Securing Remedial Action Schemes Under Data Measurement Cyber Threats

A Thesis

Presented in Partial Fulfillment of the Requirements for the

Degree of Master of Science

with a

Major in Electrical Engineering

in the

College of Graduate Studies

University of Idaho

by

Parviz Khaledian

Major Professors: Brian K. Johnson, Ph.D. and Saied Hemati, PhD.

Committee Members: Herbert L. Hess, Ph.D.; Yacine Chakhchoukh, Ph.D.

Department Administrator: Joseph D. Law, Ph.D.

August 2018

Authorization to Submit Thesis

This thesis of Parviz Khaledian, submitted for the degree of Master of Science with a major in Electrical Engineering and titled "Securing Remedial Action Schemes Under Data Measurement Cyber Threats," has been reviewed in final form. Permission, as indicated by the signatures and dates given below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professors: _____Date_____
Brian K. Johnson, Ph.D.

_____Date_____
Saied Hemati, Ph.D.

Committee Members: _____Date_____
Herbert L. Hess, Ph.D.

_____Date_____
Yacine Chakhchoukh, Ph.D.

Department Administrator: _____Date_____
Joseph D. Law, Ph.D.

Abstract

In this thesis, different methods for power grid vulnerability assessment under cyber threats are developed and utilized. A new combined method is developed for better susceptibility analysis. Critical lines are identified using several different methods and remedial action schemes are examined on these critical lines to observe the reliability and resiliency improvement of the system. Furthermore, a new method to detect and fix false measurements on inputs to remedial action schemes is presented. With this false measurement detection method, this type of attack is more difficult as the malicious party needs to compromise a large number of meters in order to inject a manipulated measurement. As a result, actions by remedial action schemes are taken based on more reliable data and at the same time the true state of the local system is estimated. The required logic to correctly detect and fix the measurements are tested using the 118 bus IEEE test system.

The thesis concludes by presenting a novel approach to detect and fix false measurements developed in this project to ensure proper automatic action by remedial action schemes. It can be further developed and extended to provide an alternative way to improve system resiliency.

Acknowledgements

I would like to thank Professor Brian Johnson who supported me the since Aug 2017 through NSF funded project (Grant No. 1600058). His advice, guidance, and financial support helped me to be determined to accomplish good results and to focus on the project.

In addition, I would like to again thank Dr. Brian Johnson, Dr. Saied Hemati and Dr. Herbert Hess for their exceptional instruction and guidance in and out of the classroom. All three reflect the commitment and integrity that I hope to emulate in all endeavors that I pursue in the future.

Finally, I would like to thank my sisters, Sana and Adibeh, who have always been my supporter and encouragement.

Dedication

To my Parents, Fata gyan and Hama gyan
who stay as symbols of humanity to me and who spent their life to train their children and support their education in order to help in making the world a better place.
To accomplish their mission and make up their efforts, I will forever try to improve and make positive impacts.

Table of Contents

List of Tables

List of Figures

List of Equations

Glossary

$G = (V, E)$	...	Power network with V nodes and E edges
$C_{(i,j)}$	...	Power capacity of the network in G = (V, E), for each edge (i, j)
$f_{(i,j)}$	...	Power flow on the edge (i, j)
$G_f(V, E_f)$	...	Residual power of the system
G_f	...	The system power capacity
$V_{i,j}$	...	Vulnerability index of edge (i, j)
f_{Max}^{uv}	...	Maximum flow from the source u to the sink v
f_{ij}^{uv}	...	Portion of the flow transferring through edge E_{ij}
m_i	...	Number of segments of the i^{th} fault chain
T_{ij}	...	j^{th} segment of the i^{th} fault chain
v_{ij}	...	j^{th} influencing factor
$\omega_{H_{ij}}$	...	Sensitivity coefficient of the j^{th} factor for i^{th} fault chain
k_x	...	Specific number of influencing factors
k_i	...	Number of all influencing factors
$q_{\overrightarrow{Li}}$	...	Probability of the i^{th} fault chain occurring
$T_{(i(j-p))}$	...	Fault segment on line k-p
$S_{max}^{(k+1)}$	...	Maximum power capacity of line k+1
$\omega_k^{(k+1)}$	...	Weight normalizers
$F_{(i(j+1))}^{(k+1)}$	...	Next segment to fault on the i^{th} fault chain
$\phi(Mi)$	...	Vulnerability index of an event
s_j	...	Number of the fault chains including the j^{th} transmission section

$I_{r1}^{'}$	...	Fundamental frequency current
ψ_{m1}	...	Fundamental frequency flux
$\psi_{m(pk+1)}$	...	the $(pk+1)^{th}$ airgap flux harmonic
$I_{r(pk+1)}^{'}$	...	$(pk+1)^{th}$ current harmonic of the rotor
ω_s	...	Applied frequency to the stator
T_{pk+1}	...	Torque harmonic generated from the $(pk+1)^{th}$ voltage harmonic
θ_{pk+1}	...	Angle of the torque harmonics
A_{pk+1}	...	Amplitude of the torque harmonics
RAS	...	Remedial Action Scheme
PMU	...	Phasor Measurement Unit
$FACTS$	...	Flexible Alternating Current Transmission System
$SCADA$	...	Supervisory Control And Data Acquisition
SE	...	State Estimation
AC	...	Alternating Current
DC	...	Direct Current
PDC	...	Phasor Data Concentrator
DSA	...	Dynamic Security Assessment
$PSAT$	...	Powerflow and Short circuit Assessment Tool
$VSAT$	...	Voltage Security Assessment Tool
$PMCU$	...	Phasor Measurement Control Unit

Chapter 1: Introduction

A reliable power supply is one of the important requirements of our society. Disruptions to electrical power grids paralyze the daily life in modern societies causing huge economic and social costs for these societies. It is very difficult or even unfeasible to guarantee a 100% secure and reliable system, however, it is important to design a resilient system that continues to operate with outages. Challenges to the power system include, but are not limited to, increasing connection of renewable sources to the power grid, operating sensitive loads on the system, continuous changes in online operations, relying more on vulnerable communication components, and more possibility of intentional attacks. These challenges lead to vulnerability and in some scenarios even instability in the system and eventually may lead to a cascading outage and system failure. Therefore, power system vulnerability assessment is crucial.

Therefore, as a primary task, identifying the vulnerable components in a power grid is vital to the design and operation of a secure and stable system. One aspect of vulnerability analysis is to identify transmission lines where the loss of that line or transformer leads to major disruptions to the grid. Part of our work is to determine these crucial components of the system.

Next step is to determine the fault chains and calculating vulnerability indices based on fault chain theory. Cascading failures are the typical reasons for blackouts in power grids [1]. The grid topology plays an important role in determining the dynamics of cascading failures in power grids. Measures for vulnerability analysis are crucial to assure a higher level of robustness of power grids. We use three different method to perform this analysis and determine crucial lines. Hence, another task is to prioritize these critical lines in monitoring, controlling, and implementing special protection schemes such as Remedial Action Schemes (RAS).

RAS have been increasingly used by utilities to mitigate instability problems following the loss of one or more transmission lines on a transmission corridor to prevent out-of-step

conditions that may result in cascading system-wide outages. Application of RAS mitigates the system problems and as a result reduces the system vulnerability and decreases the possibility of cascading failures.

These remediation techniques are based on the real-time measurements from Phasor Measurement Units (PMUs) along with Supervisory Control And Data Acquisition (SCADA) system. Because these systems rely on data communication that is vulnerable to cyber-attack, another important task is to ensure the reliability of a power system and its protection by detecting false measurements, identifying any related event, and try to fix the data.

In this thesis, each chapter discusses results and outcomes for each task as presented in a paper.

Chapter 2 is a paper that was submitted to the ?Industrial Electronics Society Conference (IECON). In the paper, we use a power flow-based method to assess the vulnerability of the system before and after applying remedial action schemes. To demonstrate the system resiliency improvement, we model and simulate a modified version of the IEEE 9 bus system in the Powerworld simulator to examine our method and verify the assessments' results.

Chapter 3 discusses assessing the vulnerability of a system using both fault chain theory and a power flow-based method and calculate the probability of cascading outages. Further, we consider a Remedial Action Scheme (RAS) to reduce the vulnerability of the system and to harden the critical components against intentional attacks. To identify the most critical lines more efficiently, a new vulnerability index is presented. The effectiveness of the new index and the impact of the applied RAS is illustrated on the IEEE 14-bus test system. This chapter was presented at the 2018 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS).

In Chapter 4, the placement of PMUs using a method from the literature is discussed. There are several methods to identify the false measurements, but each of them has its own obstacles and disadvantages. In this chapter, we present a new method to detect the false measurement with more immunity against attacks and measurement error and then we

propose a method to fix the false measurement and provide valid data to the remedial action scheme.

The objectives in this thesis can be summarized as followings:

- Recognize critical components and quantify vulnerability
- Apply remedial action schemes
- Detect and fix false measurements
- Reduce vulnerability
- Maintain or improve system reliability
- Improve system resiliency

In each chapter, the results of our work demonstrate the level of achievement on these goals. Furthermore, in the conclusions chapter, Section 5.2 is allocated to review the accomplishments on our objectives, followed by suggestions for future work.

Chapter 2: Power Grid Resiliency Improvement Through Remedial Action Schemes

The results of this work have been submitted to the 44th annual IEEE Industrial Electronics Conference (IECON 2018) [2]. Here, the numbers for citations, equations, tables, and sections have been updated for inclusion in this thesis and therefore differ from the publications originally accepted form. The original paper is available upon request.

2.1 Introduction

Power grid resiliency is an important requirement for our community. The complexity of the power system structure is constantly increasing as the power supply demand patterns change every year and more renewable energy sources are connected to the network. While they have many benefits, these intermittent renewable sources have potential to negatively impact system resiliency and can cause instability in the system [3], which could result in system problems. Thus, it is important to identify the critical lines in order to help prevent cascading outages by applying corrective actions and protections such as remedial action scheme (RAS). The analysis of critical parts of the system helps to explore the nature of complex power grid. Therefore, power system vulnerability assessment is necessary to determine the most critical lines and provide proper RAS in these vulnerable areas. Furthermore, vulnerability assessment of transmission lines is an important measure of the systems' susceptibility [4].

The potential vulnerabilities in a power grid can be analyzed by identifying those areas where a failure or an attack causes maximum disruption to the grid. We can quantify disruptions in several different ways, including (a) sudden deviation of the voltage magnitudes or phase angles at the buses from operating values, and (b) determining the minimal amount of generation or load that must be shed in order to restore the grid to stable operation.

