distribution function to SSE_t

Step 4. Test Detection Algorithm

for $t = 2 \times tSim + 2$ to T do

Sample generator status

Obtain an estimate for the flows at time t, $\hat{P}$, by using the load and the flows at time $t - 1$ as input to the neural network

Compute the vector $\hat{U}$ by dividing $\hat{P}$ by the maximum emergency capacity of the transmission lines

Solve the OPF using the load at time t

Compute the vector U by dividing the power flows obtained from the OPF by the maximum emergency capacity of the transmission lines

Compute the mean of the sum of squared error SSE_t between $\hat{U}$ and U

If $SSE_t > \epsilon$ then an anomaly exists

Else the system is in control

end if

end for

We have scaled down the power flows (matrix U) to values between 0 and 1 to avoid a computer overflow when computing the sum of the squared errors. A summary of the algorithm is shown as a flowchart in Figure 1.5.

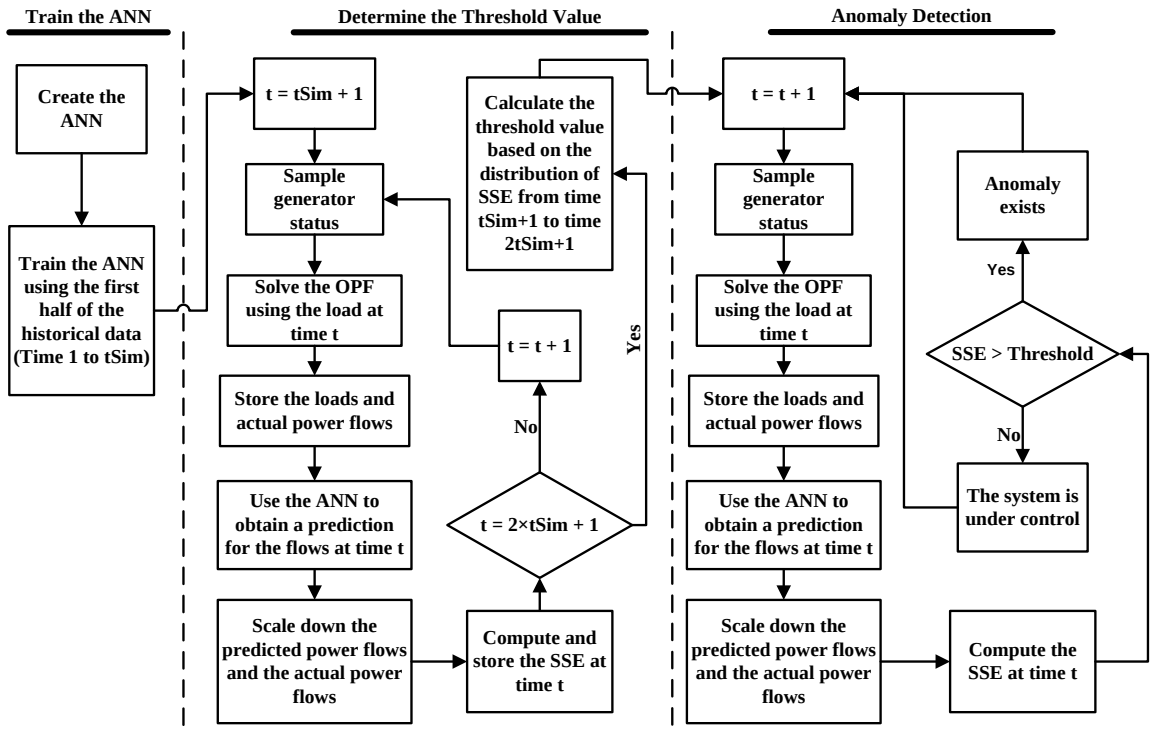


Figure 1.5: Flowchart of the anomaly detection algorithm

1.6 Experimental Results

To assess the performance of our detection algorithm, we use data from the IEEE Reliability Test System [22]. We run our experiments on the 24-bus system which consists of 38 transmission lines, 24 buses of which 17 have loads, and 33 generators. A picture of the 24-bus test system is provided in Figure 1.6. We refer the readers to [18] and [22] for additional details.

The load data are obtained from the PJM [23]. A standardized load profile of 744 hours by scaling down the load data based on the peak load is created so that the value 1.0

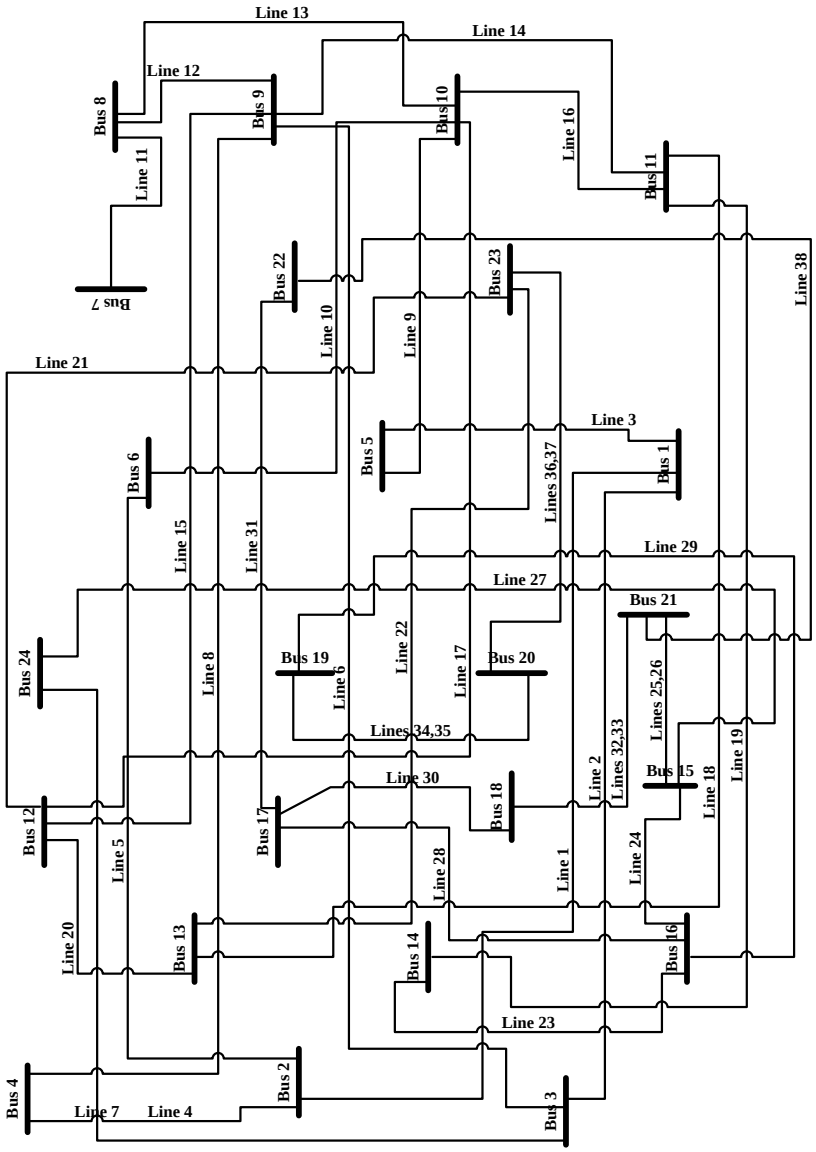


Figure 1.6: 24-bus test system

corresponds to the peak load. The load at each hour is calculated by applying the load profile to the IEEE test system. Although the load at each bus follows the same variability pattern, the actual values are distinct at different buses. Figure 1.7 is a plot of the standardized load of the first 168 hours, used to train the neural network.

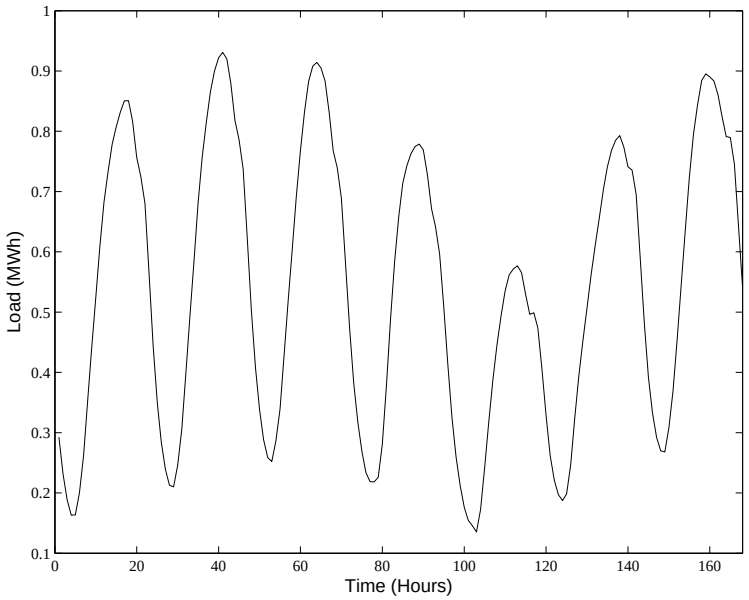


Figure 1.7: Standardized load

1.6.1 DC-OPF Detection Algorithm

In this section, we develop the detection algorithm for DC-OPF. We first construct the configuration of the ANN. The loads of buses and power flows of transmission lines (at time $t-1$) are the input variables to the ANN. The output variables are the forecasted power flows for time t.

ANN Configuration

We use the multi-layer feed-forward back-propagation technique with an adaptive learning rate and momentum. The learning rate, which controls the rate of convergence, is chosen to be 0.05. The training process is stopped when either the minimum performance gradient is reached or the performance goal is met. We simulate the operation of the power system using the DC-OPF for 168 hours (1/4 of the total hours of available data) to generate the historical power flows which are used to train the neural network. To simulate generator failures, we sample the state of the generators according to a continuous-time two-state Markov

chain. Figure 1.8 shows the variations of the power flows on four of the lines in the 24-bus test system during the training period.

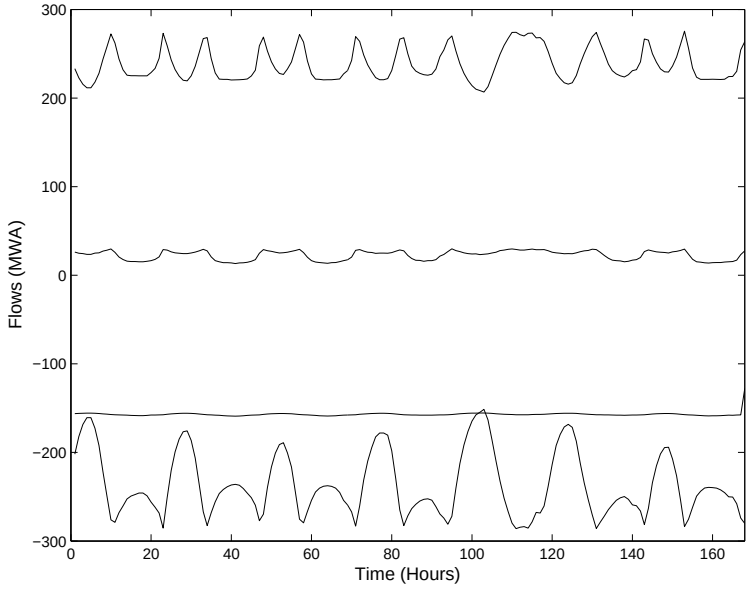


Figure 1.8: Power flows of four lines during the training period

We design two configurations, ANN-1 and ANN-2. ANN-1 uses all buses and lines (62 inputs) while ANN-2 uses the reduced network obtained by solving the MILP formulation described in section 1.4. The performance of the ANN depends on its configuration and the best configuration depends on the power network. To find the best configuration for a given power system, we have developed a computer code. The computer code tries different number of neurons for the ANN and computes the mean and standard deviation of the sum of squared errors (MSSE, SSSE) of the target output and the ANNs outputs of each configuration. The performance of an ANN configuration is defined as MSSE+SSSE and computed by using the data for hours 169 to 337. This process needs to be executed every time a new system is studied.

In our experiments, a total of 500 different ANN configurations are generated by changing the number of layers and the number of neurons on each layer. TABLE 1.5 shows the statistics of the ten best configurations for ANN-1. Based on the criterion mentioned above,

the configuration in the first row is selected for ANN-1, which is a four-layer feed-forward ANN. This network is activated by the tan-sigmoid (2 layers), log-sigmoid (1 layer) and linear (output layer) functions.

Table 1.5: Configurations of ANN-1

Configuration	Number of Neurons			The Sum of Squared Errors			
	Layer 1	Layer 2	Layer 3	Min	Mean	Max	Standard Deviation
1	17	17	15	0.0002	0.0362	0.2156	0.2154
2	17	17	18	0.0002	0.0362	0.2644	0.2642
3	15	20	15	0.0002	0.0362	0.2973	0.2935
4	15	15	15	0.0002	0.0364	0.2965	0.2963
5	14	18	18	0.0003	0.0377	0.2385	0.0547
6	17	15	16	0.0005	0.0377	0.3722	0.0652
7	7	7	0	0.0005	0.0394	0.5256	0.5251
8	8	10	0	0.0003	0.0405	0.2214	0.2211
9	11	8	0	0.0005	0.0462	0.2653	0.2648
10	13	8	0	0.0002	0.0462	0.3027	0.3025

Similarly, we determine the best configurations for ANN-2. This network uses as input the load at buses and power flows on lines determined by the mentioned MILP formulation. We solve the optimization model for the 24-bus test system. The solution is given in TABLE 1.6, which shows that by applying the network observability rules we decrease the size of the input vector by 42% (from 62 to 36 inputs). For such a small system, the reduction of the number of input/output variables may not be strictly necessary. However, for real world power systems where thousands of buses and transmission lines may exist, without reduction the number of input variables could be extremely large and prohibited for

computation. The advantage of using network observability rules is that the crucial variables are maintained in the reduced set.

Table 1.6: Solution of the MILP model

Included buses in the input vector	1, 2, 3, 5, 6, 8, 9, 10, 14, 15, 16, 19
Included lines in the input vector	3, 4, 5, 7, 8, 11, 14-22, 26-28, 30-32, 34, 36, 38

We train 500 different ANN configurations and select the one with the best performance as is done with ANN-1. TABLE 1.7 shows the ten best configurations for ANN-2. The configuration in the first row is chosen.

Table 1.7: Configurations of ANN-2

Configuration	Number of Neurons			The Sum of Squared Errors			
	Layer 1	Layer 2	Layer 3	Min	Mean	Max	Standard Deviation
1	9	13	10	0.0001	0.0145	0.0976	0.0179
2	9	10	8	0	0.0156	0.0908	0.0181
3	7	11	12	0.0002	0.0162	0.1055	0.0203
4	13	9	7	0.0001	0.0174	0.1021	0.0215
5	12	11	9	0.0001	0.0178	0.1003	0.0217
6	12	7	8	0.0003	0.0194	0.0919	0.0223
7	10	12	7	0	0.0194	0.1158	0.0240
8	12	7	10	0.0001	0.0193	0.1217	0.0245
9	8	10	8	0.0001	0.0193	0.1153	0.0247
10	9	10	9	0.0002	0.0202	0.0966	0.0238

Determining the Threshold Value

First, we statistically determine the threshold value ϵ_1 for the ANN-1 model and calculate the sum of the squared error SSE at each hour for the next 168 hours which are

hours from 169 to 337. The values of SSE are fitted to a Weibull distribution, which is commonly used in reliability engineering and failure analysis. For ANN-1, the scale and shape parameters are estimated to be 0.031 and 0.80 respectively. Assuming that a 2.5% false alarm rate is acceptable, the 97.5 percentile is considered as the threshold value, i.e. $\epsilon_1 = 0.16$. Figure 1.9 shows the cumulative distribution function of the sample data and the hypothesized distribution. Similarly, the scale and shape parameters are estimated to be 0.013 and 0.83 for ANN-2, and the threshold value is set to $\epsilon_2 = 0.05$.

