Anomaly Detection for Control Centers

Cliff O. Gyamfi

Thesis submitted to the Faculty of Electrical and Computer Engineering
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Electrical Engineering

Chen-Ching Liu, Chair
Virgilio A. Centeno
Ali Mehrizi-Sani

May 6, 2024
Blacksburg, Virginia

Keywords: Measurement-Based Cyber Attacks,State Estimation,Anomaly Detection,Energy Management System, Control Center

Anomaly Detection for Control Centers

Cliff O. Gyamfi

(ABSTRACT)

The control center is a critical location in the power system infrastructure. Decisions regarding the power system's operation and control are often made from the control center. These control actions are made possible through SCADA communication. This capability however makes the power system vulnerable to cyber attacks. Most of the decisions taken by the control center dwell on the measurement data received from substations. These measurements estimate the state of the power grid. Measurement-based cyber attacks have been well studied to be a major threat to control center operations. Stealthy false data injection attacks are known to evade bad data detection . Due to the limitations with bad data detection at the control center, a lot of approaches have been explored especially in the cyber layer to detect measurement-based attacks. Though helpful, these approaches do not look at the physical layer. This study proposes an anomaly detection system for the control center that operates on the laws of physics. The system also identifies the specific falsified measurement and proposes its estimated measurement value .

Anomaly Detection for Control Centers

Cliff O. Gyamfi

(GENERAL AUDIENCE ABSTRACT)

Electricity is an essential need for human life. The power grid is one of the most important human inventions that fueled other technological innovations in the industrial revolution. Changing demands in usage have added to its operational complexity. Several modifications have been made to the power grid since its invention to make it robust and operationally safe. Integration of ICT has significantly improved the monitoring and operability of the power grid. Improvements through ICT have also exposed the power grid to cyber vulnerabilities. Since the power system is a critical infrastructure, there is a growing need to keep it secure and operable for the long run. The control center of the power system serves mainly as the decision-making hub of the grid. It operates through a communication link with the various dispersed devices and substations on the grid. This interconnection makes remote control and monitoring decisions possible from the control center. Data from the substations through the control center are also used in electricity markets and economic dispatch. The control center is however susceptible to cyber-attacks, particularly measurement-based attacks. When attackers launch measurement attacks, their goal is to force control actions from the control center that can make the system unstable. They make use of the vulnerabilities in the cyber layer to launch these attacks. They can inject falsified data packets through this link to usurp correct ones upon arrival at the control center. This study looks at an anomaly detection system that can detect falsified measurements at the control center. It will also indicate the specific falsified measurements and provide an estimated value for further analysis.

Dedication

To Linda and Richess

Acknowledgments

I would like to express my profound gratitude to my academic advisor, Dr. Chen-Ching Liu for his immense support and guidance throughout this study. He has always motivated and shown me the pointers to guide this study. I really appreciate it. I would also like to appreciate and acknowledge the National Renewable Energy Laboratory (N.R.E.L) and the U.S Department of Energy (D.O.E)for the financial support they provided to aid this study. I also want to thank Dr. Virgilio A. Centeno, Dr. Jaime De La Ree Lopez, and Dr. Ali Mehrizi-Sani for the encouragement and support in this work. I am very grateful. I would also like to acknowledge and appreciate Dr. Vassilis Kekatos for the tutilage I received in his power system operation and control class. It contributed to my understanding for this research. The entire academic fraternity of Virginia Tech have also been of great help to me. I am grateful for the opportunity to be here and the conducive environment provided to pursue my academic dreams. I want to also appreciate past graduate students including Jennifer Appiah-Kubi and Ruoxi Zhu who offered me much cherished advice in this pursuit. I would also like to specially mention Akshay Jain, Nitasha Sahani and Akhila Herath for the immense support they provided me in this journey. Not forgetting my lab colleagues Yijie Zhou and Vishal Dixit for all the support. I also want to thank my parents and sisters for all the encouragement. I would also like to specially acknowledge my wife and daughter who have also made a lot of sacrifices for me within this period. I cherish you so much. Finally I would like to thank God for the strength and opportunity to see this day.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The power system has seen a lot of improvement in operational efficiency with the integration of Information and Communication Technology (ICT). With ICT the functions of telemetering, telecontrol and remote monitoring are made possible on the power grid through the Supervisory Control and Data Acquisition (SCADA) systems. Undoubtedly, these added functions have helped to minimize losses, reduce system downtime and energy costs.However, the increasing penetration of ICT into power system operations has also been shown to increase the attack surface for cyber intrusion on the grid[1].In 2007, Idaho National Laboratory demonstrated that circuit breakers can be manipulated through cyber intrusion, and this can subsequently lead to the destruction of a generating unit[2].In 2016, the CRASHOVERRIDE malware was deployed on the Ukrainian power grid to manipulate the relay devices on the transmission system[3].For two peak electricity consumption days in the winter of 2016, Israel also faced a massive cyber-attack on its electric grid bringing temperatures to below freezing levels[4].In April 2024, the North American Electric Reliability Corporation (NERC) reported that the U.S. power grids are increasingly vulnerable to cyberattacks, with the number of susceptible points in electrical networks increasing by about 60 per day[5].There is therefore a critical need to investigate the security of the power grid against cyber-attacks.

One of the most critical locations on the power system infrastructural set up is the control center. At the control center, critical network decisions are made to ensure stability of the power system. With the help of the SCADA communication protocols operational decisions

such as opening and closing breakers, network isolation for maintenance and fault analysis are made possible. Electricity market prices are also made based on the state estimation variables from the measurement data collected by the control center. In effect, the control center is responsible for decisions that are critical for the power grid's reliability and operational stability. However, the control center is also susceptible to network intrusion attacks, particularly measurement-based attacks.

Measurement-based attacks occur when attackers successfully modify measurement data reported from substations to the operations control center. The aim of measurement attacks is to mislead the SCADA master into taking undesirable actions that threaten the stability of the grid. For instance, consider an attacker who manages to send falsified low voltages from multiple substations to the control center. In response, operators may decide to shed some load which may lead to outages to these connected sites on the power grid. This study proposes an anomaly detection system that can assist the control center to detect falsified measurements before they damage the energy management system.

1.1 Motivation

Several works have been done to determine data falsification as a cyber security threat to smart grids[6].These attacks can be launched at substation nodes or through the communication links on the transmission system. Detecting False Data Injection attacks before measurement data goes into the energy management system can help minimize or curb the inherent impact on state estimation and security assessment functions.

It has also been established by Liu et al[7]that if the attacker has some knowledge of the power system, he is able to construct an attack model and inject falsified data that may be undetected by state estimation at the control center. This also raises the need for an intru-

sion detection system that can detect stealthy attacks on the power system. The security mechanism provided by the DNP3 Secure Authentication (DNP3-SA) protocol, which ensures secured communication between substations and the control center is not able to detect falsified measurement encapsulated in the DNP3 packets[8].There are inherent limitations to detection by anomalous packet structure rather than examining the payload. Hence a need to develop a system that can check the actual measurement data before state estimation.

1.2 Literature Review

Several approaches have been explored as measures to detect cyber intrusion in SCADA communication.[9]proposed a specification-based approach that specifies communication rules and physical limits that the system should obey.[10]proposes a behavior-based approach that analyses the control layers in industrial automated process which are stored in embedded systems to detect anomalous processes. Both approaches tackle intrusion from the cyber layer without considering the physical system. Brand et al[11]tried to bridge this gap by proposing a framework that monitors the health status of sensing devices and SCADA communication channels of the power system to detect intrusion. However, this approach does not look at actual messages or data being transferred.

State estimation's bad data detection works on the premise that all the measurement data received are authentic[12].It finds an outlier based on a defined threshold using the chi-square metrics and flags it as bad data. This process has inherent limitations. Reference [7] showed that with enough knowledge of the power system topology, an attacker can construct an attack vector that can evade this process. In[13],Che et al. also proved that a false load data attack can be modelled to impact security constrained economic dispatch, which will lead to transmission overloads and eventual system collapse when the generation schedule is

followed. In [14]Kosut et al. also proposed an attack model for some critical measurements on the power grid that makes the system unobservable to the control center's state estimation process.[15],[16]reiterates the fact that both stealthy and non-stealthy false data injection attacks pose significant problems to the power system state estimation.

To meet this challenge, Pei et al. in[17]proposed a deviation-based approach by introducing an additional Kalman filter to perform double state estimation. This approach is, however, susceptible to multiple false alarms. The canonical variate analysis-based detection method proposed in[18]monitors statistical indicators based on pre-ordered variables before and after an attack to detect intrusion. However, in a multivariate environment such as the power system, this approach is delimiting for attack detection.[19]also employs a state deviation index that takes another look at measurement data after state estimation to detect intrusion. This method is however over reliant on historical data.

In [12],a process-aware approach is employed using power flow analysis to determine anomalous measurement data. Thresholds in this method are however, empirically determined and this makes implementation questionable.[20]also employs a neural network-based approach to determine critical branches to strengthen to shield the network from load redistribution attacks.[21],[22]also proposes the optimal placement of PMUs on the power grid as an intrusion detection scheme for measurement attacks. This study proposes an anomaly detection system based on the fundamental laws of physics.

1.3 Contribution

The aim of this research is to develop a measurement Anomaly Detection system in a Control Center, ADCC, that will be able to:

- Detect measurement attacks at the control center before state estimation.
- Accurately detect stealthy attacks that evade state estimation.
- Identify the specific falsified measurement.
- Provide the system estimated measurements of falsified measurements detected.

1.4 Assumptions

In the formulation of the algorithm the assumptions made are as follows:

- Accurate GPS information is available. This will ensure that data is received with correct timestamps.
- At every point in time the attacker has control over some substations in the power system. This enables the attacker to falsify measurements received at the control center. If the attacker has control over the entire power system, (s)he can solve power flow equations with falsified measurement values. In which case this algorithm will not be able to detect intrusion.
- It is also assumed that the network is observable and so measurement data received can account for all connected buses.
- In a transmission system, the SCADA data reported to the control center include Injected power, Bus Voltages, and power flows (MW and MVAr) on lines terminating at substations. This data is also assumed to be available for analysis.

1.5 Thesis Organisation

The remainder of this study is organized as follows: Chapter 2 discusses the problem formulation and the system model. Chapter 3 discusses the algorithm formulation. The attack model and simulation results are discussed in Chapter 4 Chapter 5 provides conclusion and discusses future work.