The rest of the chapter is organized as follows. First, in Section 2.2 fundamentals of RAS are presented. Next, vulnerability assessment of the power grid is discussed in Section 2.3.

In Section 2.4, our approach for assessing system vulnerabilities using a power flow-based method is presented. Section 2.5 includes results from simulations using the IEEE 9-bus test system to examine the power flow-based analysis, the proposed vulnerability index calculation, and the effectiveness of the RAS. The positive impacts of the RAS on improving system resiliency and mitigating system vulnerabilities are demonstrated. The chapter is concluded in Section 2.6.

2.2 Remedial Action Schemes

An effective resilient system can adapt to, presume, and quickly recover from a disturbing event [5]. A RAS is one way to achieve these goals for a power transmission system. These schemes have been increasingly used by utilities to mitigate instability problems following the loss of one or more transmission lines or generators under certain loading conditions. By applying predetermined corrective plans, a RAS prevents the power system from reaching out of step conditions that may result in cascading system-wide outages [6]. Remedial action schemes, also known as special protection systems (SPS) or system integrity protection systems (SIPS) are automatic protection systems designed to detect abnormal or predetermined system conditions and then take corrective actions other than and/or in addition to the isolation of faulted components to maintain system security. Such actions may include creating sudden changes in demand, generation, or system configuration to maintain system stability, acceptable voltage, or power flows [7]. Some advantages of RAS are listed below [8]:

- Avoiding widespread outages after a severe contingency or sequence of events in the power system.
- Increasing operational transfer capability within the restrictions on the transmission system allows increased path capacity without building more power lines.
- Quickly detecting abnormal predetermined system conditions and takes a predefined

action to prevent a system problem.

- Helping balance load and generation after a loss of a generator, major lines or major loads.
- Increasing overall system reliability.
- Increasing power system resilience.

RAS do not include the following items [9]:

- Underfrequency or undervoltage load shedding.
- Protection for fault conditions that can be covered with standard relaying schemes.
- Out of Step Relaying that is not an integral part of a RAS.
- Sub-Synchronous Resonance (SSR) protection schemes.
- Auto-reclosing schemes.

A. *Common RAS Classification*

Depending on the method of detection, existing RAS can be classified as event-based or response-based [10]. Event-based RAS are designed to operate on the recognition of a combination of events (such as loss of several ties). Response-based RAS are based on real-time measurement and initiate control actions when the responses hit the trigger level. Event-based RAS can be fast. Therefore, there is no need to wait for the response development. On the other hand, response-based RAS have mainly been applied for slower phenomena and can operate for unknown events and varying operating scenarios. The next generation of corrective controls requires fast detection of system instability based on both events and responses from wide area monitoring. This has become possible with the deployment of real time phasor measurement units (PMUs), as well as with modern communication systems. In addition, PMUs may allow disturbances to be detected more quickly, requiring less severe action. However, utilization of PMUs in RAS also opens new avenues for vulnerabilities for RAS operation and to system stability. A cyberattack at the measurements used in the RAS could lead to incorrect action, either in failing to act when it should, or acting when it should not.

B. *Typical RAS Features*

Critical details of the RAS design and operating characteristics must be determined through appropriate studies. The results can be used to do the following [11]:

- Identify the problem to mitigate: The issue that needs to be reduced or eliminated.
- Arming criteria: Determining critical system conditions for which a RAS should be activated to take action when required.
- Initiating conditions: Determining critical contingencies to initiate action once the scheme is armed. Parameter-based RAS detect changes in critical system conditions rather than directly detecting specific conditions.
- Actions to take: The minimum remedial action required for each contingency (when armed) and the maximum acceptable remedial action for each contingency (when pertinent).
- Time requirements or allowable time: The maximum time allowable for the remedial action to be accomplished.

It is important to identify the critical system conditions where the RAS should be armed. These conditions are often identified by one or more of the followings [12]:

- Generation patterns
- Transmission line loadings
- Load patterns
- Reactive power reserves
- System response as determined from the data provided by wide area measurement systems (WAMS), or
- Other unsustainable conditions identified by studies of system characteristics

For example, during lightly loaded system conditions, a transmission line outage may not cause any reliability criteria violations, but during heavier loading, the same outage may result in generator instability or overloads on remaining facilities. Automatic single-phase or

three-phase reclosing following temporary faults during stressed operating conditions may avoid the need to take remedial action. Appropriate RAS action may still be required if reclosing is unsuccessful. The RAS is designed to mitigate specific critical contingencies that initiate the actual system problems. There may be several critical single contingency outages for which remedial action is needed. There may also be credible double or other multiple contingencies for which remedial action is needed. Each critical contingency may require a separate arming level and different remedial actions.

C. *Actions in RAS*

Various possible remedial actions are usually available to improve system performance. These may include but are not limited to [11]:

- Islanding or other line tripping
- Generator shedding
- Load shedding (direct, underfrequency, undervoltage)
- Braking resistors
- Static VAr or other Flexible Alternating Current Transmission System (FACTS) control units
- Shunt capacitor/Reactor/Resistor insertion
- DC line runback or oscillation damping
- Series capacitor bypass

The minimum remedial action required is determined through studies that define the boundary between acceptable and unacceptable system performance and resilience. Remedial actions beyond this minimum level often can result in further system performance improvements. At some higher action level, system performance standards may again be violated if system response approaches another part of the boundary of the region of stability (e.g. high voltage due to extra load shedding). However, some extra remedial action (safety margin) should be applied to ensure that at least the minimum action will still occur even for a worst-case credible scheme failure. While actions above the necessary safety margin do

not create new violations, they may make the scheme more costly and complex, as well as result in a larger impact to customers (e.g. reduction of generating reserve, shed more load) [13]. The maximum time acceptable to act will change with the type of problem for which the RAS is a solution. Short-term angular and voltage stability problems typically require the fastest response, as fast as a few cycles but usually less than one second. Actions to mitigate steady-state stability and slow voltage collapse problems may allow several seconds. Thermal overload problems allow several tens of minutes before action is required. Most of the currently employed RAS are based on traditional, local measurements, but there has been a movement toward using phasor measurement control units (PMCUs) in recent years. The measurements from PMCU are easier to process and the local system state estimation is faster. On the other hand, phasor measurement control units are introducing some vulnerabilities to the system due to their communication schemes. In addition, there is an added cost to provide many lines with PMCUs, RAS, Phasor Data Concentrators (PDC), and communication systems (Figure 2.1) and structure them to meet NERC CIP requirements.

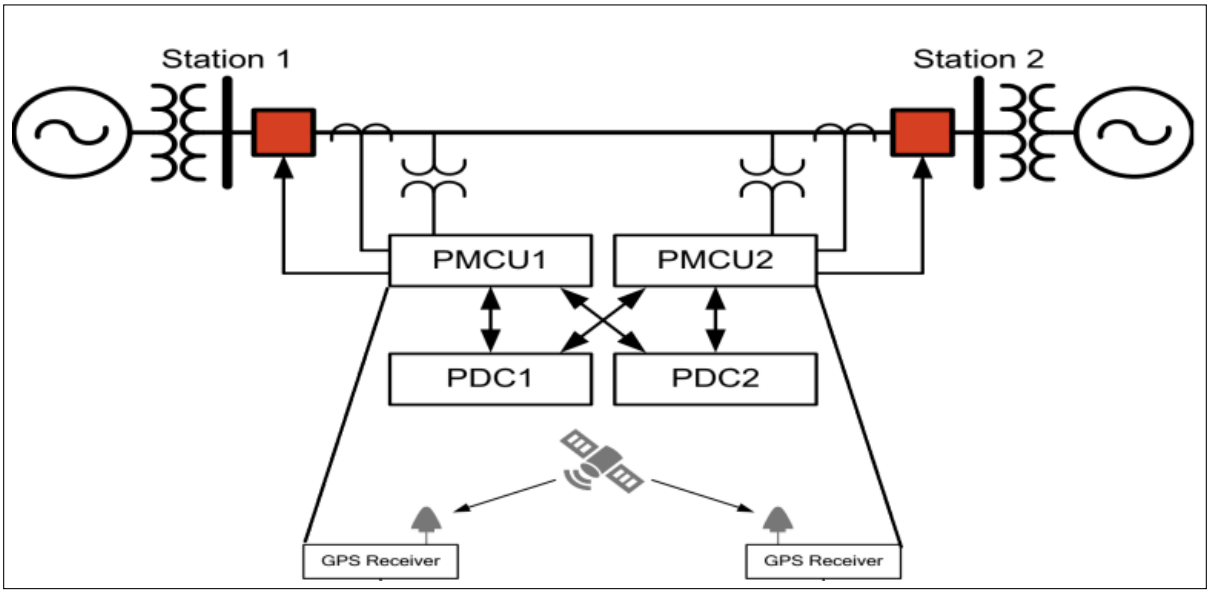

Figure 2.1: A sample of a transmission line with PMU and required components

Therefore, sensitivity analysis is performed to identify the most vulnerable locations in

the system and focus monitoring on those areas. The new susceptibilities that are introduced to the system by PMUs must be analyzed, which is out the scope of this project.

2.3 Identifying Vulnerabilities in Power System

Remedial action schemes rely on the real-time measured data from the power system. In cases where these schemes are armed by system operators, there is a need provide real-time visibility to system operators in a clear manner. Providing such information for all possible contingencies in real time is impossible and therefore, there is a need to reduce the number of monitored contingencies [14]. These contingencies are identified through system vulnerability analysis. The recent rapid rise in distributed generation and renewable energy generation introduces more stress to the whole power system, potentially exacerbating the system vulnerabilities, and increasing risk of cascading events [15]. Much work has been done to improve the system security and reliability. However, significant outages take place all over the world [16]. Therefore, it is very essential to further apply new tools and methods to prevent potential cascade blackouts. The power grid has developed to be one of the most complex human-made systems. As such, this highly clustered network in some research is presented as a small-world network [3]. Even in a large-scale network, a node can interact with others far across the system through a limited number of steps. Due to failures, the capacity of the transmitted power decreases greatly.