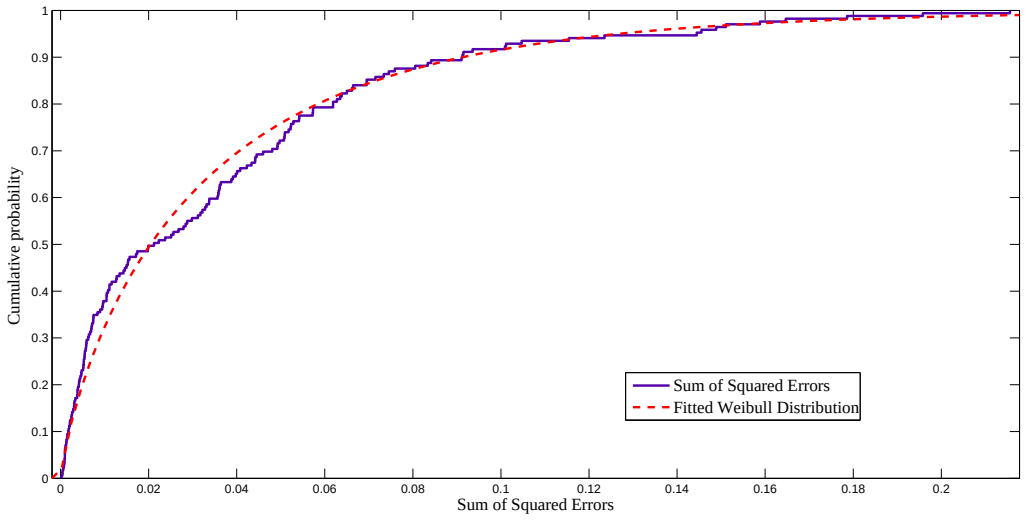


Figure 1.9: Fitted Cumulative Distribution Function to the sum of the squared errors for ANN-2

Testing the Detection Algorithm

We first study the performance of the detection algorithm under normal operation conditions. We run our simulation for the next 407 hours (hour 338 to hour 744). The normal operation includes load variability and generator outages. Figure 1.10 and Figure 1.11 show the time series of the sum of the squared errors SSE_t for ANN-1 and ANN-2, respectively. Three false alarms are observed in Figure 1.10 and seven false alarms are observed in Figure 1.11.

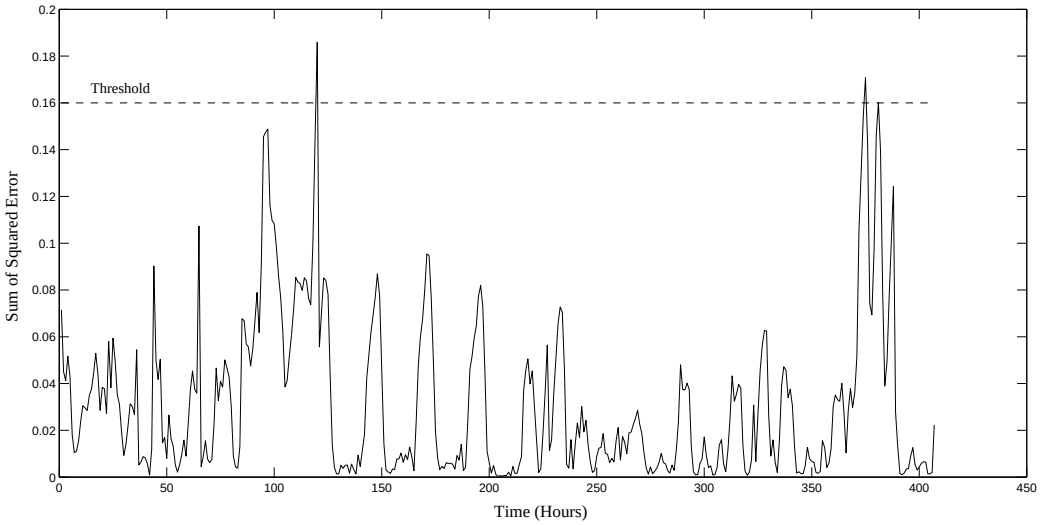


Figure 1.10: Plot of the ANN-1 false alarms

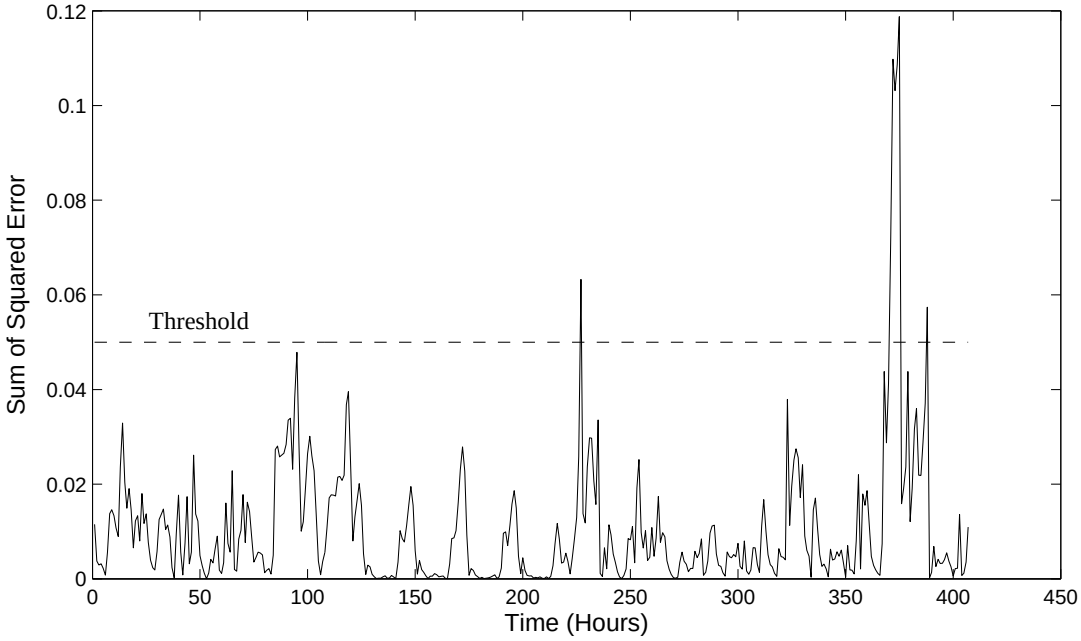


Figure 1.11: Plot of the ANN-2 false alarms

To study the performance of the detection algorithm under a cyber-attack, we change the database of the power system at one particular point in time. At hour 744, we change the phase shifter angle from 0 to $\pi/6$ radians of each line, one line at a time. We run the two

detection algorithms. TABLE 1.8 shows whether the change of a particular line is detected using either detection algorithm. The results show that ANN-1 and ANN-2 detect 37 out of the 38 injected changes.

Table 1.8: Detection results of one anomaly injection

Line	ANN-1 Detection	ANN-2 Detection	Line	ANN-1 Detection	ANN-2 Detection	Line	ANN-1 Detection	ANN-2 Detection
1	Yes	Yes	14	Yes	Yes	27	Yes	Yes
2	Yes	Yes	15	Yes	Yes	28	Yes	Yes
3	Yes	Yes	16	Yes	Yes	29	Yes	Yes
4	Yes	Yes	17	Yes	Yes	30	Yes	Yes
5	Yes	Yes	18	Yes	Yes	31	Yes	Yes
6	Yes	Yes	19	Yes	Yes	32	Yes	Yes
7	Yes	Yes	20	Yes	Yes	33	Yes	Yes
8	Yes	Yes	21	Yes	Yes	34	Yes	Yes
9	Yes	Yes	22	Yes	Yes	35	Yes	Yes
10	Yes	Yes	23	Yes	Yes	36	Yes	Yes
11	Yes	No	24	Yes	Yes	37	Yes	Yes
12	Yes	Yes	25	Yes	Yes	38	Yes	Yes
13	No	Yes	26	Yes	Yes			

Next, we create four other cyber-attack scenarios in which we change multiple lines simultaneously. Since multiple lines can be randomly selected, we run 200 replications for each attack scenario. It is assumed that the attacker may change the origin/destination of a transmission line, $H_{k,l}$, the normal capacity of a transmission line, F_l^{max} or the line availability status. We assume that the attacker may decrease the capacity of a transmission line to 10% of its original value. It is important to mention that under certain cyber-attacks the DC-OPF cannot obtain a feasible solution. Since the operator should be alerted to this condition, this cyber-attack scenario is considered detected. The cyber-attack scenarios are summarized in TABLE 1.9.

The performances of the detection algorithms ANN-1 and ANN-2 are given in TABLE 1.10. The results show that the reduced ANN-2 which eliminates redundant information performs slightly better than ANN-1 for scenarios A, B and C. In scenario D the performances of both algorithms are comparable. Hence, the reduced ANN is chosen for experiments with the AC-OPF based detection algorithm.

Table 1.9: Cyber-attack scenarios

Line	Scenarios			
	A	B	C	D
1st	Modify Origin	Modify Origin	Modify Capacity	Modify Origin
2nd	Modify Destination	Modify Capacity	Modify Capacity	Modify Origin
3rd		Remove	Modify Capacity	Modify Origin

Table 1.10: DC-OPF detection results in different cyber-attack scenarios

Scenario	%Detection	
	ANN-1 DC-OPF Model	ANN-2 DC-OPF Model
A	92.5	97.5
B	95.0	97.0
C	95.5	97.5
D	99.5	98.5

1.6.2 AC-OPF Detection Algorithm

The AC-OPF detection algorithm, ANN-3, is similar to the DC-OPF detection algorithm except that the AC-OPF algorithm takes the real AC power flows obtained from AC-OPF as inputs to the ANN and returns the estimate of the real AC power flows of the next period. The same process used for DC-OPF is used to determine the best design for ANN-3. TABLE 1.11 shows the best configurations of ANN-3. The first configuration is selected.

Table 1.11: Configurations of ANN-3

Configuration	Number of Neurons			The Sum of Squared Errors			
	Layer 1	Layer 2	Layer 3	Min	Mean	Max	Standard Deviation
1	13	11	8	0.0001	0.0163	0.1035	0.0223
2	12	8	11	0.0001	0.0204	0.0822	0.0236
3	13	11	12	0.0003	0.0182	0.1337	0.0262
4	9	8	12	0.0005	0.0183	0.1269	0.0261
5	9	9	12	0.0003	0.0165	0.1698	0.0288

For ANN-3, the scale and shape parameters are estimated to be 0.013 and 0.74 respectively. Assuming that a 2.5% false alarm rate is acceptable, the 97.5 percentile is considered as the threshold value, i.e. $\epsilon_3 = 0.078$.

Similarly, to study the performance of the AC-OPF detection algorithm under normal operation conditions, we run our simulation for hours 338 to hour 744. Figure 1.12 shows the time series of the sum of the squared errors. Eight false alarms are observed in Figure 1.12.

To study the performance of ANN-3 in detecting anomalies, the same attack scenarios mentioned in TABLE 1.12 are used. The detection results are provided in TABLE 1.12. The results show that the algorithm performance is highly satisfactory. The percentage of detection is greater than 95% under all scenarios.

Table 1.12: AC-OPF detection results in different cyber-attack scenarios

Scenario	% Detection of ANN-3 (AC-OPF Model)
A	95.0
B	95.0
C	98.5
D	99.0

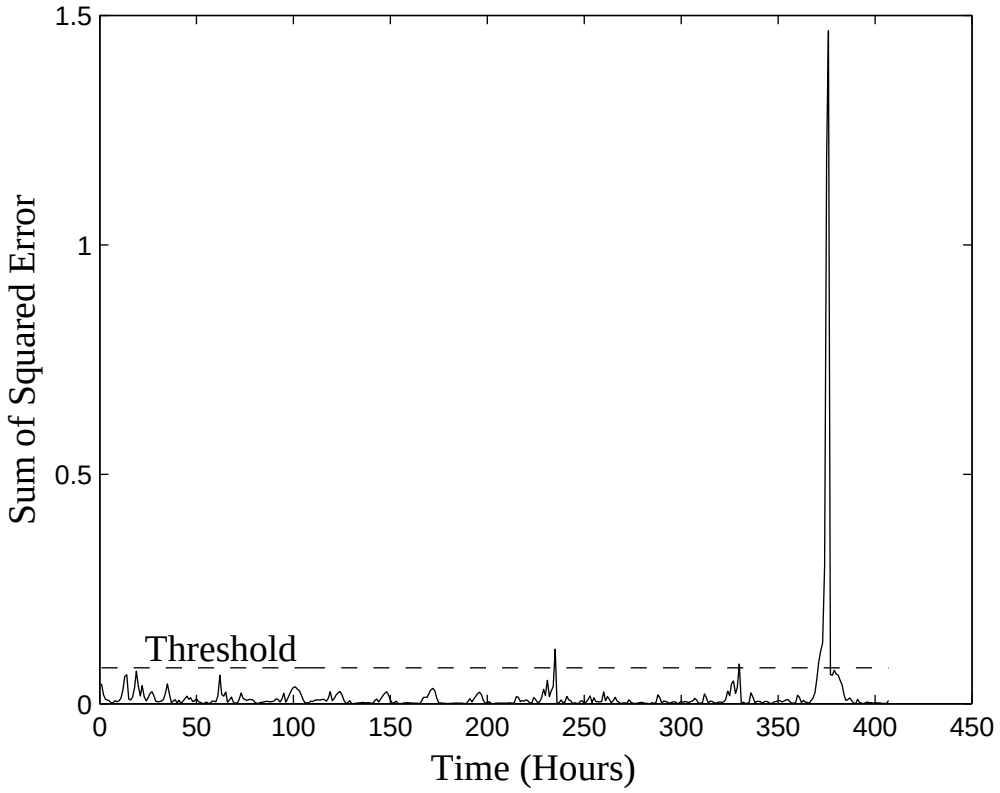


Figure 1.12: Plot of the ANN-3 false alarms

1.6.3 Computational Time Analysis

All experiments are performed on a 64-bit laptop with an Intel Core i5 2.4GHz processor and 4GB RAM. The training time of the artificial neural network and execution time of 100 replications of anomaly detections are given in TABLE 1.12.

Table 1.13: Training and Detection Computational Times

Artificial Neural Network	Training Time (s)	Detection Time (s)
ANN1	35.19	7.05
ANN2	17.53	10.55
ANN3	10.77	24.15

1.7 Conclusions

We have illustrated that cyber-attacks could be as dangerous as physical attacks to the power grid since they could cause major physical losses and damages. Current data cleansing methods are not powerful enough to detect all cyber-attacks. We have proposed an algorithm which uses artificial neural networks to detect cyber-attacks against the transmission network data of an electric power system, which is an additional security measure to the traditional state estimation software. An alarm from our algorithm would indicate that a parameter was changed deliberately.

We have used network observability rules to reduce the size of the inputs to the ANN while maintaining the critical variables. We have tested our algorithm in two software modules, DC-OPF and AC-OPF. We have simulated cyber-attacks by changing the parameters of components and transmission lines. The algorithm was able to detect 92 to 99.5% of the introduced anomalies with a small number of false alarms. The detection capability of the algorithm depends on how the altered parameters change transmission power flows. Although the algorithm is effective on detecting the presence of an anomaly in the system, it cannot identify, locate, or eliminate the anomaly.

The main obstacle for using the algorithm on a much larger power system is the computer processing time, which is highly depending on the number of input/output variables of the ANN. Fortunately, the ANN approach accepts parallel computing and can be easily implemented on a computer with multiprocessors. Certainly, more research needs to be done on studying the performance and the level of scalability of the proposed approach. However, the results from the 24-bus power system have shown that the algorithm is a promising tool for adding an extra level of cyber-security to a power system.

References

[1] S. Halilcevic, F. Gubina, and A. F. Gubina, "Prediction of power system security levels," *IEEE Transactions on Power Systems*, vol. 24, pp. 368–377, 2009.

[2] I. L.G.Pearson, "Smart grid cybersecurity for europe," *Energy Policy*, vol. 39, pp. 5211–5218, 2011.