Chapter 2

Problem Formulation

The control center receives measurements from all substations in the power network and these provide an estimate of the state of the network. This is made possible through communication links. In the transmission system, SCADA protocols enable communication between the control center and all remote substations. The IEEE std 1815 [Distributed Network Protocol (DNP3)] specifies a standard mapping for interconnection with IEC 6185 based substation[23].

DNP3 is an object-oriented network-based protocol that has a master server, which interfaces the monitored devices and the Human Machine interface (HMI) at the control center[24].The corresponding outstation server also interfaces the master and the monitored substation[24].The DNP3 master mainly sends read/write requests to the substation's Intelligent Electronic Devices (IEDs) through the outstation equipment. IEDs may also send unsolicited messages like alarms to the master DNP3 without being polled[23].SCADA data polling intervals are often between 2 to 10 seconds[25].This is open-source information and hence provides an avenue for bad actors to craft cyber intrusion strategies for the DNP3 protocol.

At the substation level IEEE 6185 communication among the connected devices makes use of GOOSE, Sample Value and MMS messages[8].Substation computers with direct links to these devices are susceptible to malware attacks as explored in the CRASHOVERRIDE attack on the Ukrainian power grid[2].Dictionary attacks can also leak authorization credentials,

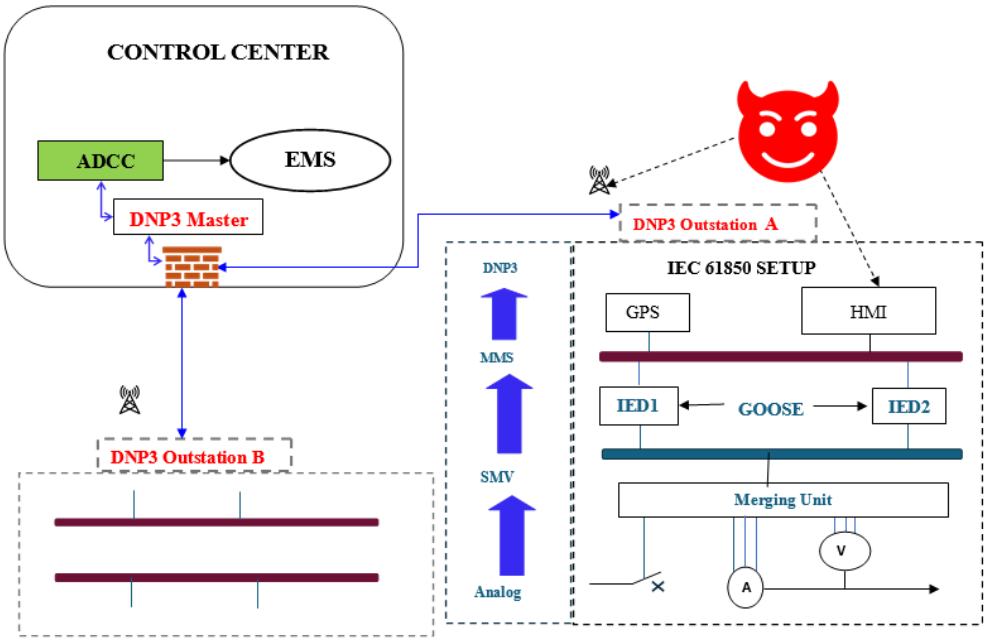

Figure 2.1: Communication set up and vulnerable points on the power grid

granting access through these computers for remote manipulation of data being sent to the control center.

Before measurement data leaves the substation to the control center, they are encapsulated in DNP3 packets and transmitted through the DNP3 link. This link is usually established over a wireless or fiber network privately owned by the utility or leased to a third-party agent. This section of the communication link also provides an entry point for false data injection or manipulation. Attackers can perform a man-in-the-middle, replay or reflection attacks targeting the SCADA data being polled. Even though the DNP3-SA provides some security for the exchange of packets,[8] reports that this security mechanism does not look at the payload.

The proposed anomaly detection for the control center will be sited at the entrance of the control center to look at the contents of the DNPs packets before they move into the energy management system as shown in Figure 2.1. Measurements from each connected bus and

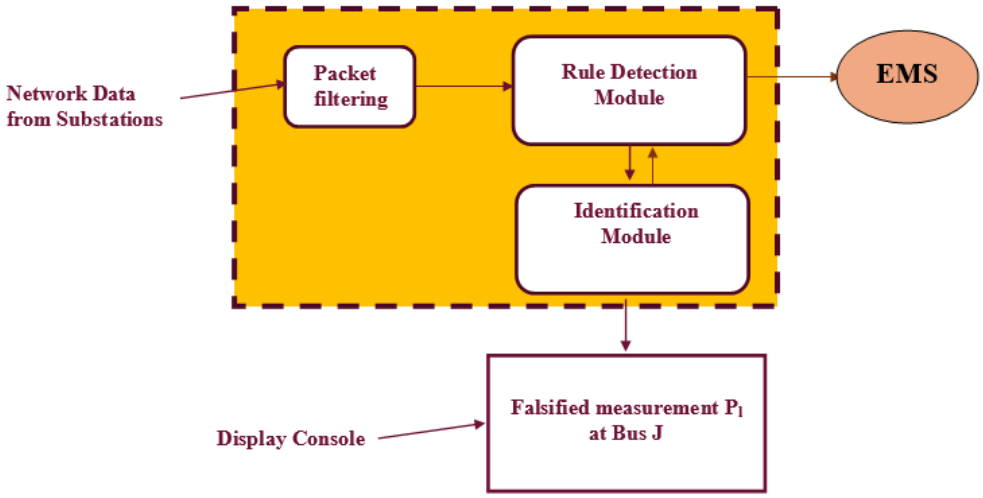

Figure 2.2: Model of ADCC

line in the power system network will be subjected to the fundamental laws of physics to determine anomalous data. Feedback will be visibly displayed for the viewing of the SCADA master. Falsified packets will be dropped, and their estimated measurements provided for system analysis.

2.1 System Model

The ADCC performs a security check on all measurement DNP3 packets received from all substations connected in the grid. These measurements arrive through the SCADA communication link. In this system, the control center also has PMU data collected from all substations. The sampling rate of PMU data is usually higher than that of the SCADA data. It is therefore important to have the dataset from the two sources synchronized to receive the optimal results.

Figure 2.2 provides a model of how the ADCC will operate. The packet filtering module will

ensure the relevant data is fed to the ADCC. The term relevant is used here to describe the information or measurement data needed for analysis. After filtering, the data goes through the detection module. In the detection module, each bus and branch measurement values at the same time stamp are subjected to the algorithm rules based on equations under section 3.5. If a set of measurements at a particular time instant sees a violation of any of the rules, the measurements are transferred to the identification module. However, if no violation is detected, measurement values proceed to the Energy management system (EMS).

At the identification module, the system uses circuit laws and Phasor Measurement Unit(PMU) data to estimate the falsified measurement value(s). The estimated value is compared with the SCADA value based on a defined threshold. If the threshold is violated the specific falsified measurement is identified. The SCADA data is dropped and replaced the estimated value to be sent into the EMS.

Chapter 3

Algorithm Formulation

The algorithm for the ADCC will be formulated in two (2) parts. The first part will be formulated from the fundamental laws of physics namely, Kirchoff's Voltage Law (KVL), Kirchoff's Current Law (KCL) and Ohm's Law. This study has however shown that if all measurements are available and Ohm's Law is satisfied, KVL will automatically be satisfied. This identity is termed, "the zero-loop sum identity". Therefore KVL will not be considered in formulating this part of the algorithm. The ADCC will evaluate a set of measurements at a particular time instant to determine if any of the laws are falsified. If falsification is identified, then the second part of the algorithm will be launched. The second part will identify the specific falsified measurement. This part will also provide an estimated value for the identified falsified measurement.

3.1 Proof of the zero-loop sum identity

The proof will be considered under two (2) scenarios. In this proof the assumption is that all measurements are available.

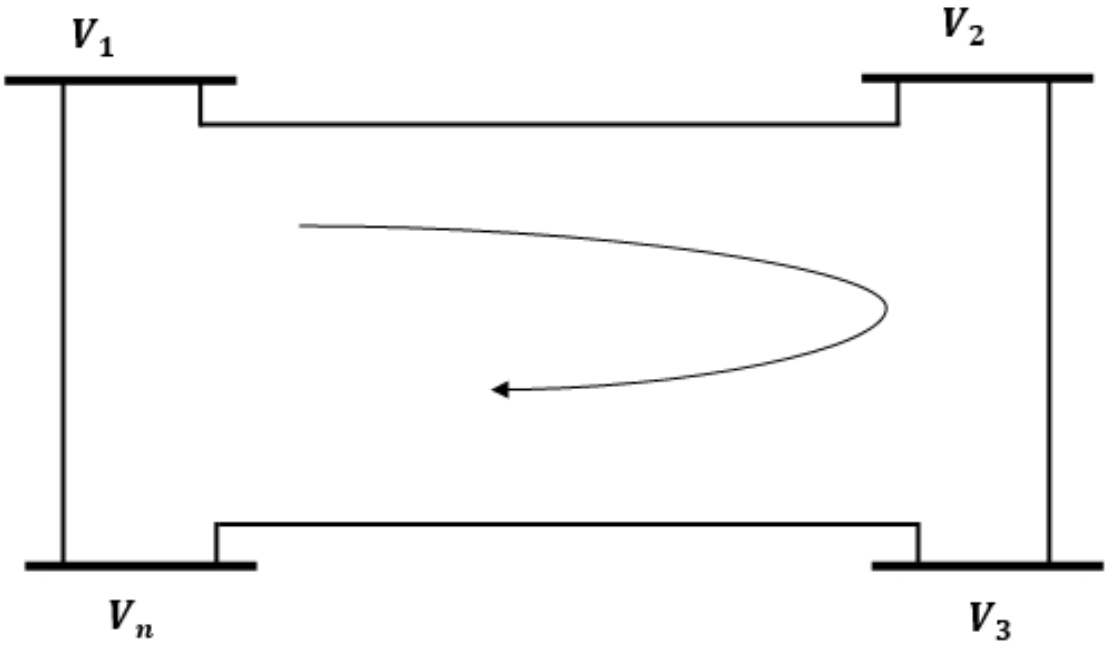

Figure 3.1: N Buses connected in a loop

3.1.1 Scenario 1

In this scenario, consider a loop formed by N buses that are connected by N branches. The connection is such that the Nth bus is connected to the first Bus to form the loop. See Figure 3.1.