2.4 Power Flow Based Method

Although, remedial action schemes are generally applied to large power systems, here, we study the IEEE 9 bus system to demonstrate our analysis approach and demonstrate the improvement in system resiliency (Figure 2.2). This model is based on a directed graph and weighted by the power flow. Unlike an electrical efficiency model, the edge with a higher weight transfers more power in this method. In the power flow-based method, the capacity

of a line and the actual power transfer determine a lines vulnerability ranking. This method deals with the weighted network and directed power flow. The following assumptions are made [17]:

- Each bus is a node and each line us an edge. Nodes are reliable, and edges are in either working or fail states.
- Direction of the power flow in each transmission line is the direction of the related edge.
- The minimum degree of each node is 2, except for the source and sink nodes.

To evaluate the vulnerability of transmission lines and rank them, the vulnerability index (V.I.) is calculated using the following procedure [6], [18]:

- Build a connected network graph of the system.
- Estimate the steady-state power flow (Figure 2.2).
- Determine the weight and direction of the power flow on each edge of the network (Figure 2.2).

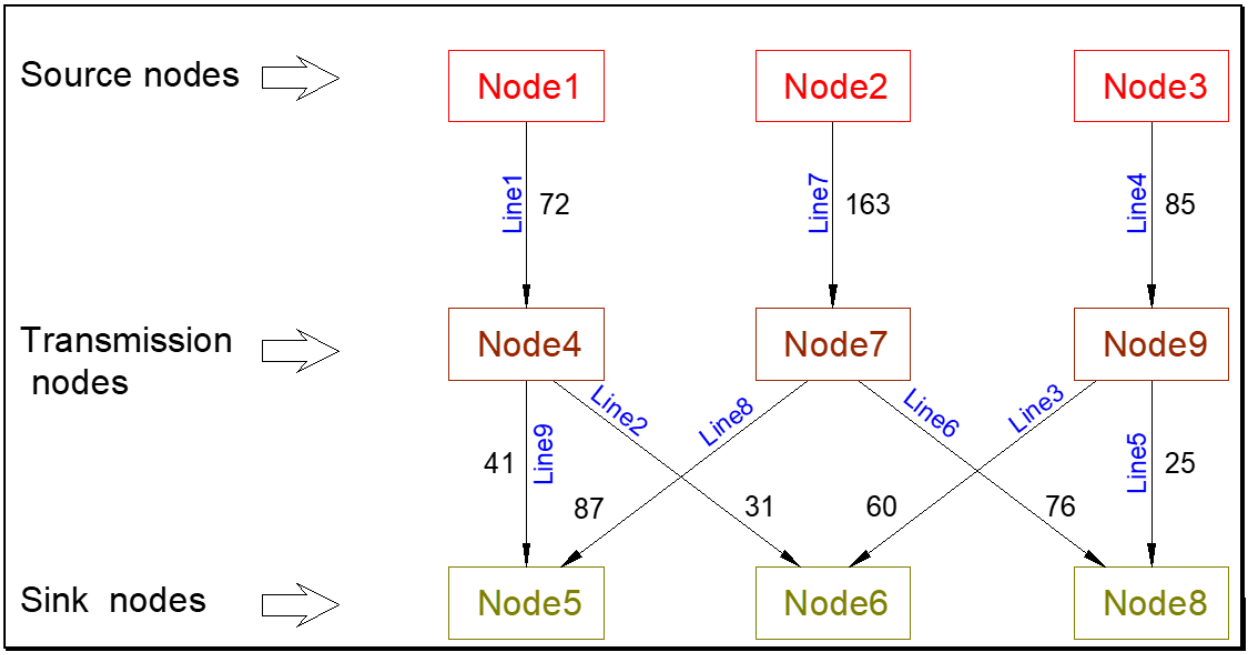

Figure 2.2: Steady-state power flow weights on the IEEE 14-bust test system.

- Evaluate the maximum flow for each source sink combination. Considering the network as G = (V, E), for each edge (i, j), the capacity is denoted as $C_{(i,j)}$, and flow on the edge is denoted as $f_{(i,j)}$. A source node is denoted as s, and a sink node by t. The residual network of the system is presented by $G_f(V, E_f)$. The system capacity G_f is defined by (2.1)

$$C_{f(i,j)} = C_{(i,j)} - f_{(i,j)} \tag{2.1}$$

To obtain the maximum source-sink flow:

Initially, for each edge (i, j), set the flow at $f_{(i,j)} = 0$. Given a path p from s to t in G_f , for all edges $(i, j) \in p$, find

$$C_{f(p)} = min\left\{C_{f(i,j)} | (i, j) \in p\right\} \tag{2.2}$$

For each edge $(i, j) \in p$, set

$$f_{(i,j)} = f_{(ij)} + c_{(f(p)} \tag{2.3}$$

$$f_{(j,i)} = f_{(j,i)} - c_{(f(p)} \tag{2.4}$$

- To compute the vulnerability index $V_{i,j}$, sum the flow values. and get the flow on each edge corresponding to the maximum flow in the network. Next, the vulnerability index of edge (i, j) is defined as the amount of flow carried by edge (i, j) relative to the maximum flow across the network between source and sink nodes.

$$V_{ij} = \frac{\sum_u^m \sum_v^n f_{ij}^{uv}}{\sum_u^m \sum_v^n f_{Max}^{uv}} \tag{2.5}$$

  where f_{Max}^{uv} is the maximum flow from the source u to the sink v, f_{ij}^{uv} is the portion of the flow transferring through edge E_{ij}.

- Label the lines based on the vulnerability index (Figure 2.3).

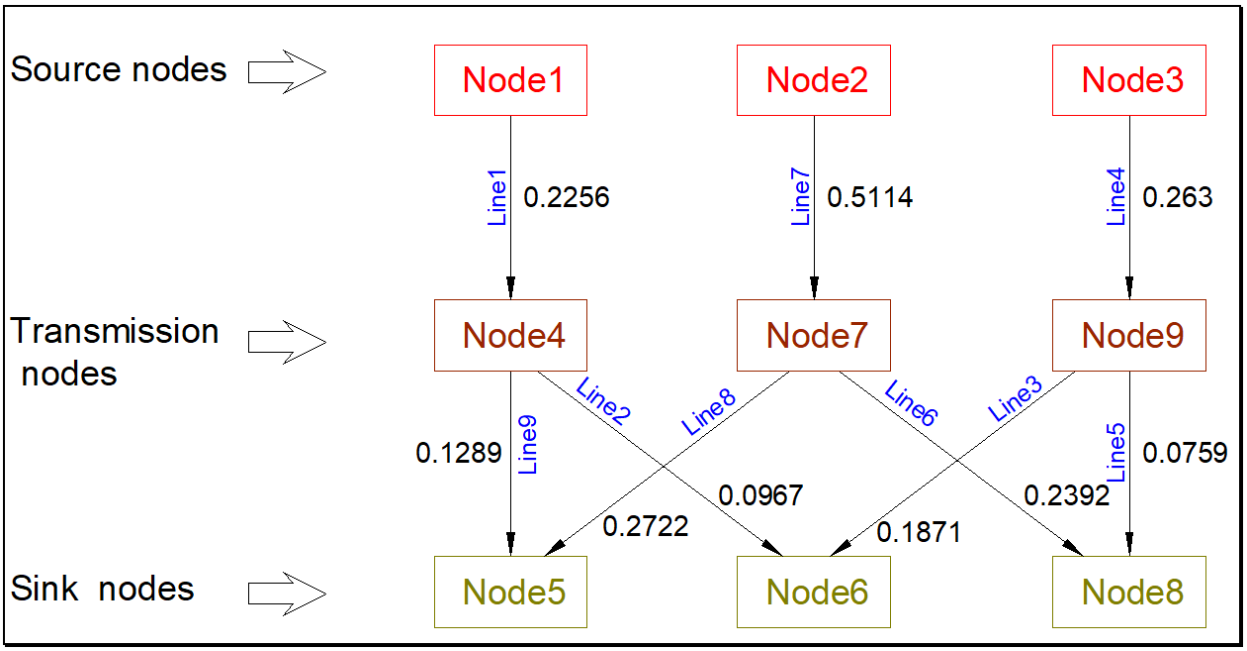

Figure 2.3: V.I. distribution for the lines in the IEEE 9 bus system.

- Rank the lines according to V.I. values. The line with a high value of index is considered as more critical in this analysis. Table 2.1 shows the vulnerable line ranking identified from the power flow model.

2.5 Simulation and Results

The power flow-based method was applied to the IEEE 9 bus system in the previous section. Here contingency analysis in applied followed by adding a RAS applied to the recognized vulnerable lines. To make this approach more understandable, the vulnerability index (V.I.) is calculated for line 4 (the line from node 3 to 9) as below:

- Step 1, 2, and 3 are done by Powerworld and the results are shown in Figure 2.2.
- Step 4: From the Powerworld flow information and branch information: $f_{(39_{Max})} = 86.41$, $f_{(27_{Max})} = 163.37$, $f_{(14_{Max})} = 76.87$
- Step 5:

$\sum_u^m \sum_v^n f_{Max}^{uv} = 86.41 + 163.37 + 76.87 = 326.65$

$V_{39} = 85.8/326.65$ so $V_{39} = 0.26288$

- Step 6: Distribute the V.I. values on the network model (Figure 2.3).
- Step 7: Rank the lines according to V.I. values (Table 2.1).

Table 2.1: Vulnerability Ranking Based on V.I.

	V-Rank	V-Index	Line	from BUS	to BUS
An example of V.I. threshold: 0.24	1	0.5114	7	2	7
	2	0.2722	8	5	7
	3	0.263	4	3	9
	4	0.2392	6	8	7
	5	0.2256	1	1	4
	6	0.1871	3	6	9
	7	0.1289	9	5	4
	8	0.0967	2	6	4
	9	0.0759	5	8	9

To provide more options for corrective actions, the IEEE 9 bus system was modified as shown in Figure 2.4. The generator at Bus 2 was divided into three units with the same total rating. Similarly, the loads at Buses 5 and 6 were divided into 2 loads with the ability to shed less critical loads first. Next, we perform contingency analysis on a case where one line (line 4) or one generator (bus 3) is lost (Figure 2.4). Power systems must be able to handle one contingency, and the effort is to make a system resilient in cases with multiple outages. Having this said, in this project we consider one major contingency since it is a small system. Because, a major contingency such as losing generator or transmission line can make the whole system unstable and cause a total blackout.