[3] C. W. Ten, C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *IEEE Transactions on Power Systems*, vol. 23, pp. 1836–46, 2008.

[4] F. C. Schweppe and J. Wildes, "Power system static-state estimation, part i-iii," *IEEE Transactions on Powe*, vol. PAS-89, pp. 120–135, 1970.

[5] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, pp. 659–666, 2011.

[6] V. H. Quintana, A. Simoes-Costa, and M. Mier, "Bad data detection and identification techniques using estimation orthogonal methods," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-101, pp. 3356–3364, 1982.

[7] H. M. Merrill and F. C. Schweppe, "Bad data suppression in power system static state estimation," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-90, pp. 2718–2725, 1971.

[8] E. Handschin, F. C. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Transactions on Power Apparatus and Systems*, vol. 94, pp. 329–337, 1975.

[9] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Transactions on Power Systems*, vol. PP, no. 99, p. 1, 2012.

[10] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD, USA, 2010, pp. 226–231.

[11] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *16th ACM Conference on Computer and Communication Security*, Chicago, IL, USA, 2009.

[12] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. Marcel Dekker Inc., 2004.

[13] C. W. Ten, G. Manimaran, and C. C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 40, pp. 853–865, 2010.

[14] Z. C. Z and J. C. Maun, "Artificial neural network approach to single-ended fault locator for transmission lines," *IEEE Transactions on Power System*, vol. 15, pp. 370–375, 2000.

[15] A. G. Bakirtzis, J. B. Theocharis, S. J. Kiartzis, and K. J. Satsios, "Short term load forecasting using fuzzy neural networks," *IEEE Transactions on Power System*, vol. 10, pp. 1518–1524, 1995.

[16] K. Meng, Z. Y. Dong, D. H. Wang, and K. P. Wong, "A self-adaptive RBF neural network classifier for transformer fault analysis," *IEEE Transactions on Power System*, vol. 25, pp. 1350–1360, 2010.

[17] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation and Control*. John Wiley & Sons, 1996.

[18] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, pp. 12–19, 2011.

[19] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on the Smart Grid*, vol. 2, pp. 659–666, 2011.

[20] M. H. Beale, M. T. Hagan, and H. B. Demuth, *Neural Network Toolbox User Guide's*. The MathWorks, Inc, 2011.

[21] J. Peng, Y. Sun, and H. F. Wang, "Optimal pmu placement for full network observability using tabu search algorithm," *Electrical Power and Energy Systems*, vol. 28, pp. 223–231, 2006.

[22] Subcommittee, "IEEE reliability test system," *IEEE Transactions on Power Apparatus and Systems*, vol. 98, pp. 2047–2054, 1979.

[23] www.pjm.com.

Chapter 2

A Probabilistic Risk Mitigation Model for Cyber-Attacks to PMU Networks

2.1 Abstract

The power grid is becoming more dependent on information and communication technologies. Complex networks of advanced sensors such as PMUs are used to collect real time data to improve the observability of the power system. Recent studies have shown that the power grid has significant cyber vulnerabilities which could increase when PMUs are used extensively. Therefore, recognizing and responding to vulnerabilities are critical to the security of the power grid. This paper proposes a risk mitigation model for optimal response to cyber-attacks to PMU networks. We model the optimal response action as a mixed integer linear programming (MILP) problem to prevent propagation of the cyber-attacks and maintain the observability of the power system.

keywords: Cyber-attack, Phasor Measurement Units, Cyber-security, Networks, Observability

Nomenclature

Sets and Indices

Υ: Set of buses

Θ: Set of buses equipped with PMUs

Γ: Set of PMUs detected as compromised

Ψ: Set of buses with conventional devices

Ω: Set of branches with conventional devices

i, j, k: Indices of buses

Constants

M: Number of detected compromised PMUs

$H_{i,j}$: Connectivity between buses i and j

T_i: Threshold threat level (between 0 and 1) of PMU_i

D_{ij}: Nodal distance between PMU_i and PMU_j

Δt: Time that a propagation attempt takes

m: Number of Δt that the system operator takes to respond to the cyber-attack

Decision Variables

x_j: : Binary decision variable which equals 1 if PMU_j is kept connected to the network, and 0 otherwise

φ_i: Observability number, number of times that bus i is observed, which is ≥ 1 if bus i is observable

$y_{i,j}$: Binary variable which equals 1 if the measurement from the conventional device at bus j is assigned to compute the unknown voltage phasor of bus i, and 0 otherwise.

$\rho_{i,j}$: Binary variable which equals 1 if the measurement from the conventional device at transmission line $i-j$ is assigned to compute the unknown voltage phasor of bus i, and 0 otherwise.

Random Variables

$A_j(t)$: random variable which equals 1 if PMU_j is attacked, and 0 otherwise

Probabilities

α_{ij}: The probability that PMU_j is attacked through PMU_i

λ: The probability that an attack propagates through a router

γ: The probability that an attack propagates to a PMU through a router

$\theta_j(t)$: The threat level of PMU_j at time t

2.2 Introduction

The power grid is increasingly dependent on information and communication technologies due to the integration of intelligent measurement devices such as phasor measurement units (PMU). Smart grid investment grants and demonstration project investments have significantly accelerated the pace of phasor technology deployment [1]. According to [2], PMUs will ultimately replace conventional devices. PMUs can measure in real time synchronized phasors of bus voltages and currents for better observability of the power grid [3]. Synchronization is achieved by timing signals from the Global Positioning System (GPS) satellite. A PMU takes about 30 to 120 measurements per second and sends its measurements to a phasor data concentrator (PDC) through a wireless communication network based on the NASPInet architecture [4, 5]. In the NASPInet architecture, PMUs are connected to an IP-based communication network like an Intranet. Although the communication network is dedicated Intranet and isolated from public networks, it is not immune to cyber-attacks [6]. Currently, PMUs transmit their measurements to a pre-defined PDC in a hierarchical manner by using the IP Unicast routing protocol. However, hierarchical architectures suffer from drawbacks such as delays of messages. A technical report from CISCO proposes that PMUs should send measurements using the IP Multicast routing protocol [7]. Under this protocol, a PMU is directly connected to a router and sends out data packets to pre-configured destinations. The list of these predetermined destinations can be further manipulated by a cyber-attacker to propagate the cyber-attack to other PMUs. The propagation of the cyber-attacks in shared communication networks has been also studied in [8–13]. Furthermore, it has been reported that the communication network shows poor network security and insufficient software security [14]. Moreover, the authors in [15] studied the spoofing attack as an optimization problem to maximize the PMU's receiver clock offset before and after the attack. The authors in [16] mentioned that there is no available defense against GPS spoofing which is a threat to critical infrastructure applications such as PMUs that rely on the publicly known civilian GPS signal. Under these conditions, cyber-attackers could gain

access to the PMU communication network, inject false measurement data and propagate their cyber-attack to the other PMUs to endanger the reliability of the power grid.

Dealing with erroneous data has been a concern of state estimation programs since their inception in the late nineteen-sixties [17]. It is shown in [18] that sophisticated attacks may not be detected by conventional state estimation algorithms. Thus, the detection problem is considered to be challenging and several algorithms have been proposed. The authors in [19] presented a Principal Component Analysis (PCA) based approach to detect cyber-attacks in the optimal power flow (OPF) module. The authors in [20] showed how data attacks can endanger the physical structure of the power grid and developed a detection algorithm using the artificial neural networks. The authors in [21] have proposed new points of view to enrich the detection solutions such as modeling the dynamics of attacker versus defender. The authors in [22] developed greedy algorithms to obtain perfect protection and partial protection against stealth attacks given a limited budget for protection. In [23], the authors used the generalized likelihood ratio test to develop a computationally efficient detection algorithm where the cyber-attacker uses a graph theoretic approach to launch stealthy malicious data attacks. After the detection, actions need to be taken to prevent the propagation of the cyber-attack.

The authors of [13] have formulated an optimization model to avoid propagation of the cyber-attacks in open-science computer network where collaboration and communication exist among network sites. The optimization model is a mixed integer linear programming problem, which determines the sites to be disconnected from the network to maximize the number of users connected to the network resources. The decision is constrained to keep the threat levels of the sites below a certain threshold value. However, such a model cannot be directly applied to a PMU network as that model is focused more on maximizing the available connections on the network, which is not a priority for PMUs. Additionally, observability is not an issue in open-science computer networks.

In this paper, we propose an optimal response model to cyber-attacks to PMU networks where the state estimation principally relies on PMUs. Our model minimizes the threat levels by disabling known compromised PMUs and PMUs that are likely to be compromised due to the propagation of the cyber-attacks, while keeping the power system observable. Here, a threat level represents the probability of a PMU being contaminated at a certain time. We first use a probabilistic model to estimate the threat levels for PMUs and then formulate the optimal response as a mixed-integer linear programming problem. Here, a response stands for disconnecting the contaminated PMU buses to ensure the resultant PMU network is secure and the grid is observable.

The rest of this chapter is organized as follows: Section 2.3 describes threat level estimation. Section 2.4 explains our proposed optimization model. Experimental results are provided in Section 2.5 and the conclusions are reported in Section 2.6.

2.3 Estimating the Threat Levels

In this section, we calculate the threat levels of the uncompromised PMUs if an intruder were to attacked one or more PMUs. Propagation of the cyber-attack has been studied on the other networks. As a case in point, the authors in [24] and [25] considered worm propagation in mobile ad-hoc networks and energy meters in a secondary distribution network, respectively. Similarly in a PMU network, the intruder controls the attacked PMUs which can be used to transmit false measurements. Moreover, the intruder can use the communication links between PMUs to disseminate the attack to the other PMUs via the compromised PMUs. If the attack propagates to more PMUs, it could jeopardize the observability of the power system even further. The attack could propagate via all routers between the compromised and uncompromised PMUs to contaminate the uncompromised PMUs.

Let us assume at time $t = 0$, M PMUs are detected to be compromised while the remaining PMUs are uncompromised. It takes time Δt to disable the compromised PMUs from the communication network. Naturally, their measurements will no longer be used for

the state estimation software. Disabling PMUs can be done automatically by the detection software or manually by the system operator. During this time, there is a chance that the attack could have been propagated to uncompromised PMUs and the detection software has not detected them yet. The reason is that the detection software cannot detect at 100% efficiency [21]. The cyber-attack can propagate to uncompromised PMUs through a path of interconnected routers. If the cyber-attack successfully breaks into all routers between the compromised and uncompromised PMUs, it is likely to contaminate the uncompromised PMUs as well. Moreover, these new compromised PMUs can further infect other PMUs, and so forth. We represent by the probability, $\theta_j(t)$, the likelihood of a PMU being compromised (also called threat level) at time t. Notice that the threat levels increase over time as long as the network still contains compromised PMUs. It takes a time period of $m\Delta t$ for the system operator to run the optimization model to obtain the optimal response and confirm that the alarm is not a false alarm. Thus, certain PMUs, determined by the optimization model, are disabled at time $(m+1)\Delta t$.

At time $t = 0$, equations (2.1) and (2.2) hold.

$$\Pr(A_j(0) = 1) = 1 \qquad \forall j \in \Gamma \tag{2.1}$$

$$\Pr(A_j(0) = 1) = 0 \qquad \forall j \notin \Gamma \tag{2.2}$$

By time Δt, all compromised PMUs are disabled. However, due to the possible propagation of the cyber-attack, there is a chance that the remaining PMUs could have been compromised and undetected. Therefore at time Δt, equations (2.3) and (2.4) hold.

$$\Pr(A_j(\Delta t) = 1) = 0 \qquad \forall j \in \Gamma \tag{2.3}$$

$$\Pr(A_j(\Delta t) = 1) = 1 - \prod_{i \in \Gamma}(1 - \alpha_{ij}) \qquad \forall j \notin \Gamma \tag{2.4}$$

where α_{ij} is the probability that the attack propagates from compromised PMU_i to an uncompromised PMU_j during the time Δt, and it is given by equation (2.5).

$$\alpha_{ij} = \gamma \lambda^{D_{ij}} \qquad i \in \Gamma,\ j \notin \Gamma \tag{2.5}$$

In equation (2.5), λ is the probability that an attack propagates through a router, γ is the probability that an attack propagates to another PMU and D_{ij}, called nodal distance, is the minimum number of routers that connect PMU_i and PMU_j on the communication network. It is likely that there are multiple shortest paths between two PMUs in a large communication network. In this case, the value of α_{ij} would increase and would be given by equation (2.6).

$$\alpha_{ij} = 1 - (1 - \gamma \lambda^{D_{ij}})^{N_{ij}} \tag{2.6}$$

Where N_{ij} is the number of shortest paths between PMU_i and PMU_j. There may be other paths in addition to the shortest paths. Considering that it may not be simple to find all paths between every two PMUs, and that the probability α_{ij} decreases exponentially when the distance increases, we use equation (2.6) to estimate the probability that the attack propagates from one PMU to another. This function indicates that the propagation becomes less probable when the nodal distance between the two PMUs becomes larger.

We have stated that it takes time Δt to disable the compromised PMUs. If, during $m\Delta t$, the system operator concludes that the alarm is false, the disabled PMUs would be enabled again. Otherwise, the operator would begin disabling the PMUs as determined by the optimization model discussed in the next section at $m\Delta t$ and all contaminated PMUs would be disabled by time $(m+1)\Delta t$. Thus, we need to calculate the threat levels at time $(m+1)\Delta t$. Since the threat levels are calculated in an iterative process, we need to calculate

the threat levels at time $2\Delta t$, $3\Delta t$, ..., $n\Delta t$. Equations (2.7) and (2.8) hold at time $2\Delta t$.

$$\begin{aligned}
\Pr(A_j(2\Delta t)=1) &= 0 \qquad\qquad \forall j \in \Gamma \qquad (2.7)\\
\Pr(A_j(2\Delta t)=1) &= \Pr\{(A_j(2\Delta t)=1 | A_j(\Delta t)=0\} \\
&\times \Pr\{A_j(\Delta t)=0\} \\
&+ \Pr\{(A_j(2\Delta t)=1 | A_j(\Delta t)=1\} \\
&\times \Pr\{A_j(\Delta t)=1)\} \qquad \forall j \notin \Gamma \qquad (2.8)
\end{aligned}$$

In equation (2.8), we have expressions for all terms except for $\Pr\{(A_j(2\Delta t)=1 | A_j(\Delta t)=0\}$, which can be obtained from equation (2.9).

$$\begin{aligned}
&\Pr\{A_j(2\Delta t)=1 | A_j(\Delta t)=0\} = \\
&1 - \Pr\{A_j(2\Delta t)=0 | A_j(\Delta t)=0\} = \\
&1 - \prod_{\substack{k,j\notin\Gamma \\ k\neq j}} (1 - \Pr(A_k(\Delta t)=1) \times \alpha_{kj}) \qquad j,k \in \Theta \qquad (2.9)
\end{aligned}$$

We denote $\Pr(A_j(t)=1)$ by $\theta_j(t)$. Therefore, we can rewrite equation (2.8) as equation (2.10) in terms of threat levels.

$$\theta_j(2\Delta t) = \left(1 - \prod_{\substack{k,j\notin\Gamma \\ k\neq j}} (1 - \theta_k(\Delta t) \times \alpha_{kj})\right) \times (1 - \theta_j(\Delta t)) + 1 \times \theta_j(\Delta t) \qquad j,k \in \Theta \qquad (2.10)$$

It can be shown that equation (2.11) is true when $n \geq 2$ and can be used to calculate threat levels for time $2\Delta t$ and further.

$$\begin{aligned}
\theta_j(n\Delta t) &= \left(1 - \prod_{\substack{k,j\notin\Gamma \\ k\neq j}} (1 - \theta_k((n-1)\Delta t) \times \alpha_{kj})\right) \times \left(1 - \theta_j((n-1)\Delta t)\right) + \theta_j((n-1)\Delta t) \\
&= 1 - \left(\prod_{\substack{k,j\notin\Gamma \\ k\neq j}} (1 - \theta_k((n-1)\Delta t) \times \alpha_{kj})\right) \times (1 - \theta_j((n-1)\Delta t) \qquad j,k \in \Theta \qquad (2.11)
\end{aligned}$$

If another cyber-attack is detected by time $(m+1)\Delta t$, the fundamental change due to the new attack is the change on set Γ, meaning that the set of the detected compromised PMUs is adjusted to include the new detected PMUs. In this case, the threat levels after the new cyber-attack are re-calculated by setting the initial threat levels to the threat levels of the previous attack. This is, if the second detection occurs at time $S = n\Delta t$ and $1 \leq n \leq (m+1)$:

$$\theta_{j,new-attack}(0) = \theta_{j,old-attack}(n\Delta t) \qquad \forall j \notin \Gamma \tag{2.12}$$

In the next step, equation (2.11) will be used to update the threat levels after time $S = n\Delta t$.