According to Ohm's Law

$$V_1 - V_2 = I_{12}Z_{12}$$

$$V_2 - V_3 = I_{23}Z_{23}$$

$$\ldots$$

$$V_n - V_1 = I_{n1}Z_{n1}$$

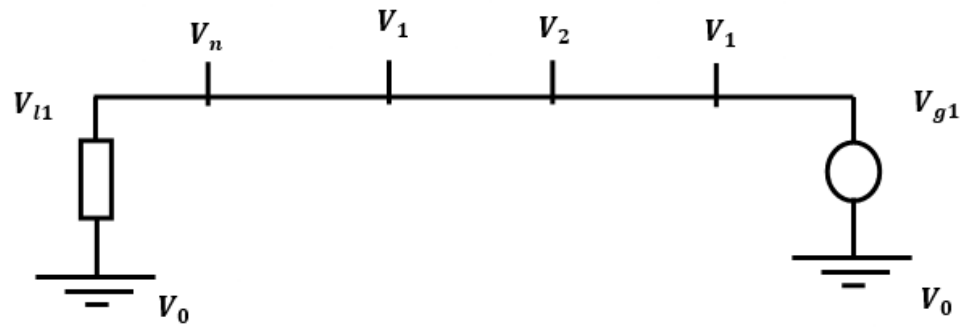

Figure 3.2: Loop on the power system formed by Generator and Load

Summing both sides,

$$I_{12}Z_{12} + ... + I_{n1}Z_{n1} = V_1 - V_2 + V_2 + ... - V_n + V_n - V_1 = 0 \tag{3.1}$$

This is known as the zero loop-sum identity. Therefore if Ohm's law is satisfied for all branches, then KVL will be satisfied.

3.1.2 Scenario 2

In this second scenario, consider a loop formed with the ground that has generation and load. This is depicted in Figure 3.2.

According to Ohm's Law

$$V_0 - V_{g1} = I_{g1}Z_{g1}$$

$$V_{g1} - V_1 = I_{1g1}Z_{1g1}$$

$$...$$

$$V_{l1} - V_0 = I_{l1}Z_{l1}$$

Summing both sides,

$$I_{g1}Z_{g1} + ... + I_{l1}Z_{l1} = V_0 - V_{g1} + V_{g1}... - V_{l1} + V_{l1} - V_0 = 0 \tag{3.2}$$

If V_0=0, then the equation becomes

$$\sum IZ = V_{g1} - V_{l1} \tag{3.3}$$

Again if Ohm's law is satisfied for all branches, then the zero-loop sum identity will lead to KVL being satisfied. Both scenarios have therefore proved that when all measurements for a loop are collected, the sum of the measurement values in the loop will be zero (satisfying KVL), only when Ohm's law is satisfied.

The algorithm will therefore be formulated from Ohm's law and KCL. This is an important finding since it reduces the computational burden of the algorithm. It is worth noting that at the control center the SCADA measurements available include voltage measurements, power flow measurements, load, and power generation. The algorithm will therefore be formulated with this in mind.

3.2 Detection Phase: Ohm's Law Check

From Figure 4, two substations, I and J are shown to be connected. These substations are assumed to have a generator and load connected. This is to make a general case for all buses connected in a system. The power injections have also been labelled. See Figure 3.3

On the assumption that a very negligible charging current flows to ground on the transmission line, and $cos\ (\theta_{vi} - \theta_{vj}) \approx 1$,equations 3.4 and 3.5 can be formulated for the ohm's law check.

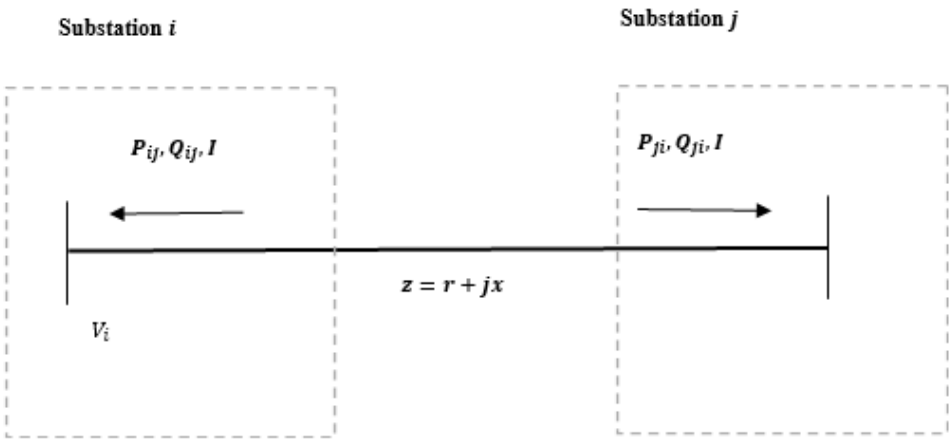

Figure 3.3: Single line diagram of two connected substations

For each branch I $\leftrightarrow$ J, the Ohm's Law check in the algorithm will be,

$$|V_i|^2 + |V_j|^2 - 2|V_i||V_j| - r(P_{ij} + P_{ji}) - x(Q_{ij} + Q_{ji}) = 0 \tag{3.4}$$

$$(P_{ij} + P_{ji})x - (Q_{ij} + Q_{ji})r = 0 \tag{3.5}$$

This forms the Ohm's law condition for this algorithm.

3.3 Detection Phase: KCL Check/ Conservation of Complex Powers

According to KCL, the algebraic sum of all currents at bus I is zero. Thus

$$\sum I_{iG} - \sum I_{iL} = \sum_{j=1}^{N} I_{ij} \tag{3.6}$$

Multiplying through by V_i, the equation becomes Equation 3.7

$$\sum (P_{iG} + jQ_{iG}) - \sum (P_{iL} + jQ_{iL}) = \sum_{j=1}^{N} (P_{ij} + jQ_{ij}) \tag{3.7}$$

From 3.7, KCL becomes the conservation of complex powers (CoCP). Equating real and imaginary parts, equations 3.8 and 3.9 are obtained.

$$\sum P_{iG} - \sum P_{iL} = \sum_{j=1}^{N} P_{ij} \tag{3.8}$$

$$\sum Q_{iG} - \sum Q_{iL} = \sum_{j=1}^{N} Q_{ij} \tag{3.9}$$

Equations 3.8 and 3.9 will feed into the algorithm as the CoCP check. These equations will check for potential falsified measurements at each bus.

3.4 Impact of Instrument Errors

Measurements from instrument transformers come with some errors. The measurement error rate of CTs and PTs at the substation tend to be small. For instance, a PT with accuracy class of 0.1 has a percentage voltage error of $\pm$ 0.1%, whereas a PT with an accuracy class of 0.2 has a percentage voltage error of $\pm$ 0.2% [26]. To minimize the rate of false alarms, the accuracy class of the instrument transformers will be used to determine the thresholds in the algorithm.

Let there be an instrument with a small ±k error rate, and a true value of y_{tr} to be measured. Then the maximum measurement that the instrument may record is given by equation 3.10

$$y = y_{tr} + y_{err} = y_{tr} + ky_{tr} \tag{3.10}$$

However, since k is small, it follows that:

$$ky \approx ky_{tr} \tag{3.11}$$

Hence, the measurement error,ky_{tr}, may be approximated by ky, the product of the measured value and the error rate. Let $\pm k_{vi}$ be the error rate of the PT at the ith substation, and $\pm k_{ci}$ be the error rate of the CT at the same substation. It should be noted that a substation may have a PT and CT on each line terminating at the substation. Thus, there may be more than one PT and CT. For this, each substation may be thought of as a cluster of substations.

Since measurement data received at the control center are mainly Bus voltages, active and reactive power, it is important to determine the accuracy class for measurement of power.

$$k_p = k_c \pm k_v \pm k_c k_v \tag{3.12}$$

$$k_q = k_c \pm k_v \pm k_c k_v \tag{3.13}$$

Where k_p and k_q are the accuracy class components for active and reactive Power measurement in the equation k_c and k_v are the accuracy classes for CT and PT measuring the current and voltage respectively on the line whose power is being measured.

3.5 Equations for Detection phase of the algorithm

For each line, the error tolerance is obtained from Ohm's Law across bus I and bus J on the two sides of the line:

$$|V_i^2 + V_j^2 - 2V_iV_j - (P_{ij} + P_{ji})r_{ij} - (Q_{ij} + Q_{ji})x_{ij}| \leq |k_{vi}^2 V_i^2| + |k_{vj}^2 V_j^2| + |2k_{vi}k_{vj}V_iV_j| + |r_{ij}k_{ij}P_{ij}| + |r_{ij}k_{ji}P_{ji}| + |x_{ij}k_{ij}Q_{ij}| + |x_{ij}k_{ji}Q_{ji}| \quad (3.14)$$

$$|(P_{ij} + P_{ji})x_{ij} - (Q_{ij} + Q_{ji})x_{ij} \leq |x_{ij}k_{ij}P_{ij}| + |x_{ij}k_{ji}P_{ji}| + |r_{ij}k_{ij}Q_{ij}| + |r_{ij}k_{ji}Q_{ji}| \quad (3.15)$$

For each bus, the conservation of P and Q, respectively, is satisfied if the following inequalities hold.

$$|\sum P_{iG} - \sum P_{iL} - \sum_{1}^{N} P_{ij}| \leq |\sum k_{iG}P_{iG}| + |\sum k_{iL}P_{iL}| + |\sum_{j=1}^{N} k_{ij}P_{ij}| \quad (3.16)$$

$$|\sum Q_{iG} - \sum Q_{iL} - \sum_{1}^{N} Q_{ij}| \leq |\sum k_{iG}Q_{iG}| + |\sum k_{iL}Q_{iL}| + |\sum_{j=1}^{N} k_{ij}Q_{ij}| \quad (3.17)$$

If this part of the algorithm successfully detects a falsified measurement, then the next part will set in.

3.6 Identification Phase: Identifying the specific falsified measurement

The second part of the algorithm only kick-starts after Part A is verified. The goal is to identify the specific falsified measurement for which reason the bus or branch algorithm has

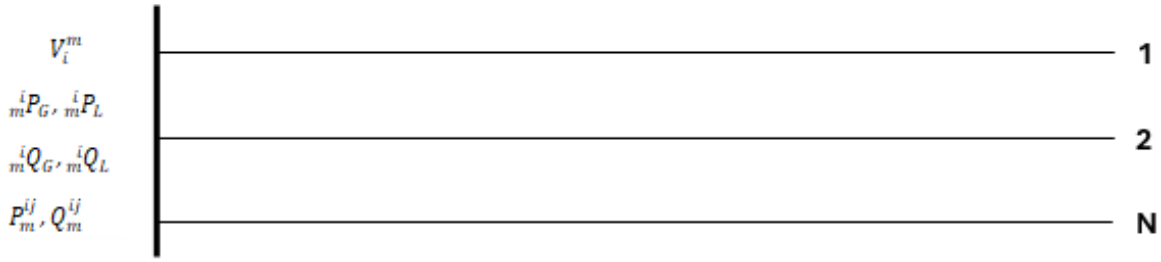

Figure 3.4: Single Bus, I connected to N buses

failed. Different scenarios will be looked at to identify the falsified measurement.