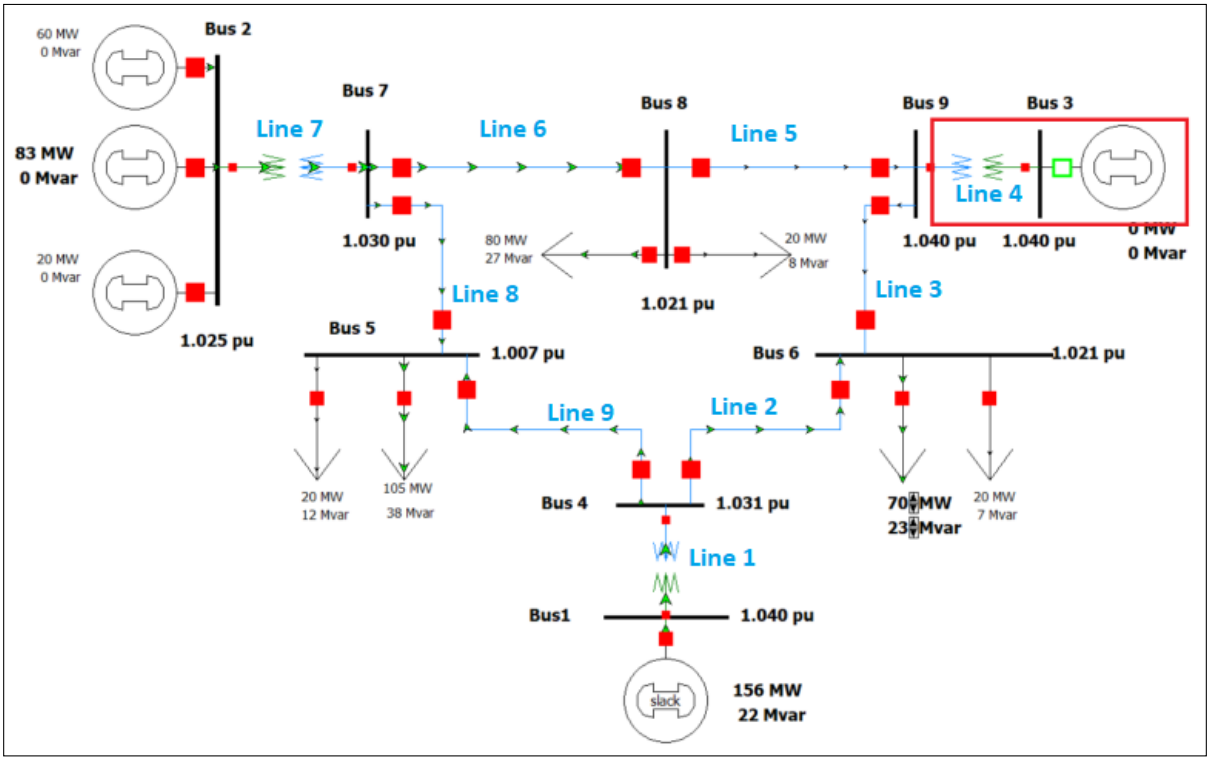

Figure 2.4: The modified IEEE 9 bus system with power flow directions and a main contingency.

As we discussed earlier, losing a transmission line or a generator is one of the major contingencies and can have a huge impact on the system. This can be clearly seen in Figure 2.5. Except for line 3, line 7 and line 8, all other lines are experiencing a significant overload (for line 5 the power flow is even reversed), and this will either lead to a failure of the transmission lines or triggering the protection systems on the lines to disconnect the lines. This process will include most of the lines and cause cascading outages.

Here, two important assumptions are made. First, the transmission lines can withstand the extra power flow, and second, generators can feed the required extra generation in new system configuration. Furthermore, the power flow on Line 7 is slightly less than the expected power flow. This could be due to the loss in the new system configuration.

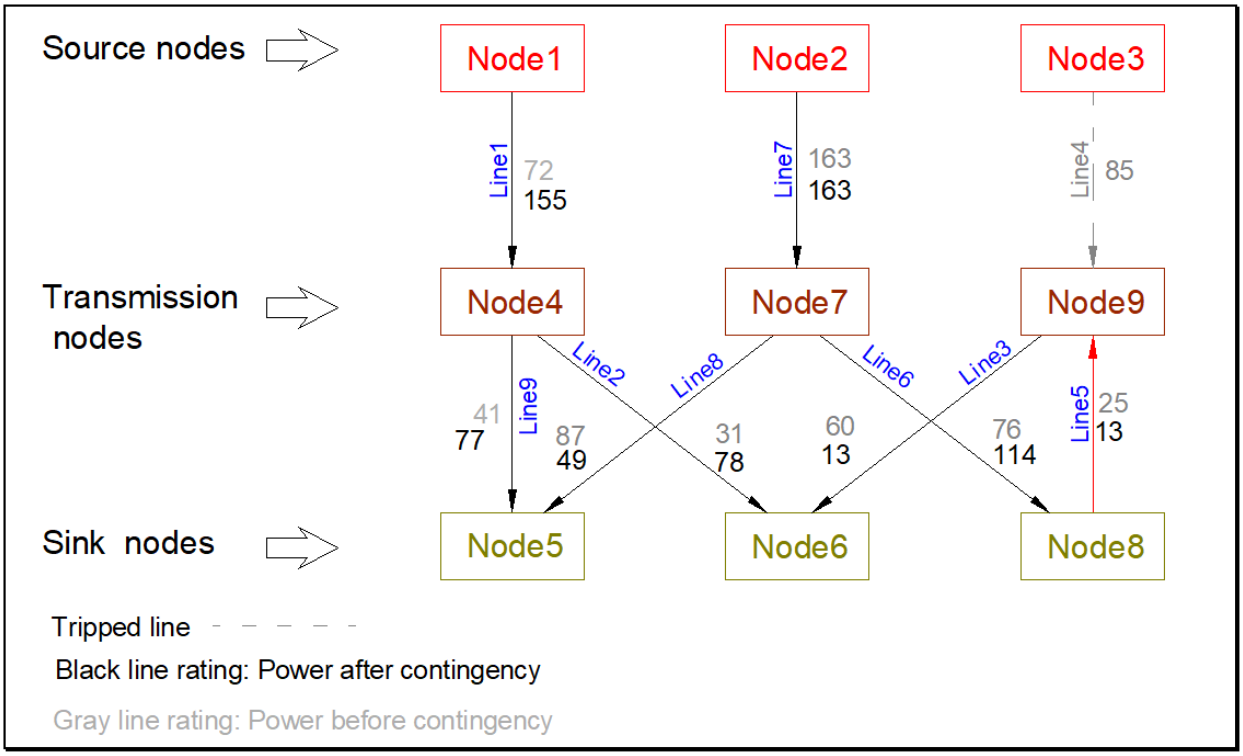

Figure 2.5: The power flow-based model with one contingency

An updated vulnerability index distribution is calculated for this contingency, with the results illustrated in Figure 2.6.

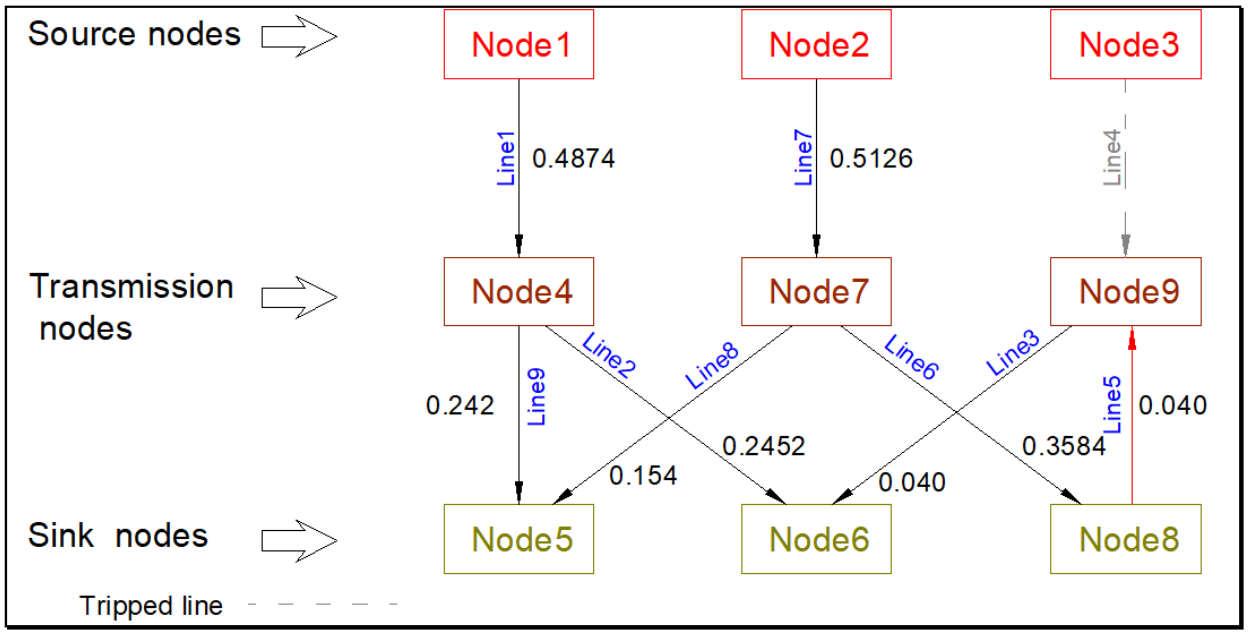

Figure 2.6: V.I. distribution of IEEE 9 bus system with one contingency

Even if we assume that all transmission capacities are more than the new power flows, the resultant V.I. listed in the Table 2.2 distinctly clarifies that the number of critical lines (by considering same V.I. threshold) are now 67% larger than for the system with this loading and no contingency.

Table 2.2: Vulnerability Ranking Based on V.I. With One Contingency

	V-Rank	V-Index	Line	from BUS	to BUS
V.I. threshold: 0.24	1	0.5126	7	2	7
	2	0.4874	1	1	4
	3	0.3584	6	8	7
	4	0.2452	2	6	4
	5	0.242	9	5	4
	6	0.154	8	5	7
	7	0.04	3	6	9
	8	0.04	5	8	9

The next step is to apply a simple RAS in the same system with the same contingency and observe the vulnerability improvement (Figure 2.7). After losing either transmission line 4 or generator 85 MW on bus 3, the new power flow in the system is calculated using a power flow program, 120MW load is shed at Buses 5 and 6, and 60MW generator on Bus 2 is shed. The corresponding power flow-based model and V.I. distributions are shown in Figure 2.8 and Figure 2.9, respectively.