2.4 Response Model

The response to cyber-attacks to a PMU network is modeled using mixed integer linear programming. The objective function of the model is the minimization of the maximum threat level of all connected PMUs at time $(m+2)\Delta t$, which is one Δt after disabling the PMUs determined by the model. The threat levels from time $t = 0$ to $t = (m+2)\Delta t$ are summarized in equations (2.13)-(2.19).

$$\theta_j(0) = 1 \qquad \forall j \in \Gamma \tag{2.13}$$

$$\theta_j(0) = 0 \qquad \forall j \notin \Gamma \tag{2.14}$$

$$\theta_j(\Delta t) = 0 \qquad \forall j \in \Gamma \tag{2.15}$$

$$\theta_j(\Delta t) = 1 - \left(\prod_{i \in \Gamma}(1 - \alpha_{ij})\right) \qquad \forall j \notin \Gamma \tag{2.16}$$

$$\theta_j(n\Delta t) = 0 \qquad \forall j \in \Gamma;\ 2 \leq n \leq m+2 \tag{2.17}$$

$$\theta_j(n\Delta t) = 1 - \left(\prod_{\substack{k, j \notin \Gamma \\ k \neq j}} (1 - \theta_k((n-1)\Delta t)\alpha_{kj})\right)$$

$$\times (1-\theta_j((n-1)\Delta t) \qquad \forall j,k \notin \Gamma; 2 \leq n \leq m+1 \tag{2.18}$$

$$\theta_j\Big((m+2)\Delta t\Big) = 1 - \Bigg(\prod_{\substack{k,j \notin \Gamma \\ k \neq j}} (1-\theta_k((m+1)\Delta t)\alpha_{kj}x_k) \Bigg)$$

$$\times (1-\theta_j((m+1)\Delta t)) \qquad\qquad \forall j,k \notin \Gamma \tag{2.19}$$

Notice the presence of the binary decision variable x_k in equation (2.19), which equals 1 if the PMU_k is kept connected to the network, and 0 otherwise. It should be also noted that threat levels from time $t = 0$ to $t = (m+1)\Delta t$ are all assumed to be constants, and the system operators cannot decrease them due to the physical constraints such as control and communication delays in disabling PMUs from the network. However, disabling of suspicious PMUs occurs at time $(m+1)\Delta t$, which decreases the threat levels of the remaining PMUs at time $(m+2)\Delta t$. In fact, the response optimization model determines which PMUs should be disabled such that the threat levels at time $(m+2)\Delta t$ are minimized.

To be able to solve the response model more efficiently, we reformulate equation (2.19) by an equivalent linear equation (2.20).

$$\ln\{1-\theta_j\Big((m+2)\Delta t\Big)\} = \sum_{\substack{j,k \notin \Gamma \\ k \neq j}} \ln(1-\theta_k\Big((m+1)\Delta t\Big)\alpha_{kj})x_k + \ln\{1-\theta_j\Big((m+1)\Delta t\Big)\} \quad \forall j \notin \Gamma \tag{2.20}$$

In obtaining equation (2.20), we have used the following equality where K is a constant (notice again that x_i is a binary variable).

$$\ln(1-Kx_i) = x_i \times \ln(1-K) \tag{2.21}$$

The objective function of the response model is the minimization of the maximum threat of all connected PMUs at time $(m+2)\Delta t$.

$$Z = \min_{\mathbf{x}} \max_{j} (\theta_j\Big((m+2)\Delta t\Big) \times x_j) \qquad \forall j \notin \Gamma \tag{2.22}$$

Since $\theta_j((m+2)\Delta t)$ and consequently the objective function are not linear, we used its equivalent function given in equation (2.23), which can be reformulated linearly in equations (2.24)-(2.29).

$$Z = \min_{\mathbf{x}} \max_{j} \left\{ -\ln[1-\theta_j\Big((m+2)\Delta t\Big)] \times x_j \right\} \ \forall j \notin \Gamma \tag{2.23}$$

Equation (2.23) can be represented by the following set of equations (2.24)-(2.29).

$$Z = \min Y \tag{2.24}$$

Subject to:

$$w_j \leq x_j \qquad \forall j \notin \Gamma \tag{2.25}$$

$$w_j \leq -\ln\left[1-\theta_j\Big((m+2)\Delta t\Big)\right] \qquad \forall j \notin \Gamma \tag{2.26}$$

$$w_j \geq -\ln\left[1-\theta_j\Big((m+2)\Delta t\Big)\right] - (1-x_j) \quad \forall j \notin \Gamma \tag{2.27}$$

$$w_j \geq 0 \qquad \forall j \notin \Gamma \tag{2.28}$$

$$w_j \leq Y \qquad \forall j \notin \Gamma \tag{2.29}$$

In the response model, we used equation (2.20) in equations (2.26)-(2.27) to obtain equivalent linear equations. Hence, equations (2.26)-(2.27) can be represented as equations (2.30)-(2.31), respectively.

$$w_j \leq -\sum_{\substack{j,k\notin\Gamma \\ k\neq j}} \ln(1-\theta_k((m+1)\Delta t)\alpha_{kj})x_k - \ln\{1-\theta_j((m+1)\Delta t)\} \qquad \forall j \notin \Gamma \tag{2.30}$$

$$w_j \geq -\sum_{\substack{j,k\notin\Gamma \\ k\neq j}} \ln(1-\theta_k((m+1)\Delta t)\alpha_{kj})x_k - \ln\{1-\theta_j((m+1)\Delta t)\} - (1-x_j) \quad \forall j \notin \Gamma \tag{2.31}$$

We add equation (2.32) to keep PMUs with threat levels less than a threshold value connected to the network.

$$\theta_j((m+2)\Delta t) > T_j - x_j \qquad \forall j \notin \Gamma \tag{2.32}$$

which can be represented by:

$$\ln[1-\theta_j\Big((m+2)\Delta t\Big)] < \ln[1-T_j+x_j] \qquad \forall j \notin \Gamma \tag{2.33}$$

We can reformulate the right-hand side to a linear equivalent equation as:

$$\ln[1-\theta_j\Big((m+2)\Delta t\Big)] < (1-x_j)\ln(1-T_j) + x_j \ln(2-T_j) \qquad \forall j \notin \Gamma \tag{2.34}$$

Using equation (2.20), equation (2.34) can be represented linearly as equation (2.35).

$$\begin{aligned} &\sum_{\substack{j,k\notin\Gamma \\ k\neq j}} \ln(1-\theta_k((m+1)\Delta t)\alpha_{kj})x_k + \ln\{1-\theta_j((m+1)\Delta t)\} \\ &\quad < (1-x_j)\ln(1-T_j) + x_j \ln(2-T_j) \qquad \forall j \notin \Gamma \end{aligned} \tag{2.35}$$

Disabling PMUs may affect the observability of the system, so there should be a set of constraints to ensure full observability. To have a full observable power system, the voltage phasors (state variables) of all buses need to be known. The values of the voltage phasors allow the calculation of all other variables such as current, real power, and reactive power.

Hence, the observability function is given in equation (3.2) [26].

$$\varphi_i = \sum_{j\in\Theta} H_{i,j}x_j + \sum_{j\in\Psi} H_{i,j}y_{i,j} + \sum_{\{i,j\}\in\Omega} H_{i,j}\rho_{i,j} \qquad \forall i \in \Upsilon \tag{2.36}$$

Where $H_{i,j}$ shows the connectivity between buses i and j. The first term of the right hand side, $\sum_{j\in\Theta} H_{i,j}x_j$, provides observability of the buses through the remaining connected PMUs; the second term, $\sum_{j\in\Psi} H_{i,j}y_{i,j}$, calculates the observability of the buses through conventional devices installed at buses, and the third term, $\sum_{\{i,j\}\in\Omega} H_{i,j}\rho_{i,j}$, represents the observability through conventional devices installed on branches. To guarantee the full observability, the observability variable value should be greater than or equal to one as given in (2.37).

$$\varphi_i \geq 1 \qquad \forall i \in \Upsilon \tag{2.37}$$

Conventional devices are used to observe a group of buses when they are not observable by PMUs direct measurements. In such cases, a system of equations is solved to obtain the unknown state variables. To guarantee the solvability of the system of equations, we need to ensure that each conventional measurement is tied to one state variable [26]. Hence, equations (2.38)-(2.39) need to be met. Equation (2.38) ensures that a conventional voltage measurement is tied to one state variable and equation (2.39) ensures that a conventional current measurement is tied to one state variable. When the system is under attack, measurements of the conventional devices may be more reliable because the attacker needs to have complete knowledge of system topology and considerable resources in order to consistently manipulate conventional measurements. Thus, we use equation (2.40) to force the measurements of conventional devices to observe more buses.

$$\sum_{i\in\Upsilon} H_{i,j}y_{i,j} = 1 \qquad \forall j \in \Psi \tag{2.38}$$

$$\rho_{i,j} + \rho_{j,i} = H_{i,j} \qquad \forall \{i,j\} \in \Omega \tag{2.39}$$

$$\sum_{j\in\Psi} H_{i,j}y_{i,j} + \sum_{\{i,j\}\in\Omega} H_{i,j}\rho_{i,j} \leq 1 \qquad \forall i \in \Upsilon \tag{2.40}$$

where $\rho_{i,j}$ is a binary variable which equals 1 if the state variable of bus i is computed by a conventional device at branch i, j, and 0 otherwise. Finally, equation (2.41) determines that the decision variables are binary.

$$x_i,\ y_{i,j},\ \rho_{i,j} \in \{0, 1\} \tag{2.41}$$

To summarize, the objective function given in equation (2.22) determines the PMUs to be disabled from the network such that the maximum threat level of the PMUs still connected to the network is minimized. If the threat level of a PMU exceeds the threshold value, the objective function would disable that PMU from the network only if it does not affect the observability. If the threat level of a PMU is less than the threshold value, the PMU is kept connected to the network. This is guaranteed by equation (2.32). Finally, equation (3.2) ensures that all buses are observable at least once by either PMUs or conventional devices. The proposed response model is given by the following mixed integer linear programming problem.

$$Z = \min Y \tag{2.42}$$

Subject to the constraints given in:

Equations (2.13)-(2.18)

Equation (2.25)

Equations (2.28)-(2.29)

Equations (2.30)-(2.31)

Equation (2.35)

Equations (3.2)-(2.41)

Finally, it is important to notice that the cyber-attack could involve blocking the communication to and from the PMUs, which may prevent the disabling of the compromised PMUs after detection. This situation is less likely to occur because the intruders would want to be undetected and a fault in the communication network would alert the system operators immediately. Nevertheless, if the communication is blocked, the PMUs would be isolated from the communication network, which has the same effect as disabling the compromised PMUs. The measurements would not be used by the state estimation software, and there would be no propagation of the cyber-attack to other PMUs.

2.5 Experimental Results

We test the performance of our response optimization model on the 6-bus and 24-bus test systems introduced in [27] and [28], respectively. We use the small power system to describe the cyber-attack propagation problem and our methodology. We use the middle size power system to test our approach. This power system includes conventional devices. We intentionally consider a few conventional devices because we want to show the use of our optimization response model where PMUs are the main devices for power system state estimation.

In our experiments, we assume that an attack to a PMU propagates through a router with probability $\lambda = 0.05$, and it effectively compromises another PMU with probability $\gamma = 0.05$. For simplicity, we also assume that there is only one shortest path between PMUs. We set $N_{ij} = 1$. We set Δt to 0.1 seconds, $\Delta t = 0.1$(s), and the threshold values to 0.005, $T_i = 0.005$. In a real case, experiments can be conducted to estimate the values of these parameters. Experimental network infrastructures such as the Virtual Network Infrastructure (VINI), X-Bone, and Violin can be used to run these experiments with real traffic and routing software [29].

2.5.1 6-bus Test System

The 6-bus test system includes six buses, three generators and eleven transmission lines. Figure 2.1 shows the 6-bus test system.

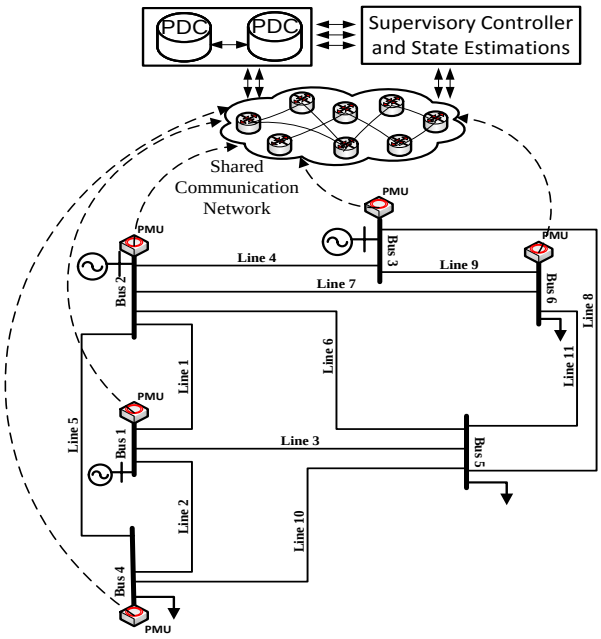


Figure 2.1: The 6-bus Test System

Buses 1, 2, 3, 4 and 6 are equipped with PMUs which make the system fully observable. Phasor measurements such as voltage magnitudes and voltage angles are transmitted to the PDCs by the five PMUs through a digital communication network. The communication network is depicted in Figure 2.1 and it consists of interconnected routers.

TABLE 2.1 shows the nodal distances between the PMUs installed in the 6-bus test system. Notice that the greater the nodal distance between two PMUs, the less likely that the cyber-attack can propagate from one PMU to another one.

For this case study, we assume that at time $t = 0$ the system operator is informed that PMU_1 and PMU_3 have been attacked by a cyber-intruder. In Figure 2.2, we show the threat levels of the three uncompromised PMUs over time when the system operator does not disable the compromised PMUs from the network. Notice that the threat levels increase

Table 2.1: Nodal distances between PMUs in the 6-bus test system

Bus	1	2	3	4	6
1	0	2	3	1	2
2	2	0	3	3	2
3	3	3	0	1	2
4	1	3	1	0	3
6	2	2	2	3	0

Table 2.2: Candidate responses for the 6-bus test system

PMU	**Candidate Response**							
Status	1	2	3	4	5	6	7	8
x_2	1	1	1	1	0	0	0	0
x_4	1	0	0	1	1	0	1	0
x_6	1	1	0	0	1	1	0	0
Threat Levels								
θ_2	0.00013	0.00013	0.00013	0.00013	0	0	0	0
θ_4	0.00500	0	0	0.00500	0.00500	0	0.00500	0
θ_6	0.00025	0.00025	0	0	0.00025	0.00025	0	0
Max(θ_j)	0.00500	0.00025	0.00013	0.00500	0.00500	0.00025	0.00500	0
Observaiblity	Yes	Yes	Yes	Yes	Yes	No	No	No

non-linearly until all PMUs become compromised with probability 1. PMU_4 is more at risk because it is closer to the compromised PMUs. The nodal distance from PMU_3 to PMU_4 is 1 while to PMU_2 is 3. Figure 2.3 illustrates the effect of the value of λ on the threat level of PMU_2.