3.6.1 Scenario 1A

In this scenario,it is assumed that Bus I, connected to N buses, is compromised.All connected Bus and branch algorithms have passed Part A at the adjacent buses. This means that the intruder is at Substation I. Parameters from the adjacent buses can be used to determine the specific falsified measurement at Substation I. See Figure 3.4

Let: V_i^m and V_i^c be the measured SCADA and estimated voltage magnitude of Bus I respectively

P_{iG}^m and P_{iG}^c be the measured SCADA and estimated Active Power generated at Bus I respectively

P_{iL}^m and P_{iL}^c be the measured SCADA and estimated Active Load Power at Bus I respectively

Q_{iG}^m and Q_{iG}^c be the measured SCADA and estimated Reactive Power generated at Bus I respectively

Q_{iL}^m and Q_{iL}^c be the measured SCADA and estimated Reactive Load Power at Bus I respectively

P_{ij}^m and P_{ij}^c be the measured SCADA and estimated Active Power flow at Bus I respectively

Q_{ij}^m and Q_{ij}^c be the measured SCADA and estimated Reactive Power flow at Bus I respectively From the branch flow model[27], the line flow measurements at Bus I can be estimated, knowing all values from adjacent buses are correct since they passed the algorithm in part A.

Compute P_{ij}^c and Q_{ij}^c from 3.18

$$P_{ij}^c = \sum_j^N \left(\frac{R_{ji}(P_{ji}^m)^2 + R_{ji}(Q_{ji}^m)^2}{(V_j^m)^2} - P_{ji}^m \right) \tag{3.18a}$$

$$Q_{ij}^c = \sum_j^N \left(\frac{X_{ji}(P_{ji}^m)^2 + X_{ji}(Q_{ji}^m)^2}{(V_j^m)^2} - Q_{ji}^m \right) \tag{3.18b}$$

The solution to equation 3.18, P_{ij}^c and Q_{ij}^c, provides a value that estimates the line flow measurement at Bus I. This will be compared with the measurement received for that parameter so that we can validate that measurement.

Check if condition 3.19 below is satisfied

$$|P_{ij}^m - P_{ij}^c| \leq |k_{ij} P_{ij}^c| \tag{3.19a}$$

$$|Q_{ij}^m - Q_{ij}^c| \leq |k_{ij} Q_{ij}^c| \tag{3.19b}$$

The premise of this condition is that the deviation from the actual measurement should be very minimal. Consequently, staying within the error bounds. The difference between the measured value and the one computed should not be more than the error tolerance of the estimated line flow value.

If condition 3.19 is not satisfied, then P_{ij}^m or Q_{ij}^m is a falsified measurement so raise an

alarm.Keep P_{ij}^c or Q_{ij}^c (depending on the specific falsified measurement) for subsequent computations wherever P_{ij}^m or Q_{ij}^m is needed. Instead of throwing away the falsified measurement value it will be replaced with the estimated measurement when being sent to the energy management system (EMS) for state estimation. This eliminates the second observability check that goes on in state estimation when an outlier is found in a set of measurement data.All parameters used to evaluate equation 3.18 can be trusted since they have successfully passed the first part of the algorithm.

Having confirmed the line flow measurement value, the next step is to estimate the bus voltage at Bus I. As stated earlier, conditions 3.19 will help determine the line flow measurements that will be used in this step. Compute V_i^c from equation 3.20 below:

$$V_i^c = \sum_j^N \sqrt{\left(\frac{R_{ij}(P_{ij}^m)^2 + R_{ij}(Q_{ij}^m)^2}{P_{ij}^m + P_{ji}^m}\right)} \tag{3.20}$$

Check if condition 3.21 is satisfied

$$|V_i^m - V_i^c| \leq |k_v V_i^c| \tag{3.21}$$

Condition 3.21 is meant to ensure that the measured value for the Bus Voltage at Bus I is within its error bounds. The difference between the measured and estimated value should not be greater than the error limit on voltage magnitude at Bus I.

If condition 3.21 is not satisfied, then V_i^m is falsified so, raise an alarm for falsified V_i^m. Keep V_i^c for subsequent computations where V_i^m is needed and discard V_i^m. However, if condition 3.21 is satisfied, then V_i^m is correct and can be kept and used for subsequent evaluations.

After confirming the values of the measurement parameters in the earlier steps, the next step is to evaluate the parameters in the substation. We consider two (2) cases; a load (P-Q)

bus and a generation (P-V) bus.

CASE 1: If I is a Load Bus

For this case, the net line flow measurement should be equal to the net power absorbed by connected load according to KCL. This is computed in the next step for equation 3.22. This provides an estimate of how the net power absorbed by the load connected to the bus should be. Estimate P_{iL}^{c} and Q_{iL}^{c} from 3.22

$$P_{iL}^{c} = -P_{ij}^{m} \tag{3.22a}$$

$$Q_{iL}^{c} = -Q_{ij}^{m} \tag{3.22b}$$

Check for condition 3.23

$$|P_{iL}^{m} - P_{iL}^{c}| \leq |k_{iL} P_{iL}^{c}| \tag{3.23a}$$

$$|Q_{iL}^{m} - Q_{iL}^{c}| \leq |k_{iL} Q_{iL}^{c}| \tag{3.23b}$$

The difference between the measured values for the power absorbed by the load and the estimated value should not exceed the error tolerance as shown in condition 3.23

If condition 3.23 is not satisfied, then P_{iL}^{c} and/or Q_{iL}^{c} is falsified so raise alarm for falsified P_{iL}^{c} and/or Q_{iL}^{c}. In that case, discard the SCADA measurement and replace with the estimated value computed from equation 3.23. However, if the measured value is within the error tolerance, then the SCADA measurement will be kept and used for subsequent evaluations.

CASE 2: If I is a Generation Bus

In this case, it is necessary to have additional measurement values to be able to evaluate the specific contributor to the net injected power that has been falsified. In that sense, the PMU measurement readings from the substation will be used. In this scenario, the PMU measurements from substation I will be used to aid further analyses of the SCADA measurements received . The PMU measurement data is assuemed to be secured from falsification in this study.

Evaluate P^u_{iG}, P^u_{iL}, Q^u_{iG} and Q^u_{iL} from the available PMU data from equation 3.24.

$$P^u_{iG} = V^u_i I^u_g \cos\ (\theta_{vi} - \theta_{ig}) \tag{3.24a}$$

$$P^u_{iL} = V^u_i I^u_L \cos\ (\theta_{vi} - \theta_{iL}) \tag{3.24b}$$

$$Q^u_{iG} = V^u_i I^u_g \sin(\theta_{vi} - \theta_{ig}) \tag{3.24c}$$

$$Q^u_{iL} = V^u_i I^u_L \sin\ (\theta_{vi} - \theta_{iL}) \tag{3.24d}$$

To determine the specific measurement which has been falsified, it is assumed that the correct measurement values for the parameters in equation 3.24 should be approximately equal to what has been calculated. With that in mind, the net injected power for each parameter is computed and compared with the line flow measurement.

Evaluate equation 3.25

$$P^m_{iG} - P^u_{iL} = P^{check}_{iG} \tag{3.25a}$$

$$P^u_{iG} - P^m_{iL} = P^{check}_{iL} \tag{3.25b}$$

$$Q^m_{iG} - Q^u_{iL} = Q^{check}_{iG} \tag{3.25c}$$

$$Q^u_{iG} - Q^m_{iL} = Q^{check}_{iL} \tag{3.25d}$$

In each case, one of the parameters being validated will be evaluated with the PMU value and the result (net injected power) is tagged with the parameter being checked as shown in equation 3.25. Conditions are formulated to identify the specific falsified measurements. This condition will be situated on the line flow values already confirmed from previous steps

Check the following conditions

$$|P_{iG}^{check} - \sum_{1}^{N} P_{ij}| \leq |\sum_{j=1}^{N} k_{ij} P_{ij}| \tag{3.26a}$$

$$|P_{iL}^{check} - \sum_{1}^{N} P_{ij}| \leq |\sum_{j=1}^{N} k_{ij} P_{ij}| \tag{3.26b}$$

$$|Q_{iG}^{check} - \sum_{1}^{N} Q_{ij}| \leq |\sum_{j=1}^{N} k_{ij} Q_{ij}| \tag{3.26c}$$

$$|Q_{iL}^{check} - \sum_{1}^{N} Q_{ij}| \leq |\sum_{j=1}^{N} k_{ij} Q_{ij}| \tag{3.26d}$$

The difference between the estimated net injection and the line flow value should not exceed the error tolerance of the line flow measurement. This is the basis for condition 3.26. We can therefore make the following deductions.

If 3.26a is not satisfied, then P_{iG}^{m} is falsified so raise an alarm for falsified P_{iG}^{m}

If 3.26b is not satisfied, then $P_{iL}^{m}$is falsified so raise an alarm for falsified P_{iL}^{m}

If 3.26c is not satisfied, then Q_{iG}^{m} is falsified so raise an alarm for falsified Q_{iG}^{m}

If 3.26dis not satisfied, then Q_{iL}^{m} is falsified so raise an alarm for falsified Q_{iL}^{m}

For any of the conditions not satisfied, the value is discarded, and the corresponding PMU value evaluated from equation 3.24 is sent in its stead to the Energy Management System. However, if the condition is satisfied, the SCADA measurement as accurate for further

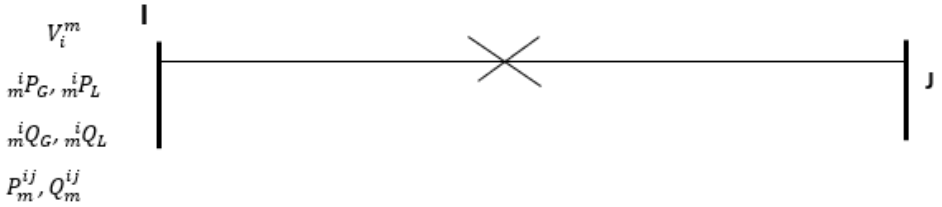

Figure 3.5: Compromised Branch

analysis.