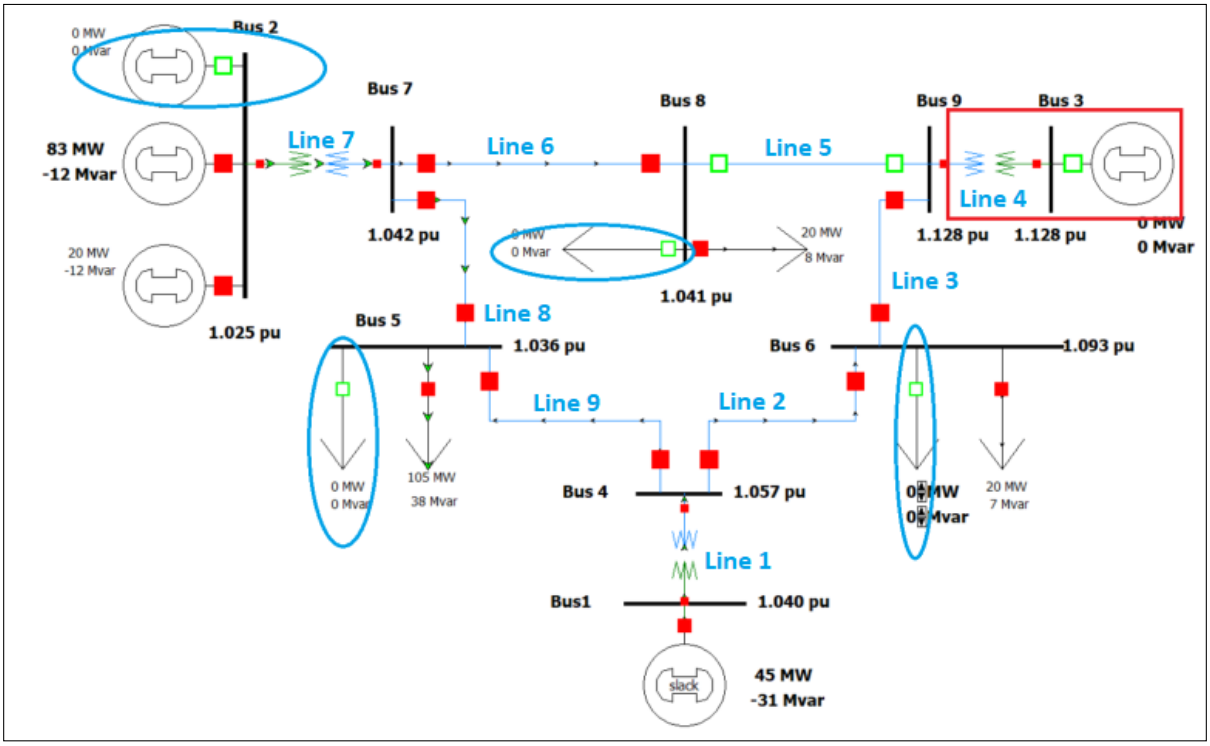

Figure 2.7: The modified IEEE 9 bus system, with one contingency and applied RAS.

After evaluating the network and estimating the new power flow, the graph is modified as Figure 2.8.

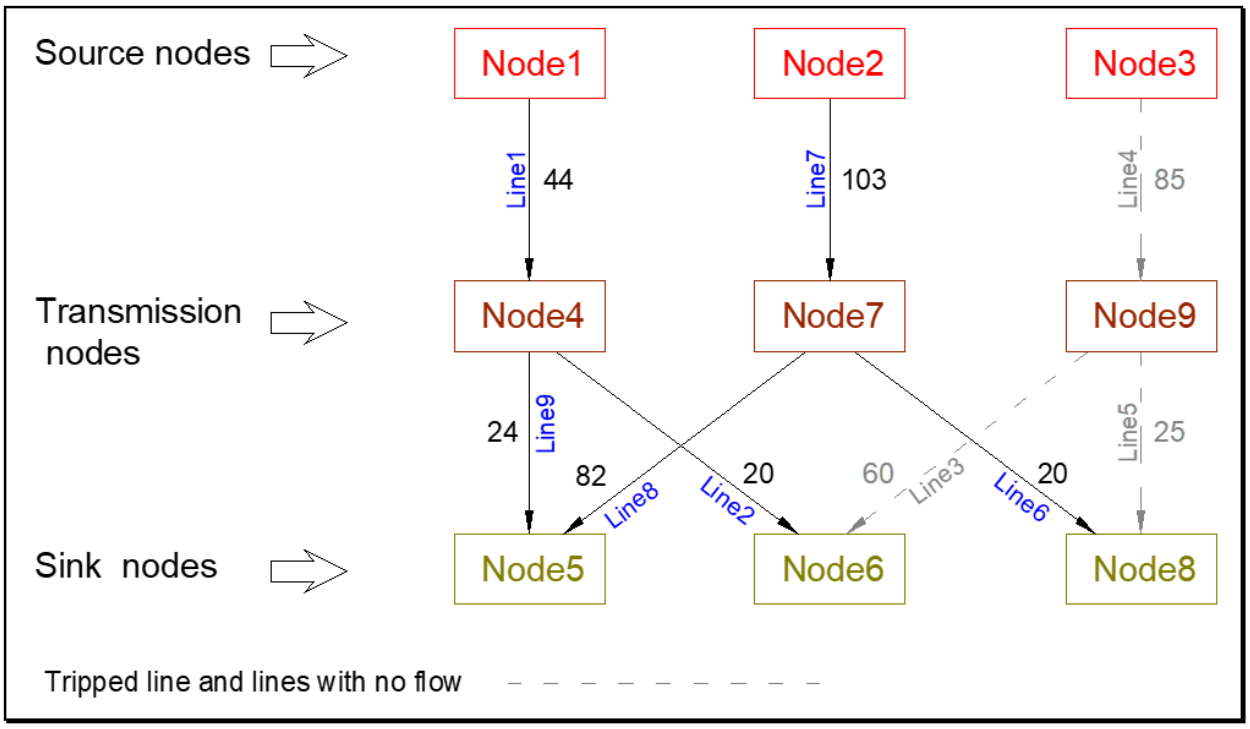

Figure 2.8: The power flow based model with one contingency and applied RAS.

With the assumed contingency and the applied RAS, the new vulnerability index distribution is depicted in Figure 2.9.

After applying RAS, the vulnerability for the system is improved by reducing the number of lines over the threshold from 5 to 3 (using same V.I. threshold) and shown Table 2.3.

Table 2.3: Vulnerability Ranking Based On V.I. With One Contingency and An Applied RAS

	V-Rank	V-Index	Line	from BUS	to BUS
An example of V.I. threshold: 0.24	1	0.7	7	2	7
	2	0.55	8	5	7
	3	0.29	1	1	4
	4	0.16	9	5	4
	5	0.13	6	8	7
	6	0.13	2	6	4
	7	0	3	6	9
	8	0	5	8	9
	9	0	4	3	9

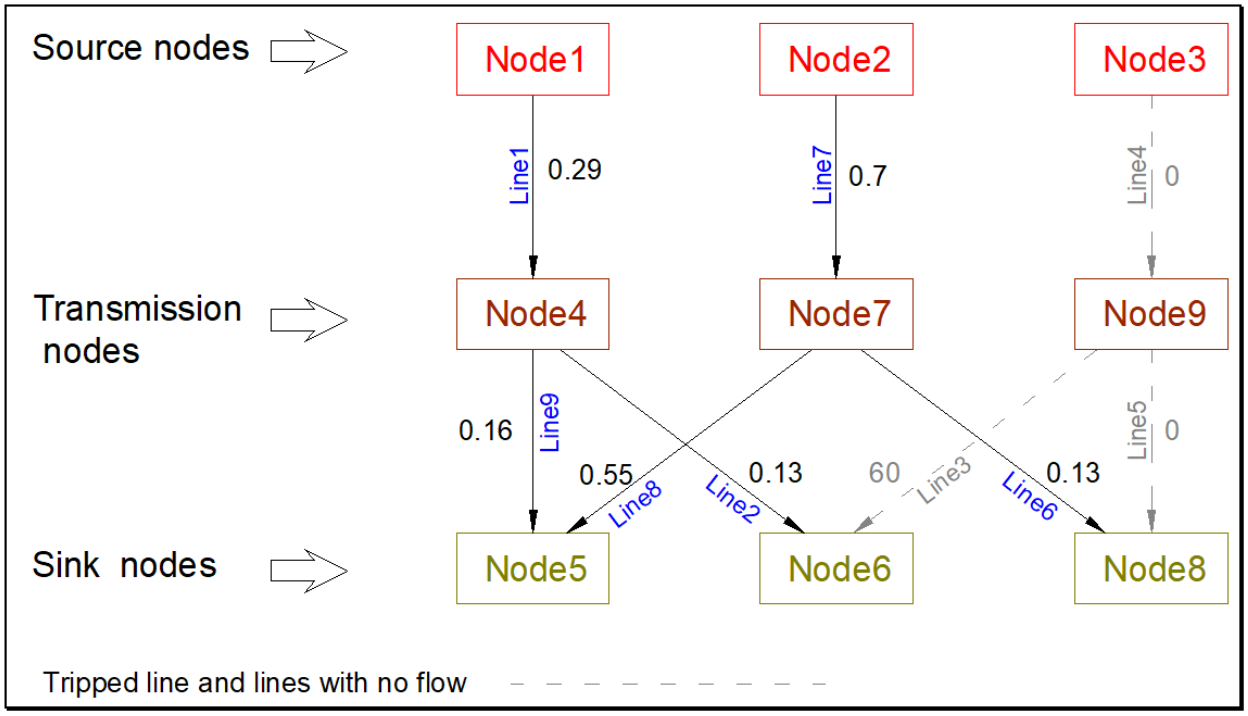

Figure 2.9: V.I. distribution of IEEE 9 bus system with one contingency and applied RAS.

Table 2.4 compares the vulnerability rankings from the three cases. A minimum RAS was applied to the system with a major contingency and it enhanced the resiliency of the system to the same level with the system that has no contingencies. In addition, lines 7 and 8 are identified the most critical lines in both original network and the network with contingency and RAS. This is clearly emphasizing that these lines are of a high importance. and can be used to identify the lines that need more extra monitoring and protection.

Table 2.4: Comparison of Vulnerability Rankings Based on V.I.