To avoid propagation, the system operator should disable the compromised PMU_1 and PMU_3 and other PMUs which may be compromised because of the propagation. There are

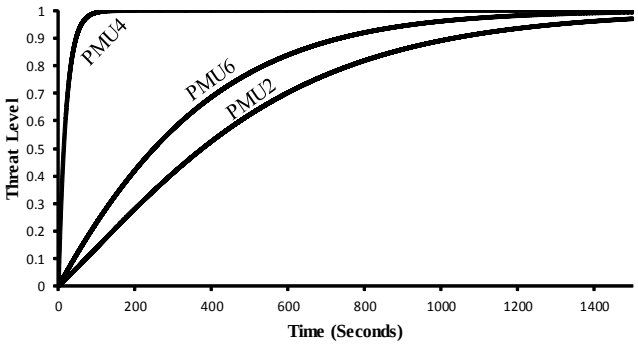


Figure 2.2: Threat levels in case of no response action

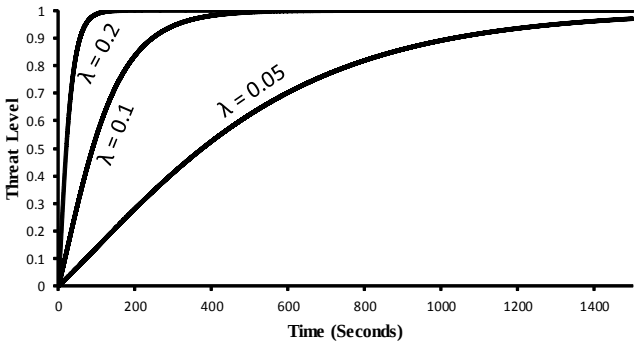


Figure 2.3: Effect of λ on threat level of PMU_2

eight possible choices which are shown in TABLE 2.2. The smallest threat levels can be obtained when all PMUs are disabled. However, this solution is not feasible since the power system would no longer be observable. The second candidate is to disable PMU_4 and PMU_6 but the threat level of PMU_6 is less than the threshold value, $T_6 = 0.005$, and therefore it should remain connected to the network. The third candidate is to disable PMU_4. This action keeps the power network observable and minimizes the maximum threat level of all connected PMUs. In TABLE 2.3, we give the optimal solution, observability number of the buses obtained from equation (3.2), and the threat level of each connected PMU right after disabling PMU_4.

Table 2.3: Optimal response action in the 6-bus system

PMU	x_j	Observability number(ϕ_i)	Threat level($\theta_j(3\Delta t)$)
1	0	1	0
2	1	2	0.00013
3	0	2	0
4	0	1	0
5	NA	2	NA
6	1	2	0.00025

We show in Figure 2.4 the maximum threat level of the connected PMUs when just the compromised PMU_1 and PMU_3 are disabled and when PMU_4 is also disabled from

the network. Notice that the threat levels still increase after the response. However, the reduction in threat levels is considerable if the optimal response action is taken.

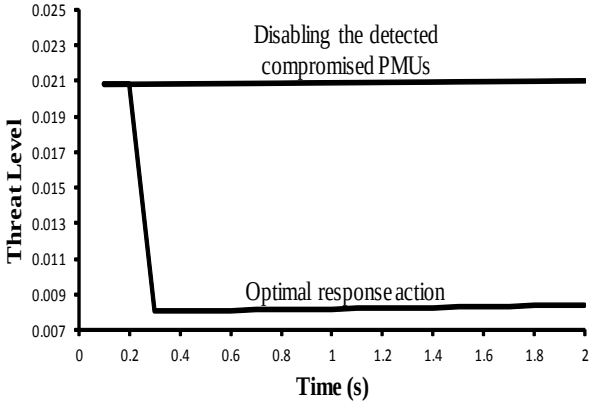


Figure 2.4: Comparison of two potential responses

We have assumed that the optimization results are obtained in 0.1 seconds. To see the effect of greater computational time, we consider that the optimal results are available at times 0.1, 2, and 5 seconds. In all of these cases, the optimal solution is to disable PMU_4. In Figure 2.5, we show the threat level for each case. Certainly, a shorter processing time is desired.

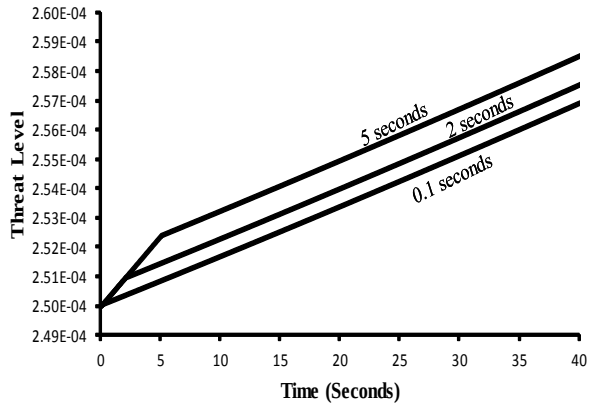


Figure 2.5: Effect of computational time on threat level of PMU_6

2.5.2 24-bus Test System

The proposed response model is tested using the IEEE 24-bus test system which consists of 38 transmission lines, 24 buses and 33 generators. The 24-bus test system is shown in Figure 2.6. We refer the readers to [28] and [30] for additional system data.

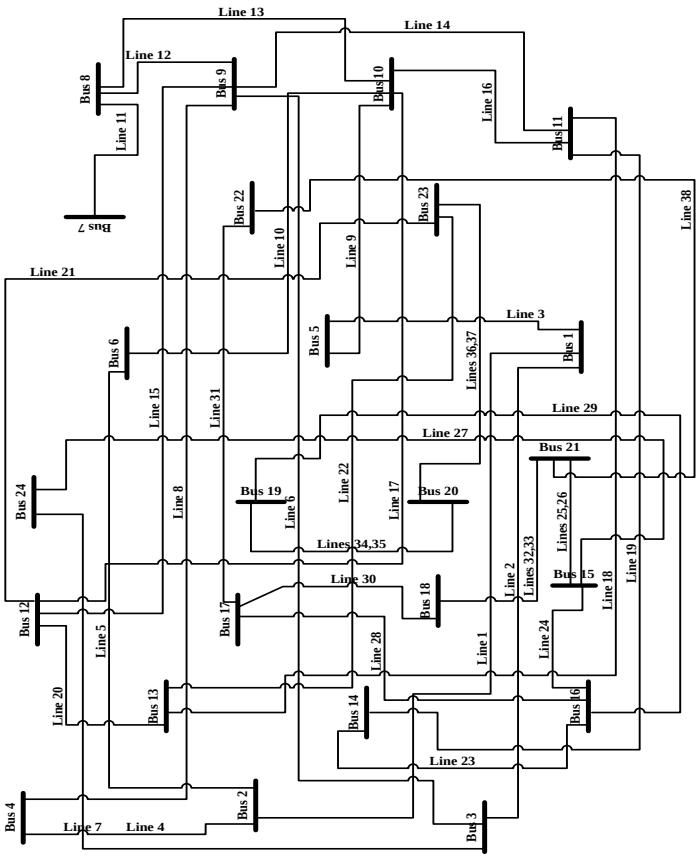


Figure 2.6: IEEE 24-bus Test System

We use the optimal placement of seven PMUs given in [31] and add seven more PMUs and five conventional measuring devices to increase the observability of the power system. The PMUs are located at buses 1, 2, 3, 4, 8, 10, 11, 15, 16, 17, 21, and 23 and the conventional units are located at buses 1, 19, 22 and transmission lines 9 and 17. The initial observability of the buses is given in TABLE 2.4. TABLE 2.5 gives PMUs' nodal distances randomly generated between 1 and 4.

Table 2.4: Initial observabilites of the 24-bus system

Bus	Observability	Bus	Observability	Bus	Observability	Bus	Observability
1	3	7	2	13	2	19	2
2	3	8	3	14	2	20	3
3	3	9	4	15	3	21	2
4	2	10	3	16	3	22	3
5	3	11	2	17	2	23	2
6	2	12	3	18	2	24	2

Table 2.5: Nodal distances between PMUs in the 24-bus test system

PMU Locations	1	2	3	4	7	8	10	11	15	16	17	20	21	23
1	0	1	2	1	2	4	4	2	3	4	1	2	3	2
2	1	0	3	3	2	1	3	2	4	3	3	3	1	3
3	2	3	0	2	1	4	2	3	1	3	3	2	1	2
4	1	3	2	0	3	1	2	2	3	4	3	3	1	1
7	2	2	1	3	0	1	3	1	1	4	1	4	2	3
8	4	1	4	1	1	0	2	3	1	1	1	2	3	2
10	4	3	2	2	3	2	0	4	4	2	3	1	2	2
11	2	2	3	2	1	3	4	0	2	2	3	2	4	1
15	3	4	1	3	1	1	4	2	0	4	1	2	2	4
16	4	3	3	4	4	1	2	2	4	0	1	4	1	1
17	1	3	3	3	1	1	3	3	1	1	0	3	4	4
20	2	3	2	3	4	2	1	2	2	4	3	0	3	3
21	3	1	1	1	2	3	2	3	2	1	4	3	0	1
23	2	3	2	1	3	2	2	1	4	1	4	3	1	0

First, we assume that just one PMU is compromised at time zero. We consider two cases to show the propagation effect of the cyber-attack. We assume: a) PMU_7 is compromised and b) PMU_{20} is compromised at time zero. In both cases, it is assumed that the compromised PMU stays connected to the network (no response action). Figure 2.7 shows the threat levels of a selected group of PMUs, PMUs 4, 10 and 15, under case (a) while Figure 2.8 shows the threat level for the same PMUs under case (b). Notice that PMU_{10} is less affected by a cyber-attack to PMU_7 but it is considerably affected if the attack occurs on PMU_{20}.

Next, we study the effect of simultaneous cyber-attacks. We assume that PMUs 1, 3, 7 and 10 are compromised at time zero and they remain connected to the network (no response action). Figure 2.9 illustrates the threat level of PMU_4 under a single attack to PMU_7 and

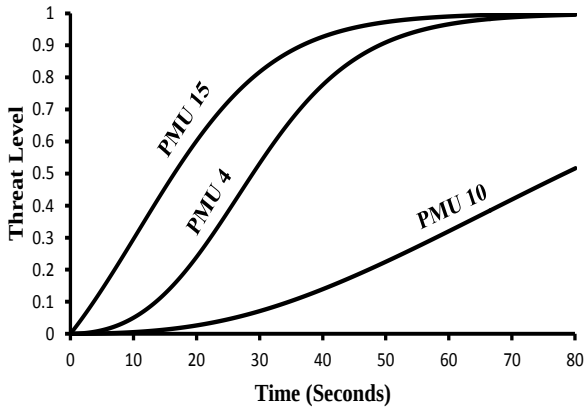


Figure 2.7: Threat levels for no response to compromised PMU_7

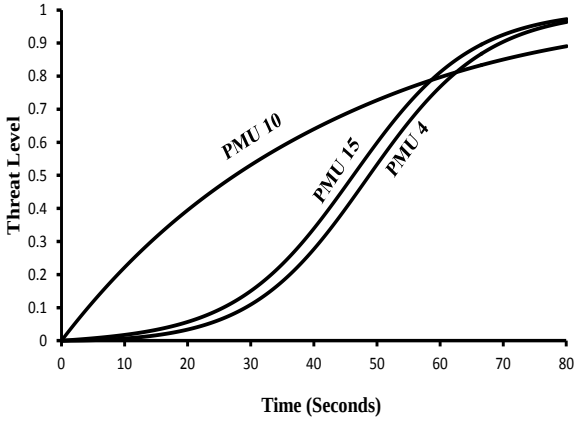


Figure 2.8: Threat levels for no response to compromised PMU_{20}

the multiple attacks. Notice the increase on the threat level of PMU_4 under a multiple attack.

To show the effect of the computational time $m\Delta t$ (time to obtain the optimal response) on the threat levels, we use the multiple attacks case. We change the value of m from 1 to 700, i.e. the time that the system operator takes to respond to the cyber-attack varies from

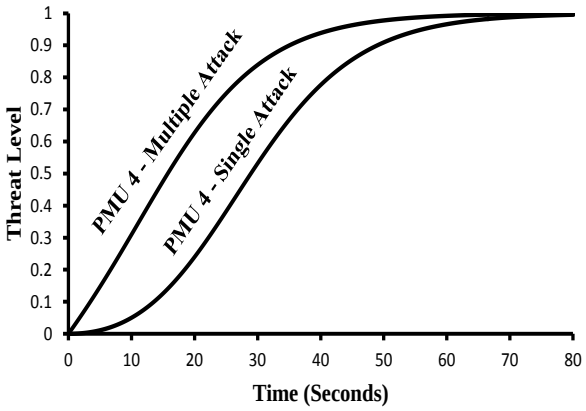


Figure 2.9: Effect of single and multiple attacks on threat levels

0.1 to 70 seconds. We obtain the optimal response for each value of m. The results are given in TABLE 2.6.

Table 2.6: Effect of response time on the optimal solution in case of multiple attacks

Case	Response time (s)	Disabled PMUs
S1	$m\Delta t \leq 8.9$	1, 3, 7, 10, 17
S2	$9.0 \leq m\Delta t \leq 10.8$	1, 3, 4, 7, 10, 17
S3	$10.9 \leq m\Delta t \leq 12.7$	1, 3, 4, 7, 10, 16, 17
S4	$12.8 \leq m\Delta t \leq 70.0$	1, 3, 4, 7, 10, 16, 17, 23
S5	$m\Delta t \geq 70.0$	Not Feasible

In Figure 2.10, we show the maximum threat level of the system (objective function of the optimization problem) when only the compromised PMUs are disabled from the network and when the optimal response is implemented. The figure shows the results under different response times. Notice that when the proposed model is used the maximum threat level is reduced for all response times considered. The reduction increases as the response time increases.

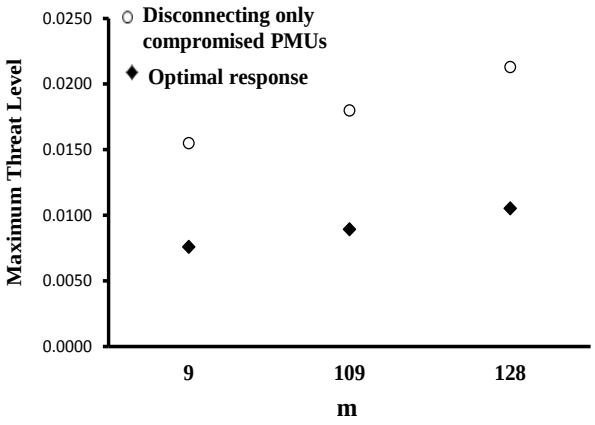


Figure 2.10: Maximum threat levels for two potential responses

2.5.3 Dealing with Large Power Systems

Since the main contribution of the paper is the formulation of the MILP and the modeling of the probabilistic threat levels, we demonstrated our approach using a small and a medium size power system. All experiments were performed on a 64-bit laptop with an Intel Core i5 2.4 GHz processor and 4GB RAM. The computation time consists of two components, the threat level calculation and the optimization time. For the experiment on the IEEE 24-bus test system, the threat level calculations using MATLAB R2012a took 6.95 seconds and the optimization using the optimization software LINGO 11.0 took 1 second.

It is known that MILP solvers suffer from the curse of dimensionality and therefore waiting to obtain the optimal solution for a larger power system can threaten the security of the power system more severely. However, considering that a single cyber-attack is more likely to occur, the proposed model can be run offline for all possible single attacks. The system operator would already know the optimal response when a single attack occurs in the network. In TABLE 2.7, we show the optimal responses within 20 seconds for all single attacks to a PMU on the 24-bus test system. This approach, however, would not work for multiple attacks due to the numerous possible combinations of cyber-attacks to PMUs. In

Table 2.7: Optimal response for single cyber-attacks to the 24-bus test system

Compromised PMU	PMUs to be disabled	Compromised PMU	PMUs to be disabled
1	1, 4, 8, 16, 17	11	7, 11
2	1, 2, 8, 16, 21	15	4, 8, 15, 16, 17
3	3, 7, 16, 17	16	4, 8, 15, 16, 17, 23
4	1, 4, 8, 16, 21, 23	17	1, 2, 8, 15, 16, 17, 23
7	4, 7, 15, 16, 17	20	20
8	1, 2, 15, 16, 17, 23	21	1, 4, 8, 16, 21, 23
10	10	23	4, 8, 16, 21, 23

this case, the optimization software can be stopped at a predetermined time. A trade-off has to be made between the closeness of the obtained solution at the predetermined time to the optimal solution and the increase of the threat levels over that time.