3.6.2 Scenario 1B: Falsified Branch measurement

To find the specific measurement that has been falsified, consider the injected power at the connected buses, thus bus I and J. See Figure 3.5. In this scenario, it is possible that one or both buses may have passed the algorithm for CoCP in Part A. This does not guarantee that the measurement values captured are accurate especially when the branch algorithm has failed. It is therefore important to start by validating the net injected power at each bus. This will enable us find which line flow parameter(s) have been falsified. Equation 3.24 provides PMU values for generation and load. It also provides an idea of how the injected power on the buses should be. The SCADA measurements received are compared with the PMU values and the difference should be minimal, not going beyond the error tolerance of the PMU measurement value. This forms the premise for condition 3.27. Validation is done

for buses I and J.

$$|P^m_{iG} - P^u_{iG}| \leq |k_{iG}P^u_{iG}| \tag{3.27a}$$

$$|P^m_{iL} - P^u_{iL}| \leq |k_{iL}P^u_{iL}| \tag{3.27b}$$

$$|Q^m_{iG} - Q^u_{iG}| \leq |k_{iG}Q^u_{iG}| \tag{3.27c}$$

$$|Q^m_{iL} - Q^u_{iL}| \leq |k_{iL}Q^u_{iL}| \tag{3.27d}$$

$$|V^m_i - V^u_i| \leq |k_{iv}V^u_i| \tag{3.27e}$$

$$|P^m_{jG} - P^u_{jG}| \leq |k_{jG}P^u_{jG}| \tag{3.27f}$$

$$|P^m_{jL} - P^u_{jL}| \leq |k_{jL}P^u_{jL}| \tag{3.27g}$$

$$|Q^m_{jG} - Q^u_{jG}| \leq |k_{jG}Q^u_{jG}| \tag{3.27h}$$

$$|Q^m_{jL} - Q^u_{jL}| \leq |k_{jL}Q^u_{jL}| \tag{3.27i}$$

$$|V^m_j - V^u_j| \leq |k_{jv}V^u_j| \tag{3.27j}$$

Should any of the conditions fail, raise an alarm for falsified SCADA measurement and discard. Keep the corresponding PMU measurement for subsequent analysis. If a condition is satisfied, then the original values measured at Bus I and J can be used for subsequent analysis.

The next step will be to evaluate the expected net power injection at each bus. Having confirmed the trusted measurement values under condition 3.27, it is possible to evaluate the net injected power at each Bus. If the Bus is not a generator bus, the generation component in equation 3.28 automatically becomes zero and the load component evaluated. The reverse occurs if there is no connected load but there is generation. In the event where there is no generation or load at the bus the line flow measurements will be used to evaluate the power balance at that bus.

Let: P_i be the net injected active power at bus I

Q_i be the net injected reactive power at bus I

P_j be the net injected active power at bus J

Q_j be the net injected reactive power at bus J

These parameters are evaluated from equation 3.28

$$P^m_{iG} - P^m_{iL} = P_i \tag{3.28a}$$

$$Q^m_{iG} - Q^m_{iL} = Q_i \tag{3.28b}$$

$$P^m_{jG} - P^m_{jL} = P_j \tag{3.28c}$$

$$Q^m_{jG} - Q^m_{jL} = Q_j \tag{3.28d}$$

Knowing the net injected power, we proceed to estimate the corresponding line flow measurements at the adjacent bus

$$P^c_{ij} = \frac{R_{ji}(P_j)^2 + R_{ji}(Q_j)^2}{(V_j)^2} - P_j \tag{3.29a}$$

$$Q^c_{ij} = \frac{X_{ji}(P_j)^2 + X_{ji}(Q_j)^2}{(V_j)^2} - Q_j \tag{3.29b}$$

$$P^c_{ji} = \frac{R_{ij}(P_i)^2 + R_{ij}(Q_i)^2}{(V_i)^2} - P_i \tag{3.29c}$$

$$Q^c_{ji} = \frac{X_{ij}(P_i)^2 + X_{ij}(Q_i)^2}{(V_i)^2} - Q_i \tag{3.29d}$$

The line flow measurements evaluated in equation 3.29 can be used to estimate the expected SCADA measurements at each bus. The difference between the SCADA measurement and the estimated value in equation 3.29 should not exceed the error tolerance for each line flow

measurement. This forms the basis for condition 3.30 below.

$$|P_{ij}^m - P_{ij}^c| \leq |k_{ij} P_{ij}^c| \tag{3.30a}$$

$$|P_{ji}^m - P_{ji}^c| \leq |k_{ij} P_{ji}^c| \tag{3.30b}$$

$$|Q_{ij}^m - Q_{ij}^c| \leq |k_{ij} Q_{ij}^c| \tag{3.30c}$$

$$|Q_{ji}^m - Q_{ji}^c| \leq |k_{ji} Q_{ji}^c| \tag{3.30d}$$

Should any of the conditions fail, raise an alarm for falsified SCADA measurement and discard. Keep the corresponding estimated measurement for subsequent analysis. If a condition is satisfied, then the original values measured at Bus I and J can be used for subsequent analysis.

It is worth nothing that this study finds this method of evaluation similar to the case where two adjacent buses or connected buses have been compromised. In such a case, even if the branch algorithms are satisfied the measurement values cannot be trusted. This is because the branch flow measurements are not guaranteed to be valid. This will therefore mean that all injected and line flow measurements will be re-evaluated as has been seen in scenario 1B.

3.6.3 Scenario 1C: Compromised branch connected to other uncompromised branches or buses

Suppose Bus I is connected to Bus H and Bus J connected to Bus K. Such that both Bus and branch algorithms pass for (Bus H, K and branch I→H and branch J→K). This scenario is depicted in Figure 3.6 The net injected Power from both buses (I and J) as calculated from equation 3.28 after evaluation and validation from condition3.27. This is equivalent to the sum of power flow at both buses. Let H and K be a group of uncompromised buses

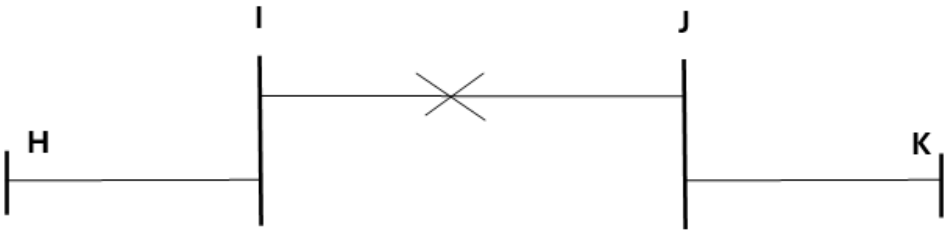

Figure 3.6: Compromised Branch connected to Other Buses

connected to I and J respectively. The net injection can be expressed below

$$P_i = P_{ij} + \sum_{h=1}^{N} P_{ih}^m \tag{3.31a}$$

$$Q_i = Q_{ij} + \sum_{h=1}^{N} Q_{ih}^m \tag{3.31b}$$

$$P_j = P_{ji} + \sum_{k=1}^{N} P_{jk}^m \tag{3.31c}$$

$$Q_j = Q_{ji} + \sum_{k=1}^{N} Q_{jk}^m \tag{3.31d}$$

They will be used to estimate what the calculated values in equation 3.32 should be.

Evaluate equation 3.32

$$P_{ij}^{c} = \frac{R_{ji}(P_j - \sum_{k=1}^{N} P_{jk}^{m})^2 + R_{ji}(Q_j - \sum_{k=1}^{N} Q_{jk}^{m})^2}{(V_j)^2} - P_j + \sum_{k=1}^{N} P_{jk}^{m} \tag{3.32a}$$

$$Q_{ij}^{c} = \frac{X_{ji}(P_j - \sum_{k=1}^{N} P_{jk}^{m})^2 + X_{ji}(Q_j - \sum_{k=1}^{N} Q_{jk}^{m})^2}{(V_j)^2} - Q_j + \sum_{k=1}^{N} Q_{jk}^{m} \tag{3.32b}$$

$$P_{ji}^{c} = \frac{R_{ij}(P_i - \sum_{h=1}^{N} P_{ih}^{m})^2 + R_{ij}(Q_i - \sum_{h=1}^{N} Q_{ih}^{m})^2}{(V_i)^2} - P_i + \sum_{h=1}^{N} P_{ih}^{m} \tag{3.32c}$$

$$Q_{ji}^{c} = \frac{X_{ij}(P_i - \sum_{h=1}^{N} P_{ih}^{m})^2 + X_{ij}(Q_i - \sum_{h=1}^{N} Q_{ih}^{m})^2}{(V_i)^2} - Q_i + \sum_{h=1}^{N} Q_{ih}^{m} \tag{3.32d}$$

The computed measurement values will then be the ones to be compared with the measurement values received. These estimated measurement values provide an estimated power flow value at each bus. The SCADA measurements received are compared with the estimated values in condition 3.30. The difference should not exceed the error tolerance of the estimated line flow measurements.

Similar conclusions and evaluations are made from the outcome of the checks made on condition 3.30.For any condition not satisfied, the SCADA measurements are discarded, and the estimated values used in subsequent analysis. However, for any condition that is satisfied, the SCADA measurements are deemed usable and true. This measurement value will be used in subsequent analysis.

3.6.4 Scenario 2A: Compromised adjacent Buses with one connected to an uncompromised bus,K

In this scenario, a compromised terminal Bus J is depicted to be connected to another compromised Bus I. However, in this scenario, Bus I is connected to a group of uncompromised

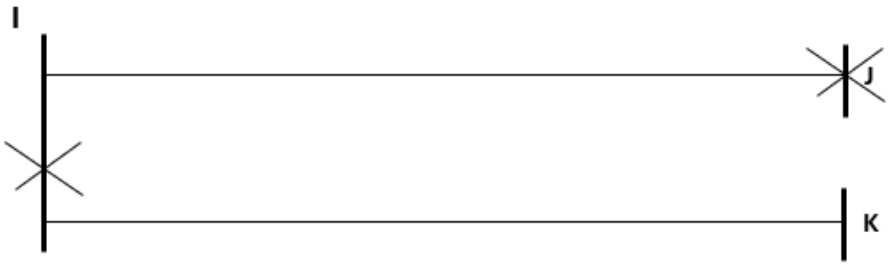

Figure 3.7: Scenario 2A

Buses, known here as Bus K. This scenario is depicted in 3.7 There is doubt about the measurement values received from Buses I and J. From Bus K, the line flow values, P_{ik}^{m} and Q_{ik}^{m} can be estimated and analysed. It is possible do so because the measurement values received from the uncompromised Buses can be trusted since they passed the first part of our algorithm.