V.I. threshold: 0.24	Ranks without contingency				Ranks in one component lost				Ranks with RAS		
	V-Rank	V-Index	Line		V-Rank	V-Index	Line		V-Rank	V-Index	Line
	1	0.5114	**7**		1	0.5126	**7**		1	0.7	**7**
	2	0.2722	**8**		2	0.4874	**1**		2	0.55	**8**
	3	0.263	**4**		3	0.3584	**6**		3	0.29	**1**
	4	0.2392	6		4	0.2452	**2**		4	0.16	9
	5	0.2256	1		5	0.242	**9**		5	0.13	6
	6	0.1871	3		6	0.154	8		6	0.13	2
	7	0.1289	9		7	0.04	3		7	0	3
	8	0.0967	2		8	0.04	5		8	0	5
	9	0.0759	5		9	0	4		9	0	4

After the sensitive lines are determined by a V.I. threshold, they need to be prioritized in protection, operation, and monitoring to improve the system resiliency and prevent blackouts [19].

2.6 Conclusion

This chapter briefly reviewed the RAS and system vulnerabilities and utilized a power flow-based method to perform vulnerability assessment on a system with an integrated RAS. The most vulnerable lines were identified, and a special protection scheme was implemented for those lines. By protecting them, the system resiliency was noticeably increased. As the simulation results demonstrate, a considerable vulnerability improvement was achieved by applying even a simple remedial action scheme. The vulnerability indices and their ranking can clearly verify the resiliency improvement of the power system and therefore better immunity against failures.

Chapter 3: Power Grid Security Improvement by Remedial Action Schemes Using Vulnerability Assessment Based on Fault Chains and Power Flow

The results of this work were published in the Proceeding of the International Conference on Probabilistic Methods Applied to Power Systems (PMAPS 2018) [6]. Here, the numbers for citations, equations, tables, and sections have been updated for inclusion in this thesis and therefore differ from the publications originally accepted form. The original paper is available upon request.

3.1 Introduction

A resilient power supply is an important requirement for our society. The power demand increases every year and the structure of power systems becomes more complex as more renewable energy sources are connected to transmission and distribution networks. These new generation sources potentially have a negative impact on the resiliency of the power grid and can possibly cause network instability [3]. Such instability could lead to blackouts in some scenarios. Critical transmission lines must be recognized by assessing the systems vulnerability and special protections and corrective actions such as Remedial Action Schemes (RAS) must be applied on these lines to prevent cascading blackouts.

In this chapter, we aim to (1) identify the most critical lines that contribute to cascading blackouts due to failures or intentional attacks, (2) analyze effects of applying RAS on these lines, and (3) illustrate the resulting decline in the probability of cascading blackouts. The domino effect of the failures demonstrates that each event of the cascading failure is dependent on other failures [20]. Thus, a series of step by step failures results in a cascading blackout. The vulnerable transmission lines of the power systems play a significant role and constitute a measure of the systems susceptibility [4]. Therefore, recognizing those lines or components and analyzing the network vulnerability degree are essential prerequisites to

monitor and control these systems. The fault chain theory deals with the possible sequence of faults in the network and its criticality ranking is based on the number of the segments in each sequence. While in power flow-based method, the amount of power carried, and the line capacity determine the vulnerability ranking. Each approach has its drawbacks. To overcome these, a new vulnerability index is presented, combining the best features of each.

By identifying critical components of the system and protecting them, its vulnerability can be improved, and the system becomes more resilient. An effective resilient system is able to prepare and plan for, anticipate, withstand, adapt to, and rapidly recover from a disturbing event [5]. One way to accomplish these objectives is to utilize RAS. RAS have been increasingly used by utilities to mitigate stability problems following the loss of one or more transmission lines or generators. A RAS prevents the power system from experiencing out of step conditions that may result in cascading system-wide outages. The remedial strategies prevent potential cascading events by applying predetermined corrective plans to the most critical lines.

The IEEE 14-bus test system is utilized to examine the fault chain-based analysis, the power flow-based analysis, the proposed index calculation, and the effectiveness of RAS. The proposed approach provides a better understanding of the operational characteristics of the network and helps in determining where to focus RAS and other protection actions by exploiting fault chains and power flows. Here, we use two different approaches to evaluate the vulnerability of transmission networks. First, we use the fault chain theory to determine the most probable sequences of failures and calculate the related vulnerability indices, which is presented in Section 3.2. Next, we assess the system vulnerability using a power flow-based method in Section 3.3. In Section 3.4, a new vulnerability index is presented to better determine the critical lines. Section 3.5 demonstrates the impacts of RAS in improving the system resiliency and mitigating the vulnerabilities to cascading outages by providing predetermined corrective actions on the critical lines.

3.2 Fault Chain Theory

In this section, four stages are discussed. First, the basic of cascading failure and fault chain is presented. Next stage is about determination of the fault chains. Then, the criticality ranking procedure is discussed. Lastly, this approach is applied on the IEEE 14 bus system.

A. *Cascading Failures and Fault Chains*

The primary reason for a widespread blackout is cascading failures. The possible causes of these failures might be human factors, relay maloperation, mismanagement, weather, overload, and intentional attacks [1]. In fault chain theory these are called the influencing factors. Suppose that in a network, the protection system isolates one line due to a fault. To supply the load, other lines must carry additional power and therefore would be loaded more heavily and potentially results in an overload risk. This process propagates through the network, overloading the lines one after another to eventually cause total system instability. The contingency analysis process contains top and basic events [21]. Basic events are those faults that create a fault chain, while a top event is a cascading outage.

In earlier literature, a fault-tree was a minimal cut-set that was achieved offline, and which was obtained by experience or contingency evaluations [21]. This was not always practical and accurate. The method in this chapter accomplishes the fault chain online by using system stability measures and operational parameters [22].

B. *Fault Chain Determination*

Fault chains and their segments are defined as

$$L = \left\{ \overrightarrow{L1}, \quad \overrightarrow{L2}, \quad ..., \ \overrightarrow{Ln} \right\} \tag{3.1}$$

$$L = \{T_{i1}, T_{i2}, ..., T_{im_i}\} \tag{3.2}$$

where n is the number of fault chains; m_i is the number of segments of the i^{th} fault chain; L is a fault chain set of a network; T_{ij} is the j^{th} segment of the i^{th} fault chain $\overrightarrow{Li}$, and $j = 1, 2, ..., m_i$. The fault tree logic is shown in Figure 3.1.

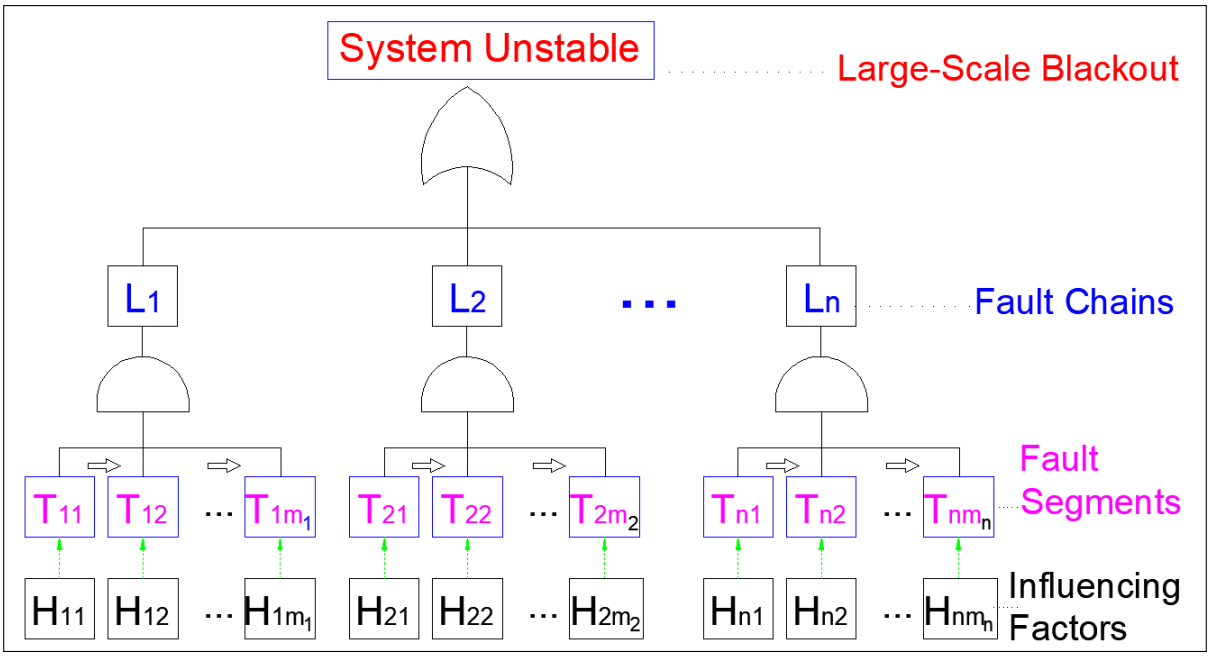

Figure 3.1: Fault chain logic indicating influencing factors, fault segments, and fault chains that can cause cascading outages.

All fault chains are included in the cascading outages vulnerability analysis by a single OR gate. Each fault chain is a result of an AND gate that comprises all related basic events and segments. Therefore, it can be understood from the tree that if all segments of a fault chain occur in sequence, then the system will be unstable, and cascading outages happen [23].

All fault chains are included in the cascading outages vulnerability analysis by a single OR gate. Each fault chain is a result of an AND gate that comprises all related basic events and segments. Therefore, it can be understood from the tree that if all segments of a fault chain occur in sequence, then the system will be unstable, and cascading outages happen [23].