2.5.4 Discussion

We have developed a response optimization model to a cyber- attack to power systems that rely heavily on PMUs for the state estimation. Thus, the proposed model becomes more beneficial as the ratio of PMUs to conventional devices increases. It is expected that in the near future, as PMUs become widespread, the state estimation process will be more influenced by PMU measurements.

The proposed model disables PMUs restricted to secure system observability. However, pseudo measurements that are used to handle measurement unavailability in conventional state estimation could be also used to remove additional PMUs at the cost of loss of observability. This feature can be incorporated to our model by adding a set of new constraints.

Furthermore, if information from a detection scheme is available it can serve as an input to our model. For example, given the estimation on the likelihood of infection of all uncompromised PMUs at the time of the detection of the cyber-attack, the initial threat level of uncompromised PMUs, $\theta_j(0)$, can be set to this value. For the sake of simplicity, in our experiments we assume that no information comes from the detection software and therefore all initial threat levels are set to zero.

2.6 Conclusions

Observability of the power system is important for grid operation and control. An attacker could design a cyber-attack to PMUs that endangers the observability of the power system. We showed that in addition to disabling the compromised PMUs, other PMUs should also be disabled to reduce the probability of propagation of the cyber-attack. We developed a mixed integer linear programming model to determine the PMUs that should be disabled under the restriction that the remaining PMUs continue to maintain the observability of the power system. The model minimizes the maximum threat level of the PMUs that remain connected to the network. We have shown experimental results for two power systems. The results in both cases demonstrated a significant reduction in the propagation of the cyber-attacks when the solution obtained by the optimization model is implemented.

References

[1] (2010, October) Real-time application of synchrophasors for improving reliability. North American Electric Reliability Corporation (NERC). [Online]. Available: https://www.naspi.org/File.aspx?fileID=519

[2] H. Lin, Y. Deng, S. Shukla, J. Thorp, and L. Mili, "Cyber security impacts on all-PMU state estimator - a case study on co-simulation platform GECO," in *IEEE SmartGrid-Comm Symposium - Wide Area Protection and Control (WAMPAC)*, 2012.

[3] D. Dua, S. Dambhare, R. K. Gajbhiye, and S. A. Soman, "Optimal multistage scheduling of PMU placement: An ILP approach," *IEEE Transactions on Power Delivery*, vol. 23, pp. 1812–1820, 2008.

[4] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, 2013.

[5] (2009, May) Data bus technical specifications for north american syncro-phasor initiative network (NASPInet). North American Syncro-Phasor Initiative Network. [Online]. Available: https://www.naspi.org/File.aspx?fileID=587

[6] H. Lin, Y. Deng, S. Shukla, J. Thorp, and L. Mili, "Cyber security impacts on all-PMU state estimator a case study on co-simulation platform GECO," in *IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, November 2012, pp. 587–592.

[7] (2012) PMU networking with IP multicast. CISCO Public. [Online]. Available: http://www.cisco.com/

[8] T. Liu, X. Guan, Q. Zheng, and Y. Qu, "A new worm exploiting IPv6 and IPv4-IPv6 dual-stack networks: experiment, modeling, simulation, and defense," *IEEE Networks*, vol. 23, pp. 22–29, 2009.

[9] B. Sun, G. Yan, Y. Xiao, and T. A. Yang, "Self-propagating mal-packets in wireless sensor networks: Dynamics and defense implications," *Ad Hoc Networks*, vol. 7, pp. 1489–1500, 2009.

[10] W. Xiaoming and L. Yingshu, "An improved SIR model for analyzing the dynamics of worm propagation in wireless sensor networks," *Chinese Journal of Electronics*, vol. 18, pp. 8–12, 2009.

[11] C. C. Zou, D. Towsley, and W. Gong, "Modeling and simulation study of the propagation and defense of internet e-mail worms," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, pp. 105–118, 2007.

[12] B. Stephenson and B. Sikdar, "A quasi-species model for the propagation and containment of polymorphic worms," *IEEE Transactions on Computers*, vol. 58, pp. 1289–1296, 2009.

[13] M. Altunay, S. Leyffer, J. T. Linderoth, and Z. Xie, "Optimal response to attacks on the open science grid," *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 55, pp. 61–73, January 2011.

[14] "NSTB assessments summary report: Common industrial control system cyber security weaknesses," Idaho National Laboratory (INL), Tech. Rep., 2010.

[15] J. Xichen, Z. Jiangmeng, B. J. Harding, J. J. Makela, and A. D. Dominguez-Garcia, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Transactions on Power Systems*, vol. 28, pp. 3253–3262, 2013.

[16] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, pp. 146–153, 2012.

[17] F. C. Schweppe, J. Wildes, and D. B. Rom, "Power system static state estimation, parts i,ii, and iii," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89, pp. 120–135, 1970.

[18] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM conference on computer and communications security*, 2009, pp. 21–32.

[19] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Transactions on Power Systems*, vol. PP, no. 99, p. 1, 2012.

[20] S. Mousavian, J. Valenzuela, and J. Wang, "Real-time data reassurance in electrical power systems based on artificial neural networks," *Electric Power Systems Research*, vol. 96, p. 285295, March 2013.

[21] C. Shuguang, H. Zhu, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Processing Magazine*, vol. 29, pp. 106–115, September 2012.

[22] G. Dan and H. Sanberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proceedings of the International IEEE Conference on Smart Grid Communications*, Gaithersburg, MD, October 2010.

[23] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proceedings of IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, October 2010.

[24] R. G. Cole, N. Phamdo, M. A. Rajab, and A. Terzis, "Requirements on worm mitigation technologies in MANETS," in *Workshop on Principles of Advanced and Distributed Simulation*, 2005, pp. 207–214.

[25] Y. H. Chang, P. Jirutitijaroen, and C.-W. Ten, "A simulation model of cyber threats for energy metering devices in a secondary distribution network," in *5th International Conference on Critical Infrastructure (CRIS)*, Beijing, 2010, pp. 1–7.

[26] S. Azizi, B. G. Gharehpetian, G. Hug-Glanzmann, and A. Dobakhshari, "Optimal integration of phasor measurement units in power systems considering conventional measurements," *IEEE Transactions on Smart Grid*, vol. 4, pp. 1113–1121, 2012.

[27] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation and Control*. John Wiley & Sons, 1996.

[28] Subcommittee, "IEEE reliability test system," *IEEE Transactions on Power Apparatus and Systems*, vol. 98, pp. 2047–2054, 1979.

[29] A. Bavier, N. Feamster, M. Huang, L. Peterson, and J. Rexford, "In VINI veritas: realistic and controlled network experimentation," in *SIGCOMM '06 Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, vol. 36, October 2006, pp. 3–14.

[30] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, pp. 12–19, 2011.

[31] B. K. S. Roy, A. K. Sinha, and A. K. Pradhan, "An optimal PMU placement technique for power system observability," *International Journal of Electrical Power & Energy Systems*, vol. 42, pp. 71–77, 2012.

Chapter 3

Investment Decisions on Optimal Allocation of Phasor Measurement Units

3.1 Abstract

Reliability of the electrical power systems necessitates wide-area monitoring and full observability of the power grid. Phasor measurement units (PMUs), as the state-of-the-art measurement devices, collect synchronized phasors of voltages and currents in real time and are utilized for full observability of the power systems. Due to budget restrictions and considerable cost of installing PMUs, it is not possible to equip all buses with PMUs. In this paper, we discuss the necessity of considering transmission switching and single contingencies in the optimal PMU placement problem. We show that considering transmission switching and single contingencies increases the PMU investment costs substantially and propose an integer linear programming model to determine the optimal PMU placement plan in two investment phases. In the first phase, PMUs are installed to achieve full observability of the power grid whereas additional PMUs will be installed in the second phase to guarantee the $N-1$ observability of the power grid. In each phase, power grid observability is guaranteed for all resulting topologies of the power grid stem from transmission switching. Simulation results are provided on several IEEE test systems which show that our proposed approach is a promising enhancement to the methods available for the optimal placement of PMUs.

keywords: Phasor measurement unit, Optimal placement, Network observability, Transmission switching, Integer linear programming

Nomenclature

Sets and Indices

Ω: Set of buses

Φ: Set of power grid topologies stem from transmission switching

i, j: Indices of buses

ϕ: Index of topologies

Constants

α_i: Observability number of bus i

α_i^{ϕ}: Observability number of bus i after the first phase of PMU placement under topology ϕ

β_i^{ϕ}: Observability number of bus i after the second phase of PMU placement under topology ϕ

C_j: Cost of installing a PMU at bus j

γ: The annual percentage of the change in PMU prices

$H_{i,j}$: Binary parameter that equals to 1 if $i = j$ or there is a transmission line between bus i and bus j, and 0 otherwise.

$H_{i,j}^{\phi}$: Binary parameter that equals to 1 if $i = j$ or there is a transmission line between bus i and bus j under topology ϕ, and 0 otherwise.

I: Inflation-free interest rate

K: Number of years between two phases of investment

Decision Variables

x_j: Binary decision variable which is equal to 1 if bus j is equipped with a PMU in the first phase, and 0 otherwise.

y_j: Binary decision variable which is equal to 1 if bus j is equipped with a PMU in the second phase, and 0 otherwise.

3.2 Introduction

Wide-area monitoring and full network observability of the electrical power systems in real time was impractical until the emergence of phasor measurement units (PMUs). PMUs are power system devices that measure synchronized phasors of voltages and currents in real time [1]. Synchronization is achieved by timing signals from the global positioning system (GPS) satellite with the accuracy in the order of 1 microsecond. In the future, it is expected that the smart grid will consist of at least 10,000 PMUs each taking about 30 to 120 measurements per second [2].

To ensure the observability of the power system, voltage phasors of all buses should be either directly measured or computed from other measurements [3]. Two types of observability have been addressed, numerical and topological observability. A network is numerically observable if the measurement Jacobian is of full rank [4, 5]. These methods are computationally extensive due to the iterative procedure of matrix manipulations [6]. Alternatively, topological observability considers interconnections of the buses and network observability rules to obtain the states vector of the power system. Unlike conventional measurement devices, a PMU can measure the current phasors of multiple lines and provide measurements to compute the voltage phasors of adjacent buses. Thus, there is no need, in terms of observability, to install a PMU at all buses.

Recently, the problem concerning Optimal Placement of PMUs (OPP) has been studied by researchers. The OPP problem considers the minimum number of PMUs and their installation locations that makes the power system observable. Many researchers have developed heuristic and meta-heuristic methods to solve the OPP problem. Chakrabarti and Kyriakides in [7] applied an exhaustive binary search methodology to tackle the OPP problem and find the associated locations of PMUs. An iterative three-stage heuristic method has been introduced in [8] where in the first two stages less important and strategically important buses are determined, and the last stage returns the optimal solution using pruning operation. In [9] and [10], simulated annealing is used to solve the OPP problem. Other

meta-heuristic methods such as Tabu search in [11] and binary particle swarm optimization in [12] have been applied to find the minimum number of PMUs required for full observability of the power system. Integer programming is used in [13] and [14] to find the optimal placement of PMUs. The authors in [15] applied integer linear programming (ILP) to solve the OPP problem considering conventional measurement devices. Although the OPP problem has been studied by many researchers, there are still certain practical aspects of the problem that need to be considered. In this paper, we consider new investment decisions on the placement of PMUs and deliver the following outcomes as our contributions.

First, failure of any PMU or transmission line may affect full observability of the power grid. Therefore, considering single contingencies in the allocation of PMUs is essential to meet the reliability requirements of the power system [15]. However, considering single contingencies increases the investment costs substantially, more than twice the initial costs in many cases. We refer the readers to Section 3.3.2 that illustrates this observation. Hence, we propose an integer linear programming problem that minimizes the total investment costs and determines the optimal placement of PMUs in two investment phases. In the first investment phase, PMUs are installed to achieve full observability of the grid. In the second phase of investment, additional PMUs are placed in service to meet the $N-1$ reliability requirement, which assures the full observability of the power grid even in the case of single contingencies.

Secondly, it has been discussed in the literature that transmission switching can provide additional economical advantages for a power system through changing its topology during operations [16–20]. Hence, transmission switching should be considered in the optimal placement of PMUs. Otherwise, it may put the observability of the power grid at risk. We refer the readers to Section 3.3.4 for a case study on how transmission switching may affect power grid observability.

Finally, we propose an integer linear programming model for optimal placement of PMUs in two investment phases. The model minimizes the total investment costs and considers transmission switching in the optimal PMU allocations.

The rest of this chapter is organized as follows: Section 3.3 describes the general optimal PMU placement model and our developed case studies. Section 3.4 discusses our proposed two-phase optimal PMU placement model. Section 3.5 provides some experimental results and Section 3.6 reports our conclusions.

3.3 PMU Placement Model

The Optimal PMU placement problem is defined as finding the installation location of PMUs required for the observability of the power system such that the total cost is minimized. Network observability rules can be used to avoid installing PMUs at all buses and reduce associated costs significantly.

3.3.1 Network Observability Rules

The network observability rules for topological observability of the power system given in [12] are described here.

1. If a PMU is installed at bus i, voltage phasor of bus i and current phasors of all incident transmission lines to bus i are known (Figure 3.1).

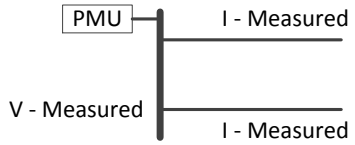


Figure 3.1: Network Observability Rule 1

2. If voltage phasor of one end of a transmission line and the current phasor of the transmission line are known, the voltage phasor of the other end of the transmission line can be calculated (Figure 3.2).

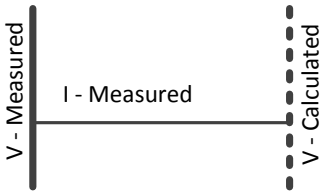


Figure 3.2: Network Observability Rule 2

3. If voltage phasors of both ends of a transmission line are known, the current phasor of the transmission line can be calculated (Figure 3.3).

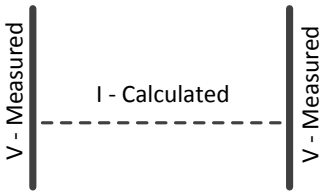


Figure 3.3: Network Observability Rule 3

Measurements obtained by Rule 1 are direct measurements. Rules 2 and 3 provide pseudo measurements. Zero-injection buses, which do not inject currents into the system, have the potential to reduce the number of required PMUs for observability of the power system, but we do not consider zero-injection buses in this paper. We refer the reader to [12] for more information on the network observability rules on zero-injection buses.

3.3.2 Single-phase Optimal PMU Placement Model

The objective function of the optimal PMU placement problem is to minimize the investment cost of PMUs. The objective function is given in equation (3.1).

$$Z = \min_{\mathbf{x}} \sum_{j \in \Omega} C_j x_j \tag{3.1}$$

A PMU at bus j can make all the adjacent buses observable by measuring the current phasors of the incident lines. Hence, the observability number of a bus is obtained by equation (3.2) using the network observability rules.

$$\alpha_i = \sum_{j \in \Omega} H_{i,j} x_j \qquad \forall i \in \Omega \tag{3.2}$$

We refer to the number of PMUs that make bus i observable, α_i, as the observability number of bus i. To have a topologically observable power system, the observability number of all buses should be greater than or equal to 1. Therefore, we write equation (3.3).

$$\alpha_i \geq 1 \qquad \forall i \in \Omega \tag{3.3}$$

Equations (3.1)-(3.3) assure the full observability of the power grid with minimum investment costs. Without loss of generality, it is common to assume that $C_j = 1$. Thus, the investment cost is interpreted in terms of number of PMUs. Moreover, single contingencies such as failure of a PMU or a transmission line should be taken into account in the placement of PMUs. Therefore, each bus in the power grid should be observable by at least two PMUs to make sure that any single contingency does not affect the full observability of the network. Mathematically speaking, we write equation (3.4) to ensure that the optimal placement is resilient against any single contingencies.

$$\alpha_i \geq 2 \qquad \forall i \in \Omega \tag{3.4}$$

We denote the ILP model given in Equations (3.1)-(3.4) by single-phase optimal PMU placement model since it is assumed that all PMUs are installed together. The single-phase optimal PMU placement problem with and without considering single contingencies have been solved by different heuristic, meta-heuristic and ILP methods. Table 3.1 shows the minimum number of PMUs required to make different test systems observable with and without considering single contingencies [8, 21].