Evaluate line flow values from equation 3.33

$$P_{ik}^{c} = \sum_{k}^{N} \left(\frac{R_{ki}(P_{ki}^{m})^2 + R_{ki}(Q_{ki}^{m})^2}{(V_{k}^{m})^2} - P_{ki}^{m} \right) \tag{3.33a}$$

$$Q_{ik}^{c} = \sum_{k}^{N} \left(\frac{X_{ki}(P_{ki}^{m})^2 + X_{ki}(Q_{ki}^{m})^2}{(V_{k}^{m})^2} - Q_{ki}^{m} \right) \tag{3.33b}$$

After evaluation, check for condition 3.34 below:

$$|P_{ik}^{m} - P_{ik}^{c}| \leq |k_{ik} P_{ik}^{c}| \tag{3.34a}$$

$$|Q_{ik}^{m} - Q_{ik}^{c}| \leq |k_{ij} Q_{ik}^{c}| \tag{3.34b}$$

It follows from the established steps that if any of these thresholds are breached, an alarm should be raised for the specific measurement.

The SCADA measurement is deemed falsified if its deviation from the estimated value in equation 3.33 is greater than the estimated line flow tolerance. Such falsified measurements are discarded, and the corresponding estimated value kept for subsequent analysis. Otherwise, the SCADA measurement is kept and used for analysis. The next step is to evaluate the line flow measurements corresponding to the two compromised buses. Equations 3.35 will be used for our estimation.

$$P_{ij}^{c} = \frac{R_{ji}(P_j)^2 + R_{ji}(Q_j)^2}{(V_j)^2} - P_j \tag{3.35a}$$

$$Q_{ij}^{c} = \frac{X_{ji}(P_j)^2 + X_{ji}(Q_j)^2}{(V_j)^2} - Q_j \tag{3.35b}$$

$$P_{ji}^{c} = \frac{R_{ij}(P_i - \sum_{h=1}^{N} P_{ik}^{m})^2 + R_{ij}(Q_i - \sum_{k=1}^{N} Q_{ik}^{m})^2}{(V_i)^2} - P_i + \sum_{k=1}^{N} P_{ik}^{m} \tag{3.35c}$$

$$Q_{ji}^{c} = \frac{X_{ij}(P_i - \sum_{h=1}^{N} P_{ik}^{m})^2 + X_{ij}(Q_i - \sum_{k=1}^{N} Q_{ik}^{m})^2}{(V_i)^2} - Q_i + \sum_{k=1}^{N} Q_{ik}^{m} \tag{3.35d}$$

Where the net injected power into buses I and J are computed from equation 3.28 when condition 3.27 is satisfied. In those steps the true measurement value is confirmed and the suspected falsified measurement discarded.

Equation 3.35 provides an estimated value for the line flow measurements at both buses. These estimated values will form the basis for the decisions in condition 3.30. As shown in prior conditions, the deviation of the measured values from the computed ones are expected to be minimal and within the error tolerance. In similar manner, check for condition 3.30 and take same decisions when any of the conditions are violated. A measurement value deemed falsified after checking condition 3.30 is discarded and replaced by the estimated value in subsequent analysis.

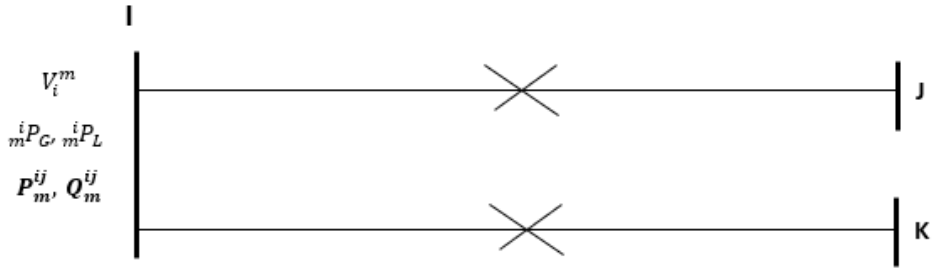

Figure 3.8: Scenario 2B

3.6.5 Scenario 2B: Two Compromised adjacent Branches

The scenario depicted in this section is also applicable to three connected buses arranged in series as shown in Figure 3.8. In this scenario, even if the bus algorithm passes for all three buses, bus bus measurements will have to be validated before being used for further evaluation. The case will however be different if any of the terminal Buses, J or K were connected to uncompromised branch and Buses. This solution will also be employed if all the three buses were compromised. To validate the line flow parameters on the falsified branches, the validated Bus parameters for I, J and K will be used. This will be done by first estimating equation 3.24 for all the buses. The next step will be to check for condition 3.27 to ascertain the correct values that will be used to compute the net injected bus power using equation 3.28. Knowing the net injected power on each Bus, the line flow measurements can then be computed and validated. At Bus I,

$$P_i = P_{ij} + P_{ik} \tag{3.36a}$$

$$Q_i = Q_{ij} + Q_{ik} \tag{3.36b}$$

Knowing P_j and Q_j,P_k and Q_k, from equation 3.28, we can evaluate power flow parameters

P_{ij}^c ,Q_{ij}^c, P_{ik}^c,and Q_{ik}^c from equation 3.37

$$P_{ij}^c = \frac{R_{ji}(P_j)^2 + R_{ji}(Q_j)^2}{(V_j)^2} - P_j \tag{3.37a}$$

$$Q_{ij}^c = \frac{X_{ji}(P_j)^2 + X_{ji}(Q_j)^2}{(V_j)^2} - Q_j \tag{3.37b}$$

$$P_{ik}^c = \frac{R_{ki}(P_k)^2 + R_{ki}(Q_k)^2}{(V_k)^2} - P_k \tag{3.37c}$$

$$Q_{ik}^c = \frac{X_{ki}(P_k)^2 + X_{ki}(Q_k)^2}{(V_k)^2} - Q_k \tag{3.37d}$$

In this equation, the net injected power is used to estimate the line flow measurements at Bus I. The estimated values will then be used to validate the measured values using condition 3.38

$$|P_{ij}^m - P_{ij}^c| \leq |k_{ij} P_{ij}^c| \tag{3.38a}$$

$$|Q_{ij}^m - Q_{ij}^c| \leq |k_{ij} Q_{ij}^c| \tag{3.38b}$$

$$|P_{ik}^m - P_{ik}^c| \leq |k_{ik} P_{ik}^c| \tag{3.38c}$$

$$|Q_{ik}^m - Q_{ik}^c| \leq |k_{ij} Q_{ik}^c| \tag{3.38d}$$

From condition 3.38, if any of the measurement values for P_{ij}^c ,Q_{ij}^c, P_{ik}^c,and Q_{ik}^c fail to satisfy the limits of its threshold, an alarm is raised for falsified measurement. The deviation is not expected to go beyond the tolerance threshold of the estimated line flow measurement.

Falsified SCADA measurements will subsequently be discarded, and the corresponding estimated value used for subsequent analysis. Otherwise, keep the SCADA measurements for subsequent evaluation. Next will be to determine the line flow measurements at Buses J and

K from equation 3.39

$$P^c_{ji} = \frac{R_{ij}(P_i - P_{ik})^2 + R_{ij}(Q_i - Q_{ik})^2}{(V_i)^2} - P_i + P_{ik} \tag{3.39a}$$

$$Q^c_{ji} = \frac{X_{ij}(P_i - P_{ik})^2 + X_{ij}(Q_i - Q_{ik})^2}{(V_i)^2} - Q_i + Q_{ik} \tag{3.39b}$$

$$P^c_{ki} = \frac{R_{ik}(P_i - P_{ij})^2 + R_{ik}(Q_i - Q_{ij})^2}{(V_i)^2} - P_i + P_{ij} \tag{3.39c}$$

$$Q^c_{ki} = \frac{X_{ik}(P_i - P_{ij})^2 + X_{ik}(Q_i - Q_{ij})^2}{(V_i)^2} - Q_i + Q_{ij} \tag{3.39d}$$

Note that the values of P_{ik}, Q_{ik}, P_{ij}, and Q_{ij} used in equation 3.39, be it the calculated or the measured value will depend on the outcome of condition3.38. Validating the line flow measurements in condition 3.38 paves way to further estimate the corresponding line flow measurements at Buses J and K

After evaluating the values in equation 3.39, check for condition 3.40

$$|P^m_{ji} - P^c_{ji}| \leq |k_{ji} P^c_{ji}| \tag{3.40a}$$

$$|Q^m_{ji} - Q^c_{ji}| \leq |k_{ji} Q^c_{ji}| \tag{3.40b}$$

$$|P^m_{ki} - P^c_{ki}| \leq |k_{ki} P^c_{ki}| \tag{3.40c}$$

$$|Q^m_{ki} - Q^c_{ki}| \leq |k_{ki} Q^c_{ki}| \tag{3.40d}$$

An alarm is raised for any of the measurement values that fail to meet the thresholds set in condition3.40. Falsified measurements are discarded, and the estimated values kept for subsequent analysis.

3.6.6 Scenario 2C: Compromised Bus, I, connected to Buses

Suppose Bus I is connected to multiple buses such that I is a compromised Bus.

Let J a) be a set of compromised Buses or compromised Branch I↔J and, b) is not connected to any other Bus or connected to uncompromised Buses and Branches

Let K be a) a set of uncompromised buses and b) Branch I↔K is uncompromised. The goal is to identify the specific falsified measurements in Buses under J

Firstly, $\forall K$ compute the P_{ik}^{c} and Q_{ik}^{c} from equation 3.41

$$P_{ik}^{c} = \frac{R_{ki}(P_{ki})^2 + R_{ki}(Q_{ki})^2}{(V_k)^2} - P_{ki} \tag{3.41a}$$

$$Q_{ik}^{c} = \frac{X_{ki}(P_{ki})^2 + X_{ji}(Q_{ki})^2}{(V_k)^2} - Q_{ki} \tag{3.41b}$$

Check condition 3.42 to confirm if the values have been falsified or not. For all estimated line flow measurements in K, check condition,

$$|P_{ik}^{m} - P_{ik}^{c}| \leq |k_{ik}P_{ik}^{c}| \tag{3.42a}$$

$$|Q_{ik}^{m} - Q_{ik}^{c}| \leq |k_{ik}Q_{ik}^{c}| \tag{3.42b}$$

Next, compute the net injected power from all buses in group J and Bus I. To do this, First evaluate equation 3.24 for all the Buses in J and Bus I. Check for condition 3.27 to ascertain the correct values that will be used to compute the net injected bus power P_i,Q_i,P_j and Q_j ($\forall$ J) using equation 3.28.