The segment faults are due to the influencing factors. These factors and the related influencing function are defined as

$$V_i = \{v_{i1,}\ v_{i2,}\ ...v_{ik_i,}\} \tag{3.3}$$

$$\phi(\overrightarrow{L_i}) = \sum_{j=1}^{k_x} \omega_{H_{ij}} v_{ij} + \sum_{j=k_x+1}^{k_i} \omega_{H_{ij}} v_{ij} \tag{3.4}$$

where v_{ij} is the j^{th} factor, $\omega_{H_{ij}}$ is the sensitivity coefficient of the j^{th} factor for i^{th} fault chain, k_x is the number of certain factors, and k_i is the number of all factors. The probability of the i^{th} fault chain occurring is defined as

$$q_{\overrightarrow{Li}} = q(T_{i1}T_{i2}...T_{im_i}) = q(\bigcap_{j=1}^{m_i} T_{ij}) \tag{3.5}$$

where j is the sequential number of basic events, and $q_{\overrightarrow{Li}}$is the i^{th} fault chain probability. From Figure 3.1, the probability of cascading outages can be obtained from the fault chain probabilities by:

$$Q_s = 1 - (1 - q_{\overrightarrow{L1}})(1 - q_{\overrightarrow{L2}})...(1 - q_{\overrightarrow{Ln}}) \tag{3.6}$$

With each line outage, a new path is taken as the most efficient one to redistribute the power flow. Using the former segments, the new segment $T_{(i(j+1))}$ is predicted with highest probability. Let's assume $T_{(i(j-2))}$ is the fault segment on line k-2, $T_{(i(j-1))}$ is the fault segment on line k-1, $T_{(j+1)}$ is the fault segment on line k, and $T_{(i(j+1))}$ is the fault segment on line k-1. To identify the fault chains, the following should be taken into consideration to determine lines [24, 25]:

- Power flow change;

$$\alpha_{ij}^{k+1} = \mid \frac{S_{ij}^{k+1} - S_{i(j-2)}^{k+1}}{S_{i(j-2)}^{k+1}} \mid + \mid \frac{S_{i(j-1)}^{k+1} - S_{i(j-2)}^{k+1}}{S_{i(j-2)}^{k+1}} \mid \tag{3.7}$$

- Overload capability;

$$\beta_{ij}^{k+1} = \mid \frac{S_{i(j-1)}^{k+1}}{S_{Max}^{k+1}} \mid + \mid \frac{S_{ij}^{k+1}}{S_{Max}} \mid \tag{3.8}$$

- Power flow change due to the previous fault segments;

$$\gamma_{ij}^{k+1} = \mid \frac{S_{ij}^{k+1} - S_{i(j-1)}^{k+1}}{S_{i(j-1)}^{k}} \mid + \mid \frac{S_{i(j-1)}^{k+1} - S_{i(j-2)}^{k+1}}{S_{i(j-2)}^{k-1}} \mid \tag{3.9}$$

where $S_{max}^{(k+1)}$ is the maximum power capacity of line k+1; $S_(i(j-2))^{(k+1)}$; $S_{(i(j-1))}^{(k+1)}$, and $S_{ij}^{(k+1)}$are complex power flows of line k+1 after the fault on segments $T_{(i(j-2))}$, $T_{(i(j-1))}$, and T_{ij}; $S_(i(j-1))^{k}$ is the complex power of line k after the fault on segment $T_{(i(j-1))}$; $S_{(i(j-2))}^{(k-1)}$ is complex power of line k-1 after the fault on segment $T_{(i(j-2))}$. The edge-weight can normalize the three indices [26]:

$$R_{ij}^{k+1} = \frac{\mid S_{ij}^{k+1} \mid}{\sum_{u-1}^{n} \mid S_{ij)}^{u} \mid} \tag{3.10}$$

$$\omega_1^{k+1} = \begin{cases} 0 & S_{ij}^{k+1} < S_{i(j-2)}^{k+1} \cap S_{i(j-1)}^{k+1} < S_{i(j-2)}^{k+1} \\ R_{ij}^{k+1} & \text{otherwise} \end{cases} \tag{3.11}$$

$$\omega_2^{k+1} = \begin{cases} 1 & S_{ij}^{k+1} > S_{Max}^{k+1} \\ R_{ij}^{k+1} & \text{otherwise} \end{cases} \tag{3.12}$$

$$\omega_3^{k+1} = \begin{cases} 1 & \triangle S_{ij}^{k+1} > S_{Max}^{k+1} \\ R_{ij}^{k+1} & \text{otherwise} \end{cases} \tag{3.13}$$

where $\omega_1^{(k+1)}$, $\omega_2^{(k+1)}$ and $\omega_3^{(k+1)}$ are the weight normalizers [22]. The next segment to fault on the i^{th} fault chain is presumed by the value of $F_{(i(j+1))}^{(k+1)}$. The next occurrence will be on the line with maximum F.

$$F_{i(j+1)}^{k+1} = \omega_1^{k+1}\alpha_{ij}^{k+1} + \omega_2^{k+1}\beta_{ij}^{k+1} + \omega_3^{k+1}\gamma_{ij}^{k+1} \tag{3.14}$$

The sequence of occurrences is presumed by calculating F repeatedly until the system is unstable. This sequence is the i^{th} fault chain. By applying the same process for all lines, a set of fault chains are obtained.

C. *Vulnerability Assessment*

In vulnerability assessment by fault chains, if a transmission line is involved in a larger number of fault chains, it will be more vulnerable. Each line has different vulnerability in each fault chain. As a starting point, suppose that the impacts of influencing factors on all segments stay the same.

If the failure event Mi occurs on a specific transmission line, then all fault chains which comprise this event are expressed as

$$L^1 = \left\{ L_1^1,\ L_2^1,\ ...,\ L_{b_1}^1 \right\} \tag{3.15}$$

$$L^2 = \left\{ L_1^2,\ L_2^2,\ ...,\ L_{b_2}^2 \right\} \tag{3.16}$$

$$L^s = \left\{ L_1^s,\ L_2^s,\ ...,\ L_{b_s}^s \right\} \tag{3.17}$$

The occurrence probability of the fault chain increases with a decrease in the number of segments in the chain. Therefore, the number of the segments of a chain determines its relative occurrence probability. The vulnerability index of an event is defined as

$$\phi(Mi) = \frac{\sum_i (\frac{a_{m_i}}{b_i})}{\sum_j \sum_k (\frac{a_j}{b_k})} \tag{3.18}$$

where i=1,2, ..., s, j=1,2, ..., q, and k=1,2, ...,s_j. Here, s_j is the number of the fault chains including the j^{th} transmission section, q is the number of all the transmission sections in network, s is the number of all chains. And a_{mi} is the number of transmission lines related to the event Mi [22].

D. *Case Study IEEE 14-Bust Test System*

The IEEE 14-bus test system is simulated using Powerworld software to verify the performance of vulnerability assessment methods (Figure 3.2).

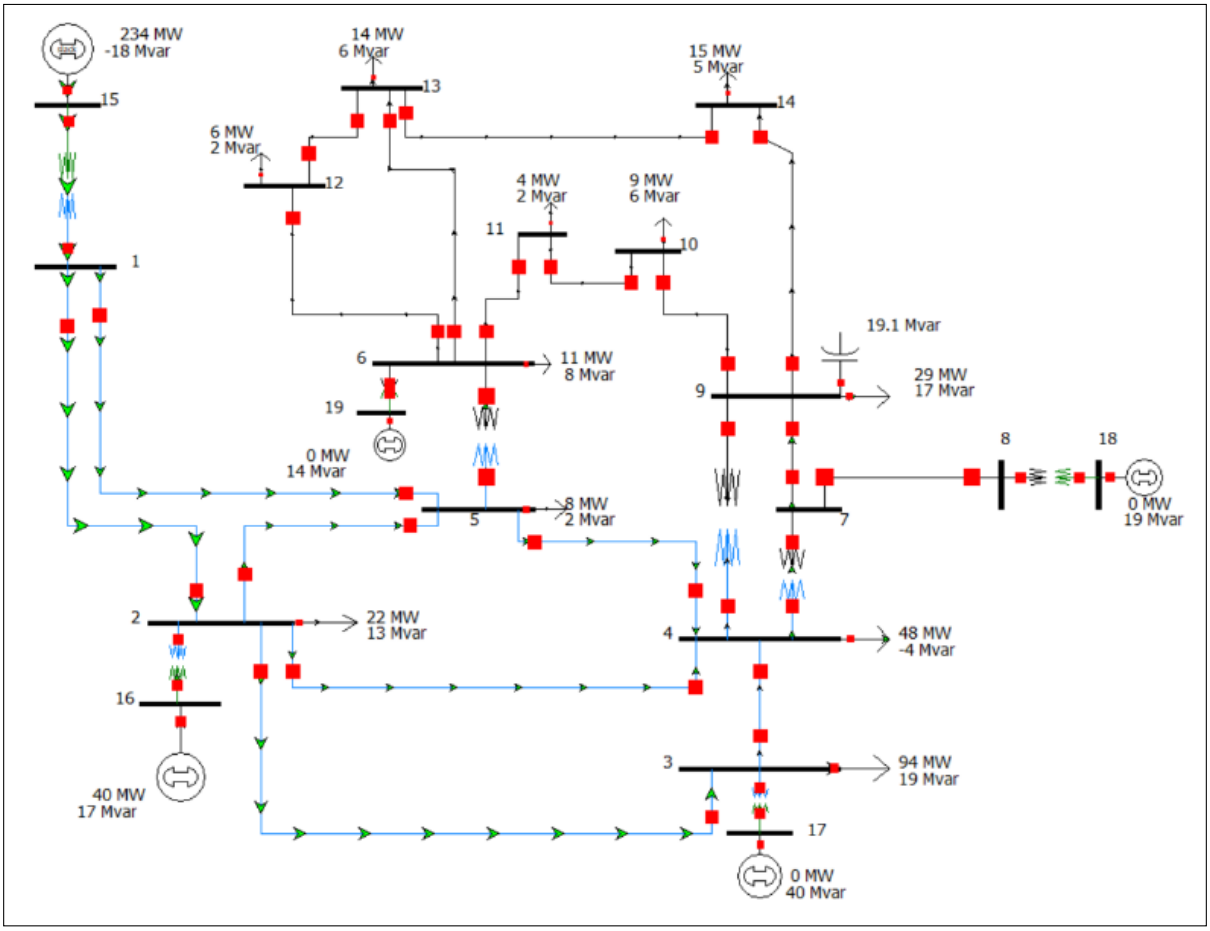

Figure 3.2: IEEE 14-bus test system implemented in Powerworld software.

This system contains 20 transmission lines, 5 generators, and 11 loads. Table 3.1 shows the fault chains and Table 3.2 ranks the lines by vulnerability index (V.I.) [22].