Table 3.1: Optimal number of PMUs for full observability

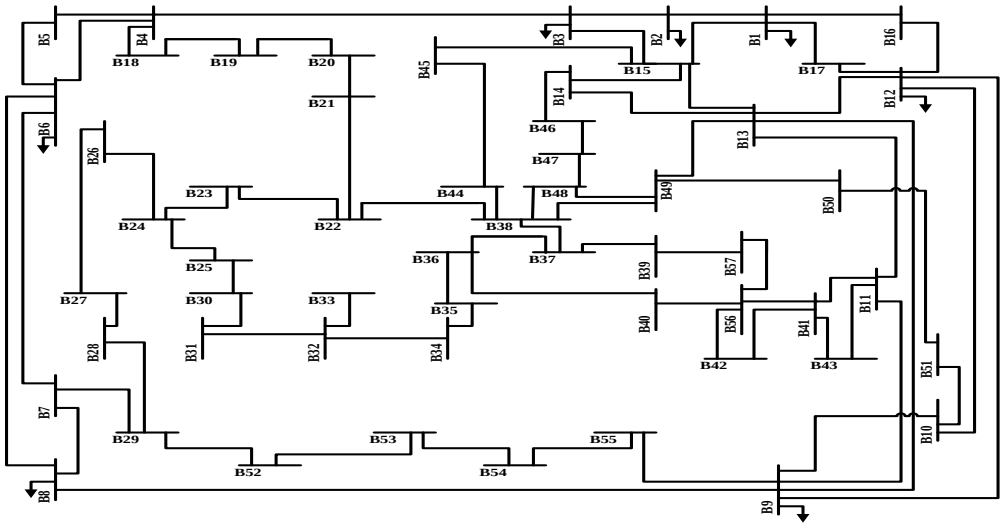
Power System	Minimum Observability	$N-1$ Observability
IEEE 14-bus	4	9
IEEE 24-bus	7	14
IEEE 30-bus	10	21
IEEE 39-bus	13	28
IEEE 57-bus	17	33
IEEE 118-bus	32	68

Considering the results provided in Table 3.1, it can be inferred that achieving the $N-1$ observability placement costs almost twice the minimum observability placement. Regarding the substantial capital cost of installing PMUs, a utility company may prefer to install PMUs in two phases. In the first phase, PMUs are installed to make the power grid fully observable by PMUs and postpone the $N-1$ observability placement to the second phase. Then, extra PMUs will be installed in the second phase to achieve $N-1$ observability. However, installing PMUs in the first phase should be done wisely to avoid any unnecessary additional investment in the second phase. In the next subsection, we discuss how PMU investment of the second phase may be affected by the PMU placement of the first phase.

3.3.3 Case Study I: Two-phase Investment Approach

To demonstrate the two-phase investment approach, we use the IEEE 57-bus system which consists of 57 buses, 80 transmission lines and 7 generators. The IEEE 57-bus test system is depicted in Figure 3.4. We refer the readers to [22] and [23] for additional system data.

Figure 3.4: IEEE 57-bus test system



From Table 3.1, we know that IEEE 57-bus system requires at least 17 PMUs for full observability and 33 PMUs for $N-1$ observability. Table 3.2 shows alternative optimal placements for full observability of the IEEE 57-bus test system. Each alternative may be selected in the first phase since they all require the minimum investment cost. However, it should be noticed that installing PMUs in the first phase creates new constraints for the optimal allocation of PMUs in the second phase. Therefore, it is likely that the total investment cost is not completely minimized if two phases are not considered together. To achieve $N-1$ observability in phase-2, we proceed and use the eight alternative solutions $(P_1 - P_8)$ given in Table 3.2. For each alternative solution, the number of PMUs and their locations to achieve the $N-1$ observability at the second-phase are given in Table 3.3. Notice that seven alternatives ultimately required more number of PMUs. The best investment

plan is given by U_8 which consists of installing 17 PMUs during the first phase and 16 PMUs during the second phase. The advantage of the two-phase plan is that the utility can decide whether to install all PMUs in one or in two phases while avoiding potential unnecessary investments.

Table 3.2: Alternative placements of the IEEE 57-bus system

Placement	PMU Locations
P_1	3, 6, 12, 15, 19, 22, 25, 27, 32, 36, 39, 41, 45, 47, 50, 52, 55
P_2	2, 6, 12, 19, 22, 25, 27, 32, 36, 39, 41, 45, 46, 49, 51, 52, 55
P_3	2, 6, 12, 19, 22, 25, 27, 32, 36, 39, 41, 45, 46, 49, 50, 52, 55
P_4	2, 6, 12, 19, 22, 25, 27, 29, 32, 36, 41, 45, 46, 49, 51, 52, 54
P_5	2, 6, 12, 15, 19, 22, 25, 27, 32, 36, 41, 44, 47, 50, 52, 54, 57
P_6	2, 6, 12, 13, 19, 22, 25, 27, 32, 36, 39, 41, 44, 47, 50, 52, 54
P_7	1, 4, 9, 19, 22, 26, 29, 30, 32, 36, 41, 45, 46, 49, 51, 54, 57
P_8	1, 4, 9, 19, 22, 26, 29, 30, 32, 36, 41, 45, 46, 47, 50, 54, 57

Table 3.3: Two-phase investment plan for alternative solutions of the IEEE 57-bus system

Investment Plan	PMU Locations - Phase 1	PMUs Phase 1	PMU Locations - Phase 2	PMUs Phase 2	Total
U_1	3, 6, 12, 15, 19, 22, 25, 27, 32, 36, 39, 41, 45, 47, 50, 52, 55	17	1, 4, 9, 20, 24, 26, 29, 30, 33, 35, 38, 43, 46, 51, 54, 56, 57	17	34
U_2	2, 6, 12, 19, 22, 25, 27, 32, 36, 39, 41, 45, 46, 49, 51, 52, 55	17	1, 4, 9, 15, 20, 23, 26, 29, 30, 33, 34, 37, 43, 44, 47, 50, 53, 56	18	35
U_3	2, 6, 12, 19, 22, 25, 27, 32, 36, 39, 41, 45, 46, 49, 50, 52, 55	17	1, 4, 9, 10, 14, 20, 23, 26, 29, 30, 33, 35, 43, 44, 48, 54, 56, 57	18	35
U_4	2, 6, 12, 19, 22, 25, 27, 29, 32, 36, 41, 45, 46, 49, 51, 52, 54	17	1, 4, 9, 11, 15, 20, 24, 28, 31, 33, 35, 38, 39, 47, 50, 55, 56, 57	18	35
U_5	2, 6, 12, 15, 19, 22, 25, 27, 32, 36, 41, 44, 47, 50, 52, 54, 57	17	1, 4, 9, 20, 24, 28, 29, 31, 33, 35, 38, 39, 43, 46, 51, 55, 56	17	34
U_6	2, 6, 12, 13, 19, 22, 25, 27, 32, 36, 39, 41, 44, 47, 50, 52, 54	17	1, 4, 9, 20, 24, 26, 29, 31, 33, 35, 38, 43, 45, 46, 51, 55, 56, 57	18	35
U_7	1, 4, 9, 19, 22, 26, 29, 30, 32, 36, 41, 45, 46, 49, 51, 54, 57	17	3, 6, 12, 15, 20, 24, 28, 31, 33, 35, 38, 39, 43, 47, 50, 53, 56	17	34
U_8	1, 4, 9, 19, 22, 26, 29, 30, 32, 36, 41, 45, 46, 47, 50, 54, 57	17	3, 6, 12, 15, 20, 24, 28, 31, 33, 35, 37, 38, 43, 51, 53, 56	16	33

3.3.4 Case Study II: The Impact of Transmission Switching on Optimal PMU Placement

Transmission switching reduces the electricity generation cost by temporarily removing inefficient transmission lines out of service. To demonstrate how transmission switching

influences the optimal placement of PMUs, we use IEEE 57-bus system, PMU placement U_8 given in Table 3.3 and developed scenarios given in Table 3.4. In each scenario, we assume that given transmission lines are removed temporarily from the power grid.

Table 3.4: Transmission switiching scenarios

Scenario	Removed Transmission Lines
S_1	No Line
S_2	7-8, 10-51, 11-13, 13-14
S_3	9-12, 19-20,
S_4	6-7, 7-29

In scenario S_1 when there is no removed transmission line, all buses are $N-1$ observable. In scenario S_2, all buses are still $N-1$ observable although four transmission lines are temporarily removed. In scenario S_3, removing two transmission lines affects the $N-1$ observability of the power grid since buses 9, 12, 19 and 20 would no longer be $N-1$ observable. Hence, a single contingency such as failure of a PMU may further affect the full observability of the grid. Removing lines 6-7 and 7-29 in scenario S_4 results in not observability of bus 7. It can be concluded that it is essential to consider transmission switching in the optimal placement of PMUs since it changes the topology of the power grid.

3.4 Two-phase optimal PMU placement model considering transmission switching

The two-phase optimal placement of PMUs considering transmission switching is modeled using integer linear programming. The optimal placement of PMUs to achieve $N-1$ observability occurs in two phases. Hence, the objective function is to minimize the present value of the total investment costs. To calculate the present value, we use the concept of constant dollar analysis [24] in which price increases due to the inflation are ignored. Hence, the inflation-free interest rate, I, is used to compare the investment costs of the two phases.

It is assumed that the second phase of PMU placement occurs K years after the initial phase. Therefore, the objective function is as follows.

$$Z = \min_{\mathbf{x},\mathbf{y}} \left(\sum_{j \in \Omega} C_j x_j + \frac{1}{(1+I)^K} \sum_{j \in \Omega} \gamma^K C_j y_j \right) \tag{3.5}$$

Where x_j equals 1 if a PMU is installed in bus j in phase 1. Similarly, y_j equals 1 if a PMU is installed in bus j in phase 2. Moreover, it is likely that PMU prices decrease annually due to the free market competitions and advancements in manufacturing of PMUs. We use parameter γ, the annual percentage of the change in PMU prices, in the objective function to consider these likely price decreases. Notice that the objective function favors installing PMUs in the second phase.

The goal of the first phase is to achieve the full observability of the power grid. Therefore, the constraints given in equations (3.6)-(3.7) should be satisfied.

$$\alpha_i = \sum_{j \in \Omega} H_{i,j} x_j \qquad \forall i \in \Omega \tag{3.6}$$

$$\alpha_i \geq 1 \qquad \forall i \in \Omega \tag{3.7}$$

However, notice that equations (3.6)-(3.7) ensure the full observability of the power grid only when all transmission lines of the power system are in service. As it is mentioned, transmission switching changes the topology of the network. Therefore, it is necessary to make sure that allocated PMUs make the power grid observable for all potential topologies of the power grid stem from transmission switching. Hence, we modify equations (3.6)-(3.7) and obtain equations (3.8)-(3.9) as follows.

$$\alpha_i^\phi = \sum_{j \in \Omega} H_{i,j}^\phi x_j \qquad \forall i \in \Omega, \forall \phi \in \Phi \tag{3.8}$$

$$\alpha_i^\phi \geq 1 \qquad \forall i \in \Omega, \forall \phi \in \Phi \tag{3.9}$$

Where α_i^ϕ represents the observability number of bus i after the first phase of PMU placements under topology $\phi \in \Phi$, and $H_{i,j}^\phi$ is the connectivity parameter of buses i and j under topology $\phi \in \Phi$.

Furthermore, $N-1$ observability should be accomplished in the second phase considering different topologies stem from the transmissions switching. Therefore, we consider the constraints given in equations (3.10)-(3.11).

$$\beta_i^\phi = \alpha_i^\phi + \sum_{j \in \Omega} H_{i,j}^\phi y_j \qquad \forall i \in \Omega, \forall \phi \in \Phi \tag{3.10}$$

$$\beta_i^\phi \geq 2 \qquad \forall i \in \Omega, \forall \phi \in \Phi \tag{3.11}$$

Where β_i^ϕ represents the observability number of bus i after the second phase of PMU placements under topology $\phi \in \Phi$.

Next, it should be ensured that at most one PMU is installed in each bus. Therefore, the constraint given in equation (3.12) should be satisfied.

$$x_i + y_i \leq 1 \qquad \forall i \in \Omega \tag{3.12}$$

Finally, equation (3.13) determines that the decision variables are binary.

$$x_i, y_i \in \{0, 1\} \qquad \forall i \in \Omega \tag{3.13}$$

3.5 Experimental Results

To test the performance of our algorithm, we use data from the IEEE Reliability Test Systems [22]. We run our experiments on the IEEE 14-bus, IEEE 24-bus, IEEE 30-bus, IEEE 39-bus, IEEE 57-bus, IEEE 118-bus, IEEE 300-bus, IEEE 2383-bus and IEEE 3120-bus test systems. In our experiments, we set the cost of installing a PMU at bus j to 1, $C_j = 1$. Also, we assume that the price of manufacturing a PMU is the same in both phases of investment, $\gamma = 1$. We arbitrarily chose the value of 0.5% for the inflation-free interest rate, $I = 0.5\%$. Finally, we assume that the two phases of investment occur in two consecutive years, $K = 1$.

3.5.1 Optimal PMU Placement without Transmission Switching

We use our two-phase ILP model to find the optimal locations of the PMUs such that full observability of the power grid is achieved in the first phase, and $N-1$ observability is accomplished in the second phase. The optimal placements are provided in Table 3.5.

Table 3.5: Two-phase investment plan for the IEEE test systems

Test System	PMU Locations - Phase 1	PMUs Phase 1	PMU Locations - Phase 2	PMUs Phase 2	Total
IEEE 14-bus System	2, 6, 7, 9	4	1, 3, 8, 11, 13	5	9
IEEE 24-bus System	3, 4, 8, 10, 16, 21, 23	7	1, 2, 7, 11, 15, 17, 20	7	14
IEEE 30-bus System	2, 3, 6, 10, 11, 12, 15, 18, 25, 27	10	1, 7, 8, 9, 13, 16, 19, 21, 23, 26, 29	11	21
IEEE 39-bus System	2, 6, 9, 10, 13, 14, 17, 19, 22, 23, 29, 34, 37	13	1, 3, 8, 11, 16, 20, 25, 26, 30, 31, 32, 33, 35, 36, 38	15	28
IEEE 57-bus System	1, 4, 9, 19, 22, 26, 29, 30, 32, 36, 41, 45, 46, 47, 50, 54, 57	17	3, 6, 12, 15, 20, 24, 28, 31, 33, 35, 37, 38, 43, 51, 53, 56	16	33
IEEE 118-bus System	2, 5, 9, 12, 15, 17, 21, 24, 26, 28, 34, 37, 41, 45, 49, 53, 56, 62, 63, 68, 71, 75, 77, 80, 85, 87, 90, 94, 102, 105, 110, 114	32	3, 6, 10, 11, 19, 22, 27, 29, 30, 32, 35, 40, 44, 46, 51, 54, 57, 59, 64, 66, 70, 73, 79, 84, 86, 89, 92, 96, 100, 107, 108, 111, 112, 116, 117, 118	36	68

The results of our proposed method are compared with available PMU placement methods given in Table 3.1. Notice that the total number of PMUs required for $N-1$ observability in a two-phase plan is the same as that of a single-phase plan for the given test systems. However, there is no guarantee that the two-phase plan always returns the same number of

PMUs as the single-phase plan. Fortunately, our method is flexible to obtain the optimal single-phase placement of PMUs as well by setting the value of the parameter k to zero. It is one of the advantages of our two-phase optimal PMU placement model that it provides the utility companies with more flexibility. They obtain the optimal PMU placements for single-phase and two-phase plans and decide whether to install all PMUs in one or in two phases while avoiding any potential unnecessary investments.