At Bus I,

$$P_i = \sum_{j=1}^{N} P_{ij} + \sum_{k=1}^{N} P_{ik} \tag{3.43a}$$

$$Q_i = \sum_{j=1}^{N} Q_{ij} + \sum_{k=1}^{N} Q_{ik} \tag{3.43b}$$

For each connected branch from bus group J, the line flow value can be evaluated, knowing the net injected power from the bus.

$\forall$ J, Compute P_{ij}^c and ,Q_{ij}^c from 3.44

$$P_{ij}^c = \frac{R_{ji}(P_{ji})^2 + R_{ki}(Q_{ji})^2}{(V_j)^2} - P_{ji} \tag{3.44a}$$

$$Q_{ij}^c = \frac{X_{ji}(P_{ji})^2 + X_{ji}(Q_{ji})^2}{(V_j)^2} - Q_{ji} \tag{3.44b}$$

Check for consistency with the measured values using conditions 3.19 for each P_{ij}^m and Q_{ij}^m . The premise here is that the PMU measurements are not compromised so they can be used to validate the SCADA measurements. Next, is to estimate the corresponding P_{ji}^c and Q_{ji}^c for each bus in J using equation 3.45 below

$$P_{ji}^c = \frac{R_{ij}(P_i - \sum_{j=1,j\neq j}^{N} P_{ij}^m - \sum_{k=1}^{N} P_{ik}^m)^2 + R_{ij}(Q_i - \sum_{j=1,j\neq j}^{N} Q_{ij}^m - \sum_{k=1}^{N} Q_{ik}^m)^2}{(V_i)^2} - P_i$$
$$+ \sum_{j=1,j\neq j}^{N} P_{ij}^m + \sum_{k=1}^{N} P_{ik}^m$$

$$Q_{ji}^c = \frac{X_{ij}(P_i - \sum_{j=1,j\neq j}^{N} P_{ij}^m - \sum_{k=1}^{N} P_{ik}^m)^2 + X_{ij}(Q_i - \sum_{j=1,j\neq j}^{N} Q_{ij}^m - \sum_{k=1}^{N} Q_{ik}^m)^2}{(V_i)^2} - Q_i$$
$$+ \sum_{j=1,j\neq j}^{N} Q_{ij}^m + \sum_{k=1}^{N} Q_{ik}^m$$

For each bus in group J, check for condition 3.40. If any of the measurements violates the set threshold, an alarm is raised for falsified measurement. A falsified measurement will be discarded and the estimated measurement value retained for subsequent analysis where necessary.

Generally,for scenario 2C, if J=0, where there are no buses under J, but K has buses in that category, then the algorithm will use scenario 1A to detect specific falsified measurements. On the other hand, if K=0, and J has a set of buses under it, then the approach will be different. This will mean that all connected buses are compromised.

The first task is to find the net injected power from all buses, thus I and all in J. This will be done by evaluating equation 3.24 for all the Buses in J and I. Check for condition 3.27 to ascertain the correct values that will be used to compute the net injected bus power P_i,Q_i and P_j,Q_j ($\forall$ J) using equation 3.24. Evaluate equation 3.44 for each Bus and compare with conditions 3.19 for the power flow measurements at Bus I.

Compute $P^c_{ji}$and Q^c_{ji} for each bus in J from equation 3.46

$$P^c_{ji} = \frac{R_{ij}(P_i - \sum_{j=1,j\neq j}^{N} P^m_{ij})^2 + R_{ij}(Q_i - \sum_{j=1,j\neq j}^{N} Q^m_{ij})^2}{(V_i)^2} - P_i + \sum_{j=1,j\neq j}^{N} P^m_{ij} \tag{3.46a}$$

$$Q^c_{ji} = \frac{X_{ij}(P_i - \sum_{j=1,j\neq j}^{N} P^m_{ij})^2 + X_{ij}(Q_i - \sum_{j=1,j\neq j}^{N} Q^m_{ij})^2}{(V_i)^2} - Q_i + \sum_{j=1,j\neq j}^{N} Q^m_{ij} \tag{3.46b}$$

For each Bus in group J, condition 3.40 is checked. Any measurement that violates this condition is flagged and an alarm raised for falsified measurement.Falsified SCADA measurements are discarded, and the estimated measurement values kept for subsequent analysis.

The scenarios and equations outlined in this section will form the algorithm being used for the anomaly detection for control centers (ADCC).

Chapter 4

Simulations and Results

The algorithm is simulated and tested in this chapter and the results will be discussed. Before that, this study will discuss the attack model being used.

4.1 Formulation of attack model

Stealthy measurement attacks are carefully crafted to evade bad data detection at the control center. In state estimation, the norm of measurement residuals is supposed to be less than the threshold in the Ch-squares table. References [28],[29],[30],[31] formulate and use the following attack model to test stealthy load redistribution attacks on the power grid. Since generation is deemed to be highly connected to the control center, the load measurements provide an alternate means of altering power flow on the grid [31]. The following equations are employed in the attack model.

$$1^{\intercal}\Delta P_l = 0 \tag{4.1a}$$

$$-\tau\Delta P_l \leq \Delta P_l \leq \tau\Delta P_l \tag{4.1b}$$

The first constraint in equation (4.1a) sets a load change constraint that ensures power balance in the entire network. An attack magnitude is used to set the set second constraint, in equation (4.1b) that determines the threshold for the load changes. This limits the attack

magnitude for power injection at each load bus. By industry practice, real time and short-term historical data are used as inputs for Security Constrained Economic Dispatch (SCED). The model further analyses the effect on SCED if the attacker successfully modifies load measurements with these defined changes. From the DC power flow model,the new power flow f^{new} will be expressed as

$$f^{new} = S \cdot (P_g - (P_l + \Delta P_l)) \tag{4.2}$$

If r is the line flow limit, the new constraints for line flow can now be expressed as:

$$-r \leq f^{new} \leq r \tag{4.3}$$

The line flow limits are seen to be affected by the newly enforced constraints. If f is the original or true line flow, it is evident that after enforcing these constraints $|f| \geq r$. Hence the true line flows will exceed its rated limits.

NERC Standard PRC-023-1 requires that the ratio of absolute value of MW line flow before line trip to the nominal line facility rating capacity to be set at least 1.5 pu [32]. If the generation dispatch is followed unknowingly, this attack will lead to multiple overloaded transmission lines, resulting in cascading line trips and load shedding [31].

In this study, a multiplication factor of 1.4 is used for the analysis (a factor below the recommendation of NERC) to determine the behavior of the ADCC.

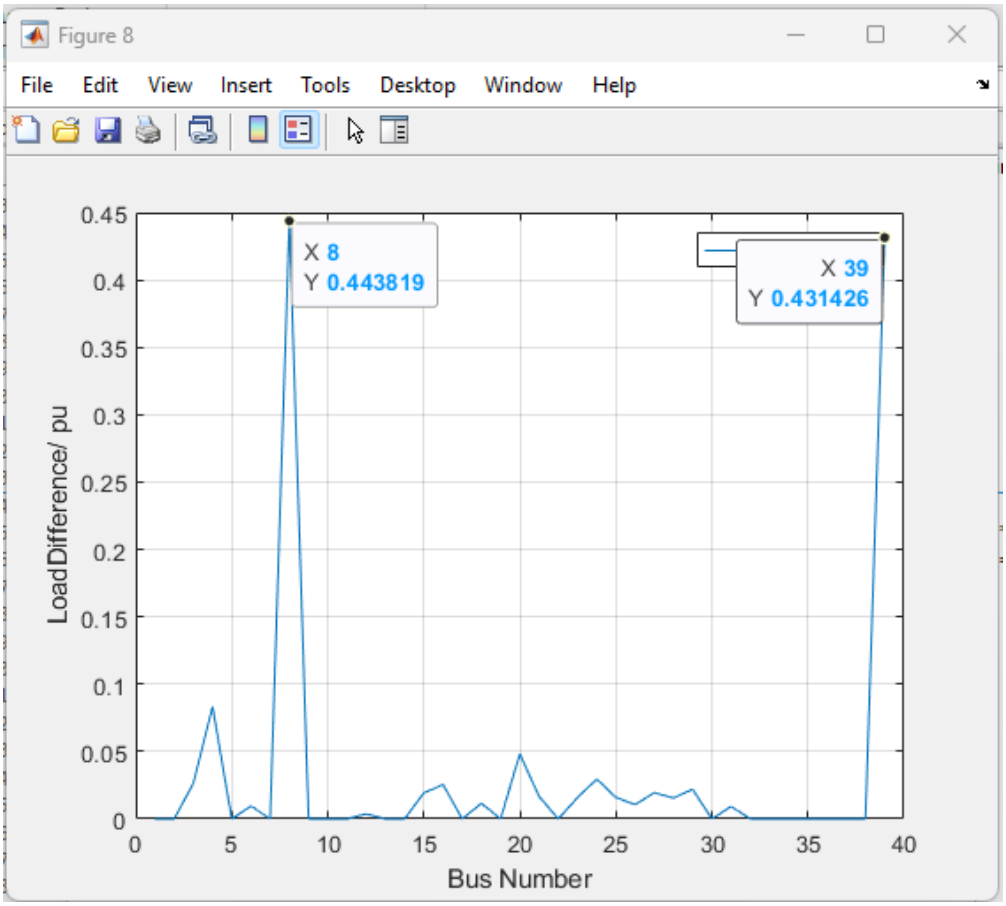

Figure 4.1: Difference in measurement after stealthy attack

4.2 ADCC Results

Measurement attacks targeting single and multiple buses on the IEEE 39 bus system are simulated. A stealthy false data injection attack using the attck model discussed in [28]-[31] is deployed and the results compared with BDD in state estimation. In this attack scenario, the load measurements are altered so that 4.1 is satisfied. In state estimation bad data detection, the limit set for the change in measurement is such that $\|P_l^{bad} - P_l^{est}\| < \tau$. Active Power load measurement for Buses 8 and 39 are falsified with a chosen attack vector that evades bad data detection in state estimation. Figure 4.1 provides the difference between the falsified SCADA measurements received and the true measurements. It is clear that this

Stealthy Attack	Attack Targets	ADCC Detection Alerts	ADCC Identification Alerts	BDD Results
$P_l^{bad} = P_l^{true} + \Delta P_l$ $1^\intercal \Delta P_l = 0$	Buses 8,39	CoCP and Ohm's Law Detect Falsified measurement at Buses 8,39	Active Load Power falsified at Buses 8,39	$\|P_l^{bad} - P_l^{est}\| < \tau$

Table 4.1: ADCC results

would have evaded BDD at the control center but the ADCC is able to detect and flag the falsified buses and compromised data. The difference is quite significant. Table 4.1 provides the results for the simulation with the ADCC algorithm. It is assumed that the attacker has partial or full knowledge of the of the system and is able to access the short-term load forecast. He can then successfully craft this attack. The ADCC is able to detect this attack. Even though the attacker is able to maintain power balance for the entire system, the CoCP detection scheme for the bus and Ohm's Law detection scheme for the branch identified the specific anomalous injected packet for elimination. The ADCC estimated values for P_{L8} and P_{L39} are 1.1912p.u and 4.0005p.u respectively compared to the true values of P_{L8} and P_{L39} which are 1.1679p.u. and 3.9221p.u respectively. Though there is minimal deviation the estimated values provide a better estimate of the true values than the falsified measurement.

Table 4.2 provides results for other multiple tests and the simulated results.

In scenario 1, the power flow measurement between Buses 39 and 1 is increased to test the performance of the ADCC. Ohm's Law check for both buses identify the falsified measurement. At Bus 39, the CoCP detection scheme is violated so another alert is raised.

In scenario 2, the attack seeks to create power balance at Bus 1. Even though the attack evades the CoCP check at Bus 1, Ohm's Law check from the connected buses, successfully detects the falsified measurement. The identification module is also able to detect the specific

Attack scenario	Attack Target(s)	ADCC Detection Alerts	ADCC Identification Alerts
1. Increase Active power flow from Bus 39 to 1 by 1.4 times	Buses 1,39	Ohm's Law Detect at Buses 1,39 CoCP Detect at Bus 39	Falsified active power flow measurement from Bus 39 to 1 Falsified active power flow measurement from Bus 39 to 1
2. Increase all Active Power Flow at Bus 1 by 3 times.	Bus 1,	Ohm's Law Detect - Falsified measurement at Bus 1,2, and 39	Falsified Active power flow measurement from Bus 1 to 2 Falsified Active Power flow measurement from Bus 1 to 39
3. Increase voltage magnitude at Bus 39 by 1.4 times.	Bus 39	Ohm's Law Detect - Falsified measurement at Bus 39	Falsified voltage measurement at Bus 39

Table 4.2: Other ADCC test scenarios

line flow measurements that are falsified.

The third scenario, tested voltage measurement violation at bus 39. This was also detected at Bus 39 by the Ohm's law check. ADCC was also able to narrow down the specific falsified measurement.

These test scenarios prove the successful implementation of the algorithm on the IEEE 39 bus system.

Chapter 5

Conclusions

The research proposes an anomaly detection system that uses the physical laws to detect falsified measurements at the control center. The proposed approach is not detached from the physical system but uses the properties of the power system to detect measurement-based attacks.To minimise the amount of computations, the study formulates an algorithm that runs bus and branch measurements on two (2) equations each. The study also introduces the "zero-loop sum identity". This property states that for any loop in a power system network, if all measurements are available and Ohm's law is satisfied, Kirchoff's Voltage Law (KVL) will automatically be satisfied. This is an important finding.

This study also determined a realistic threshold that validates bus and branch measurements in the power system. Falsified measurements that violate these thresholds are successfully flagged. The ADCC goes further to determine the specific falsified measurement(s). The algorithm also provides an estimated value of the falsified measurement.Dropped falsified packets are replaced with an estimated value that has been shown to have negligible deviation from the true values. This provides a better estimate of the identified falsified measurement. The problem of power system unobservability when falsified critical measurements are dropped, is therefore curtailed with the implementation of this algorithm.

In conclusion, the primary goal of this study has been realised since the ADCC is able to detect anomalous measurements and provide an estimated value of the specific falsified measurement.

Chapter 6

Future Work

As part of future work, this algorithm could be tested on networks with optimally placed PMUs. This can cater for scenarios where substations do not have PMUs. Again, further studies into ensuring the security of PMU measurements while incorporating the formulated algorithm could be explored. To avoid delays in DNP3 packet polling, further studies into reducing computational time of the algorithm could also be explored. Machine learning models can be explored to learn the scenarios discussed. This can aid prompt operation of the identification module,further minimizing delays. Using Graphic Processing Units (GPUs) can also help run parallel computations on the algorithm to reduce the computational times. The study also made an assumption that initial measurements received from the packet filtering module should make the power system observable. Further studies into dropped packets and loss of critical measurements can also be explored. Differentiating bad data possibly caused by instrument malfunctioning from actual measurement-based cyber attacks can also be explored in future works.

Bibliography

[1] C.-C. Liu, J. C. Bedoya, N. Sahani, A. Stefanov, J. Appiah-Kubi, C.-C. Sun, J. Y. Lee, and R. Zhu, "Cyber–physical system security of distribution systems," *Foundations and Trends in Electric Energy Systems*, vol. 4, no. 4, pp. 346–410, 2021.

[2] J. Meserve, "*Staged cyber attack reveals vulnerability in power grid* [Online]." Available: http://www.cnn.com/2007/US/09/26/power.at.risklindex.html, 2007. [Accessed: March 05,2024].

[3] A. Bindra, "Securing the power grid: Protecting smart grids and connected power systems from cyberattacks," *IEEE Power Electronics Magazine*, vol. 4, no. 3, pp. 20–27, 2017.

[4] Foxnews, "*Massive hack attack targets Israel electrical grid* [Online]." Available: www.foxnews.com/world/2016/01/27/massive-hack-attack-targets-israel-electrical-grid.html, 2016. [Accessed: March 06,2024].

[5] L. Kearney, "*US electric grid growing more vulnerable to cyberattacks* [Online]." Available: https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/, 2024. [Accessed: April 05,2024].

[6] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—attacks, impacts, and defense: A survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411–423, 2017.

[7] Y. Liu, N. Peng, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactiions*, vol. 14, no. 13, pp. 1–33, 2011.

[8] R. Zhu, C.-C. Liu, J. Hong, and J. Wang, "Intrusion detection against mms-based measurement attacks at digital substations," *IEEE Access*, vol. 9, pp. 1240–1249, 2021.

[9] G. Koutsandria, V. Muthukumar, M. Parvania, S. Peisert, C. McParland, and A. Scaglione, "A hybrid network ids for protective digital relays in the power transmission grid," in *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 908–913, 2014.

[10] C. Zhou, S. Huang, N. Xiong, S.-H. Yang, H. Li, Y. Qin, and X. Li, "Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 10, pp. 1345–1360, 2015.

[11] M. Brand, S. Ansari, F. Castro, R. Chakra, B. H. Hassan, C. Krüger, D. Babazadeh, and S. Lehnhof, "A framework for the integration of ict-relevant data in power system applications," in *2019 IEEE Milan PowerTech*, pp. 1–6, 2019.

[12] V. Menzel, N. B. Arias, J. L. Hurink, and A. Remke, "Securing smart grids locally using a power flow-based intrusion detection system," in *2023 IEEE Belgrade PowerTech*, pp. 1–9, 2023.

[13] L. Che, X. Liu, and Z. Li, "Fast screening of high-risk lines under false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4003–4014, 2019.

[14] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[15] X. Liu and Z. Li, "False data attacks against ac state estimation with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2239–2248, 2017.

[16] J. Zhao, G. Zhang, Z. Y. Dong, and K. P. Wong, "Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 6–8, 2016.

[17] C. Pei, Y. Xiao, W. Liang, and X. Han, "A deviation-based detection method against false data injection attacks in smart grid," *IEEE Access*, vol. 9, pp. 15499–15509, 2021.

[18] C. Pei, Y. Xiao, W. Liang, and X. Han, "Detecting false data injection attacks using canonical variate analysis in power grid," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 971–983, 2021.

[19] P. Hu, W. Gao, Y. Li, X. Guo, F. Hua, and L. Qiao, "Anomaly detection and state correction in smart grid using ekf and data compensation techniques," *IEEE Sensors Journal*, vol. 24, no. 8, pp. 12995–13009, 2024.

[20] J. Lei, S. Gao, J. Shi, X. Wei, M. Dong, W. Wang, and Z. Han, "A reinforcement learning approach for defending against multiscenario load redistribution attacks," *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 3711–3722, 2022.

[21] J. Zhao, G. Zhang, and R. A. Jabr, "Robust detection of cyber attacks on state estimators using phasor measurements," *IEEE Transactions on Power Systems*, vol. 32, no. 3, pp. 2468–2470, 2017.

[22] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[23] "Ieee standard for exchanging information between networks implementing iec 61850

and ieee std 1815(tm) [distributed network protocol (dnp3)]," *IEEE Std 1815.1-2015 (Incorporates IEEE Std 1815.1-2015/Cor 1-2016)*, pp. 1–358, 2016.

[24] E. P. Focus, "*DNP3 Protocol: Architecture, working, Function codes, Data format and its applications* [Online]." Available: https://www.elprocus.com/dnp3-protocol/, 2019. [Accessed: April 16,2024].

[25] S. Electric, "*Define Data polling intervals* [Online]." Available: https://tprojects.schneiderelectric.com/GeoSCADAHelp/Geo%20SCADA%202020/Default.htm#AdvancedTrioDiagnosticsDriverGuide/DefinetheDataPollingIntervals.htm, 2018. [Accessed: April 14,2024].

[26] R. Minker and E. O. Schweitzer, "Lower power voltage and current transducers for protecting and measuring medium and high voltage systems," *Western Protective Relay Conference, Spokane, WA, USA*, 1999.

[27] M. Farivar and S. H. Low, "Branch flow model: Relaxations and convexification—part i," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2554–2564, 2013.

[28] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.

[29] X. Liu, Z. Li, Z. Shuai, and Y. Wen, "Cyber attacks against the economic operation of power systems: A fast solution," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 1023–1025, 2017.

[30] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power system reliability evaluation considering load redistribution attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 889–901, 2017.

[31] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Transactions on Power Systems*, vol. 34, no. 2, pp. 1513–1523, 2019.

[32] NERC, "*NERC Standards* [Online]." Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/PRC-023-1.pdf#search=prc%2D023%2D1, 2008. [Accessed: April 18,2024].