Next, we use our model to obtain the number of PMUs required for $N-1$ observability in larger systems. The results are given in Table 3.6 for IEEE 300-bus, IEEE 2383-bus and IEEE 3120-bus test systems. The results show that there are PMU placements for these large test systems, which are optimal solutions for both single-phase and two-phase PMU placement methods.

Table 3.6: Optimal number of PMUs in large power systems

Test System	PMUs Phase 1	PMUs Phase 2	Total	Single Phase
IEEE 300-bus	87	115	202	202
IEEE 2383-bus	746	935	1681	1681
IEEE 3120-bus	994	1212	2206	2206

3.5.2 Optimal PMU Placement with Transmission Switching

In this section, we use IEEE 118-bus system to test the performance of our ILP model for two-phase optimal placement of PMUs considering the transmission switching. This test system consists of 118 buses, 186 transmission lines and 54 generators. We refer the readers to [22] and [23] for additional system data.

We create the scenarios given in Table 3.7 randomly in which mentioned transmission lines are temporarily removed. In real world, the transmission lines which might be taken off the grid for transmission switching are known in advance. Thus, different topologies of the power grid stem from transmission switching can be obtained by enumeration.

Table 3.7: Transmission switiching scenarios for IEEE 118-bus system

Scenario	Removed Transmission Lines
W_1	No Line (No Transmission Switching)
W_2	17-18, 23-25, 37-39, 78-89, 80-81
W_3	24-70, 48-49, 103-110
W_4	32-113, 65-66, 83-85, 103-105
W_5	23-25, 41-42, 49-66, 71-72, 80-96

Next, we obtain the optimal placements for all given scenarios and provide the results in Table 3.8. At the bottom of Table 3.8, we consider all scenarios together to figure out the PMU placement which makes all resulting topologies $N-1$ observable if our proposed ILP model considering transmission switching is not employed. Therefore, it requires to place 94 PMUs in service, 61 PMUs in phase-1 and 33 PMUs in phase-2. Notice that the investment cost of the first phase is increased considerably.

Afterwards, we use our proposed ILP model to find the optimal solution for the mentioned transmission switching scenarios. The optimal placement is provided in Table 3.9. It shows that the optimal placement for $N-1$ observability of the IEEE 118-bus system with mentioned transmission switching scenarios requires 76 PMUs, 35 PMUs in phase-1 and 41 PMUs in phase-2. Therefore, our proposed model could decrease a great deal of investment costs comparing to the given placement $W_1 - W_5$ provided in Table 3.8. Moreover, notice that the optimal solution needs much less number of PMUs in the first phase which is critical

Table 3.8: Optimal placements for the transmission switching scenarios of IEEE 118-bus system

Scenario	PMU Locations - Phase 1	PMUs Phase 1	PMU Locations - Phase 2	PMUs Phase 2	Total
W_1	2, 5, 9, 12, 15, 17, 21, 24, 26, 28, 34, 37, 41, 45, 49, 53, 56, 62, 63, 68, 71, 75, 77, 80, 85, 87, 90, 94, 102, 105, 110, 114	32	3, 6, 10, 11, 19, 22, 27, 29, 30, 32, 35, 40, 44, 46, 51, 54, 57, 59, 64, 66, 70, 73, 79, 84, 86, 89, 92, 96, 100, 107, 108, 111, 112, 116, 117, 118	36	68
W_2	2, 5, 9, 12, 15, 19, 22, 27, 30, 31, 32, 35, 40, 43, 45, 49, 52, 56, 62, 64, 68, 70, 71, 75, 77, 80, 85, 87, 90, 94, 101, 105, 110	33	3, 6, 10, 11, 17, 18, 21, 24, 25, 28, 34, 37, 39, 41, 46, 51, 53, 57, 59, 61, 67, 73, 78, 79, 81, 83, 86, 89, 92, 96, 100, 106, 108, 111, 112, 114, 116, 117, 118	39	72
W_3	2, 5, 9, 12, 15, 17, 21, 23, 28, 30, 36, 40, 44, 46, 50, 52, 56, 62, 63, 68, 71, 75, 77, 80, 85, 87, 90, 94, 102, 105, 110, 115	32	3, 6, 10, 11, 19, 20, 25, 29, 35, 37, 42, 43, 48, 49, 51, 54, 61, 64, 67, 70, 72, 73, 79, 84, 86, 89, 92, 96, 100, 107, 108, 111, 112, 113, 114, 116, 117, 118	38	70
W_4	2, 5, 9, 12, 15, 17, 21, 25, 29, 34, 37, 40, 45, 49, 53, 56, 62, 64, 68, 70, 71, 76, 79, 84, 87, 89, 92, 96, 100, 105, 110, 114	32	3, 6, 10, 11, 19, 22, 26, 28, 31, 35, 41, 44, 46, 51, 54, 57, 59, 65, 67, 72, 73, 75, 77, 80, 82, 85, 86, 90, 94, 102, 107, 108, 111, 112, 113, 115, 116, 117	38	70
W_5	2, 5, 9, 12, 15, 17, 21, 24, 25, 29, 34, 37, 40, 45, 49, 53, 56, 62, 63, 68, 73, 75, 77, 80, 85, 87, 90, 94, 101, 105, 110, 114	32	3, 6, 10, 11, 19, 22, 27, 28, 30, 32, 35, 41, 44, 46, 51, 54, 57, 61, 64, 66, 71, 72, 74, 78, 84, 86, 89, 92, 96, 100, 107, 108, 111, 112, 116, 117, 118	37	69
$W_1 - W_5$	2, 5, 9, 12, 15, 17, 19, 21-32, 34-37, 40, 41, 43-46, 49, 50, 52, 53, 56, 62-64, 68, 70, 71, 73, 75-77, 80, 84, 85, 87, 89, 90, 92, 94, 96, 100-102, 105, 110, 114, 115	61	3, 6, 10, 11, 18, 20, 39, 42, 48, 51, 54, 57, 59, 61, 65, 66, 67, 72, 74, 78, 81, 82, 83, 86, 106, 107, 108, 111, 112, 113, 116, 117, 118	33	94

from investment point of view. It is likely that PMU prices decrease later which benefits a utility by decreasing the investment costs even more.

Table 3.9: Optimal placement for IEEE 118-bus system considering transmission switching scenarios

Phase	PMU Locations	Number of PMUs
1	2, 5, 9, 12, 15, 17, 19, 21, 24, 25, 28, 35, 40, 43, 46, 49, 52, 56, 59, 62, 65, 68, 73, 75, 77, 80, 84, 87, 89, 92, 94, 102, 105, 110, 114	35
2	3, 6, 10, 11, 18, 22, 26, 27, 29, 36, 37, 39, 41, 44, 48, 53, 57, 58, 63, 66, 70, 71, 72, 76, 78, 79, 81, 82, 85, 86, 90, 96, 100, 107, 108, 111, 112, 113, 115, 116, 117	41

Furthermore, it is likely that a utility would like to know if they could decrease the PMU investments by not using one or more of the transmission switching scenarios. Table 3.10 provides the optimal number of PMUs if a certain scenario would not be used. As a case in point, it can be concluded that including scenario W_2 may be a strategic decision since including W_2 itself increases the number of PMUs as many as including all three scenarios W_3, W_4 and W_5. Moreover, notice that the utility needs to install eight more PMUs due to the transmission switching scenarios. Otherwise, the IEEE 118-bus system requires only 68 PMUs for $N-1$ observability.

Table 3.10: Optimal number of PMUs for removed transmission switching scenarios

Removed Scenario	PMUs Phase 1	PMUs Phase 2	Total
None	35	41	72
W_2	34	38	72
W_3	34	41	75
W_4	33	41	74
W_5	35	40	75
W_2, W_3	34	37	71
W_2, W_4	33	37	70
W_2, W_5	33	38	71
W_3, W_4	33	40	73
W_3, W_5	34	40	74
W_4, W_5	33	41	74
W_2, W_3, W_4	32	37	69
W_2, W_3, W_5	32	38	70
W_2, W_4, W_5	32	38	70
W_3, W_4, W_5	33	39	72
W_2, W_3, W_4, W_5	32	36	68

3.5.3 Computational Time Analysis

All experiments were performed on a 64-bit laptop with an Intel Core i5 2.4 GHz processor and 4GB RAM. We used IBM ILOG CPLEX Optimization Studio 12.6 as the optimization solver in our experiments.

Table 3.11 summarizes the computational time for obtaining the optimal PMU placements for different cases discussed in Section 3.5.1. Computational time analysis shows that our two-phase optimal PMU placement model is solved very quickly even for large power systems.

Table 3.11: Computational Times (s)

Test System	Single-phase	Two-phase
IEEE 14-bus	0.81	0.81
IEEE 24-bus	0.82	0.82
IEEE 30-bus	0.82	0.83
IEEE 39-bus	0.82	0.84
IEEE 57-bus	0.87	0.89
IEEE 118-bus	0.97	1.00
IEEE 300-bus	1.36	1.39
IEEE 2383-bus	33.15	33.71
IEEE 3120-bus	57.79	58.88

3.6 Conclusions

Observability of the power system is important for grid operation and control. Complex networks of PMUs, as the state-of-the-art measurement devices, are used to collect real time data to improve the observability of the power systems. However, due to budget restrictions and considerable cost of installing PMUs, it is not possible to equip all buses with PMUs. Also, it has been discussed that the reliability requirement of $N-1$ observability and including transmission switching in the optimal placement of PMUs increase the investment costs significantly. Therefore, the network observability rules and PMUs' characteristics should be used to the full extent in order to minimize the PMU investment costs. In this

paper, we developed an integer linear programming model that minimizes the investment costs of PMUs and determines the optimal locations of PMUs in two investment phases. In the first phase, PMUs are installed to achieve full observability of the power grid whereas additional PMUs will be installed in the second phase to guarantee the $N-1$ observability of the power grid. The proposed model is able to provide utilities with single-phase and two-phase optimal placements, which gives investors more flexibility on whether to install all PMUs in one or in two phases while avoiding any potential unnecessary costs.

Furthermore, it has been shown that it is critical to consider transmission switching in the optimal PMU placement problem. Transmission switching changes the topology of the power grid and may cause not observability of some buses. In our ILP model, we integrated the transmission switching concept into the optimal PMU placement problem such that the obtained optimal placement is $N-1$ observable for all topologies of the power grid stem from transmission switching.

The performance of the developed ILP model is tested on several IEEE test systems. Experimental results show that our developed model is a promising enhancement to the optimal PMU placement problem and also ensures the observability of the power systems when transmission switching is utilized. Computational times have also been reported to show that our model can be solved very quickly by optimization solvers even for large power systems.

References

[1] B. Singh, N. Sharma, A. Tiwari, K. Verma, and S. Singh, "Applications of phasor measurement units (PMUs) in electric power system networks incorporated with facts controllers," *International Journal of Engineering, Science and Technology*, vol. 3, pp. 64–82, 2011.

[2] K. P. Briman, L. Ganesh, and R. van Renesse, "Running smart grid control software on cloud computing architectures," in *Workshop Computational Needs for the Next Generation Electric Grid*. Cornell University, 2011, pp. 1–33.

[3] A. Monticelli, *State Estimation in Electric Power Systems: A Generalized Approach*. Norwell, MA: Kluwer Academic Publishers, 1999.

[4] A. B. Antonio, J. R. A. Torreao, and M. B. D. C. Filho, "Meter placement for power system state estimation using simulated annealing," in *Proceedings of the IEEE Power Tech Conference*, 2001.

[5] B. Milosevic and M. Begovic, "Nondominated sorting genetic algorithm for optimal phasor measurement placement," *IEEE Transactions on Power Systems*, vol. 18, pp. 69–75, 2003.

[6] R. Sodhi, S. C. Srivastava, and S. N. Singh, "Optimal PMU placement method for complete topological and numerical observability of power system," *Electric Power System Research*, vol. 80, pp. 1154–1159, 2010.

[7] S. Chakrabarti and E. Kyriakides, "Optimal placement of phasor measurement units for power system observability," *IEEE Transactions on Power Systems*, vol. 23, pp. 1433–1440, 2008.

[8] B. K. S. Roy, A. K. Sinha, and A. K. Pradhan, "An optimal PMU placement technique for power system observability," *Electrical Power and Energy Systems*, vol. 42, pp. 71–77, 2012.

[9] T. L. Baldwin, L. Mili, J. M. B. Boisen, and R. Adapa, "Power system observability with minimal phasor measurement placement," *IEEE Transactions on Power Systems*, vol. 8, pp. 707–715, 1993.

[10] R. F. Nuqui and A. G. Phadke, "Phasor measurement unit placement techniques for complete and incomplete observability," *IEEE Transactions on Power Delivery*, vol. 20, pp. 2381–2388, 2005.

[11] J. Peng, Y. Sun, and H. F. Wang, "Optimal PMU placement for full network observability using tabu search algorithm," *Electrical Power and Energy Systems*, vol. 28, pp. 223–231, 2006.

[12] A. Ahmadi, Y. Alinejad-Beromi, and M. Moradi, "Optimal PMU placement for power system observability using binary particle swarm optimization and considering measurement redundancy," *Expert Systems with Applications*, vol. 38, pp. 7263–7269, 2011.

[13] B. Xu and A. Abur, "Optimal placement of phasor measurement units for state estimation," PSERC, Tech. Rep., 2005.

[14] S. Azizi, A. S. Dobakhshari, S. A. N. Sarmadi, and A. M. Ranjbar, "Optimal PMU placement by an equivalent linear formulation for exhaustive search," *IEEE Transactions on Smart Grid*, vol. 3, pp. 174–182, 2012.

[15] S. Azizi, B. G. Gharehpetian, G. Hug-Glanzmann, and A. Dobakhshari, "Optimal integration of phasor measurement units in power systems considering conventional measurements," *IEEE Transactions on Smart Grid*, 2012.

[16] C. Liu, J. Wang, and J. Ostrowski, "Static switching security in multi-period transmission switching," *IEEE Transactions on Power Systems*, vol. 27, no. 4, pp. 1850–1858, November 2012.

[17] G. Granelli, M. Montagna, F. Zanellini, P. Bresesti, R. Vailati, and M. Innorta, "Optimal network recofiguration for congestion management by deterministic and genetic algorithms," *Electric Power System Research*, vol. 76, p. 549556, April 2006.

[18] R. P. O'Neill, R. Baldick, U. Helman, M. H. Rothkopf, and W. Stewart, "Dispatchable transmission in RTO markets," *IEEE Transactions on Power Systems*, vol. 20, no. 1, p. 171179, February 2005.

[19] E. B. Fisher, R. P. O'Neill, and M. C. Ferris, "Optimal transmission switching," *IEEE Transactions on Power Systems*, vol. 23, no. 3, pp. 1355–1364, August 2008.

[20] K. W. Hedman, R. P. O'Neill, E. B. Fisher, and S. S. Oren, "Optimal transmission switching - sensitivity analysis and extensions," *IEEE Transactions on Power Systems*, vol. 23, no. 3, p. 14691479, August 2008.

[21] D. Dua, S. Dambhare, R. K. Gajbhiye, and S. A. Soman, "Optimal zero injection considerations in PMU placement: An ILP approach," *IEEE Transactions on Power Delivery*, vol. 23, pp. 1812–1820, 2008.

[22] Subcommittee, "IEEE reliability test system," *IEEE Transactions on Power Apparatus and Systems*, vol. 98, pp. 2047–2054, 1979.

[23] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, pp. 12–19, 2011.

[24] C. S. Park, *Fundamentals of Engineering Economics*, 3rd ed. Prentice Hall, 2013.