Table 3.1: Fault Chains of The IEEE 14 Bus System

No	Fault Chains	No	Fault Chains
L1	b1, b4	L11	b11, b12, b8
L2	b2, b6, b3, b7, b8	L12	b12, b8, b11
L3	b3, b7, b2	L13	b13, b8, b17
L4	b4, b1	L14	b14, b13, b1, b4
L5	b5, b1, b4	L15	b15, b16, b17, b1, b4
L6	b6, b2, b1, b4	L16	b16, b19, b17, b1, b4
L7	b7, b3, b2	L17	b17, b8, b13
L8	b8, b13, b17	L18	b18, b1, b4
L9	b9, b8, b11	L19	b19, b1, b4
L10	b10, b1, b4	L20	b20, b1, b4

As previously explained, the lines in fault chains with fewer segments are more probable to cause cascading outages, such as L1 or L4. On the other hand, L15 and L16 have smaller possibilities to lead to cascading outages. For these longer chains, the probability of failing several lines is smaller, especially in that exact sequence which would lead to cascading outages. Even if these less likely events do occur, due to the high number of segments, the fault propagation time is long enough to let the protection systems kick in and prevent further failures.

Table 3.2: Vulnerability Indices and Ranking By Fault Chain

Rank	Failure event	V.I.	Rank	Failure event	V.I.
1	b1	0.18379	10	b7	0.02748
1	b4	0.18379	10	b19	0.02748
2	b8	0.11336	11	b16	0.02061
3	b13	0.06441	12	b5	0.01718
4	b2	0.05702	12	b9	0.01718
5	b17	0.05496	12	b10	0.01718
6	b11	0.05153	12	b18	0.01718
7	b6	0.04784	12	b20	0.01718
8	b3	0.04466	13	b14	0.01288
9	b12	0.03435	14	b15	0.01031

3.3 Power Flow Based Method

Another approach to assess the vulnerability index is use of a power flow-based method. This approach is based on a weighted directed network with the following assumptions [17]:

- Buses and lines in a power grid are classified as nodes and edges, respectively. Each node is perfectly reliable, and each edge has two states: working or failed.
- Each edge has its own direction, which is the same as the direction of the power flow on the transmission line.
- The degree of all nodes is at least 2, except for the source nodes and sink nodes.

The procedure of calculating and ranking the V.I. follows [18]:

- Build a connection network model of the power system.
- Calculate the steady-state power flow of the grid and collect data (Figure 3.3).
- Weight the edges in the network model with the power flow and determine the flow directions (for e.g. Figure 3.3).
- Calculate the maximum flow of the network for each source – sink combination. Given a network G = (V, E), the capacity and flow on the edge (i, j) are denoted by $c_{(ij)}$ and $f_{(ij)}$, respectively. A source node and a sink node are denoted by s and t. The residual network of G is shown by G_f (V,E_f). The capacity of G_f is defined by (2.1).

  The maximum flow is calculated as follows: Initially, for each edge (i, j), set the flow at $f_{(ij)=0}$. Given a path p from s to t in G_f , for all edges $(i, j) \in p$, find $c_{f(p)}$ from (2.2) For each edge $(i, j) \in p$ calculate f_{ij} and f_{ji} from (2.3) and (2.4), respectively.
- Using the equation (2.5), sum up the flow values and compute a vulnerability index V_{ij}. We can get the flow on each edge corresponding to the maximum flow in the network.

Then the vulnerability index of edge (i, j) can be defined as the level of flow carried by edge (i, j) compared to the maximum flow of the network.

- Rank the lines according to values of vulnerability index (Figure 3.3). The line with a high value of index is considered as more critical in this analysis.

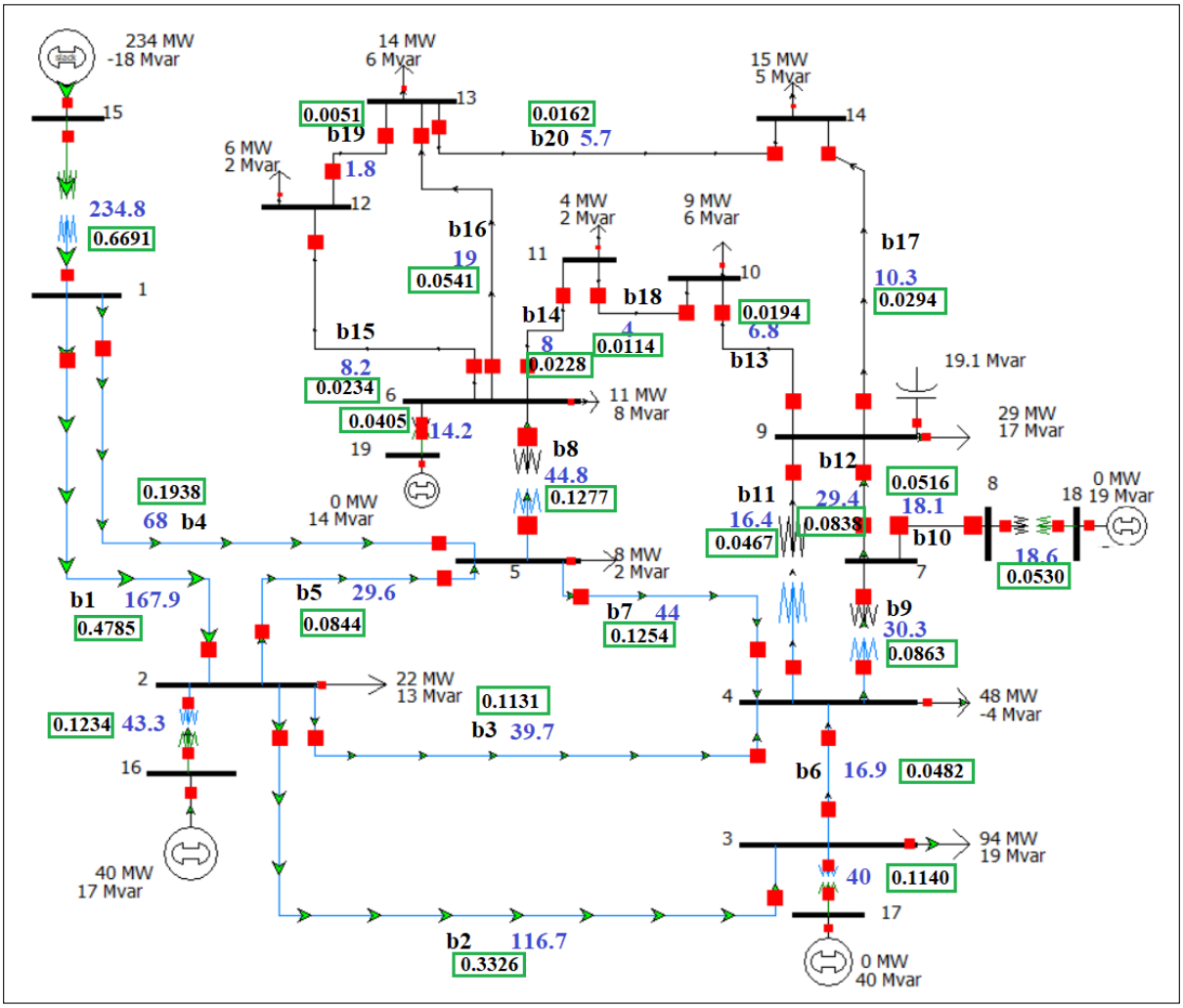

Figure 3.3: Steady-state power flow (blue text) and vulnerability index weights (black text in green box) on the IEEE 14-bust test system.

In Figure 3.3, line numbers are denoted with b1 through b20, the branch power flow, which is the Powerworld simulations result, is shown on each line, and the related vulnerability index is highlighted in a green box. The immediate lines that connect the generators to the network are not in the Table 3.3 ranking.

The ranking results are presented in Table 3.3.

Table 3.3: Vulnerability Indices and Ranking By Power Flow

Rank	Failure event	V.I.	Rank	Failure event	V.I.
1	b1	0.4785	11	b10	0.0516
2	b2	0.3326	12	b6	0.0482
3	b4	0.1938	13	b11	0.0467
4	b8	0.1277	14	b17	0.0294
5	b7	0.1254	15	b13	0.0234
6	b3	0.1131	16	b14	0.0228
7	b9	0.0863	17	b13	0.0194
8	b5	0.0844	18	b20	0.0162
9	b12	0.0838	19	b18	0.0114
10	b16	0.0541	20	b19	0.0051

3.4 The New Vulnerability Index

The fault chain theory determines the possible sequence of faults in the network and the criticality ranking is based on the number of the segments in each sequence, while, the maximum power flow of the network and of each source-sink combination is overlooked. On the other hand, in the power flow-based method, the amount of transfer power and the maximum capacity of the network are important factors, but this method doesn't provide any information regarding the sequence of events in fault chains and their occurrences. Each approach has its drawbacks. To overcome these drawbacks, a new vulnerability index V_{st}^{Mi} is presented that comprises both approaches.

The best way to combine these two indices is to find the product of indices for each line and use it in criticality ranking. Thus, the impacts of both indices are effectively applied. Other forms of combination are not suitable. For example, if they combine to form a^b, due to the fraction numbers for b, the result is actually the root of number a, which is diminishing the impact of a therefore it is not desirable. If they form $a + b$, due to the range differences between two indices, the impact of the smaller one will be overlooked. Therefore it is not is

not a proper combination too. From (3.18) and (2.5);

$$V_{st}^{Mi} = \phi(Mi)\ V_{ij} = \frac{\sum_i (\frac{a_{m_i}}{b_i})}{\sum_j \sum_k (\frac{a_j}{b_k})} \frac{\sum_u^m \sum_v^n f_{ij}^{uv}}{\sum_u^m \sum_v^n f_{Max}^{uv}} \tag{3.19}$$

where Mi is the event occurs on line i, which is between buses s and t. Here, to avoid confusion, the node labels are changed to s and t. The new ranking based on V_{st}^{Mi} index is shown in Table 3.4.

Table 3.4: Vulnerability Indices and Ranking By New V.I.

Rank	Failure event	V.I.	Rank	Failure event	V.I.
1	b1	0.08794	11	b9	0.00148
2	b4	0.03562	12	b5	0.00145
3	b2	0.01896	13	b13	0.00125
4	b8	0.01448	14	b16	0.00112
5	b3	0.00505	15	b10	0.00089
6	b7	0.00345	16	b14	0.00029
7	b12	0.00288	17	b20	0.00028
8	b11	0.00241	18	b15	0.00024
9	b6	0.00231	19	b18	0.00020
10	b17	0.00162	20	b19	0.00014

In the new ranking, the critical lines are those which carry the higher power flow in the network and contribute in a larger number of fault chains. Figure 3.4 shows the most critical lines relative to a sample V.I. threshold. By choosing 0.01 for V.I., lines b1, b4, b2, and b8 are recognized as the most critical lines.

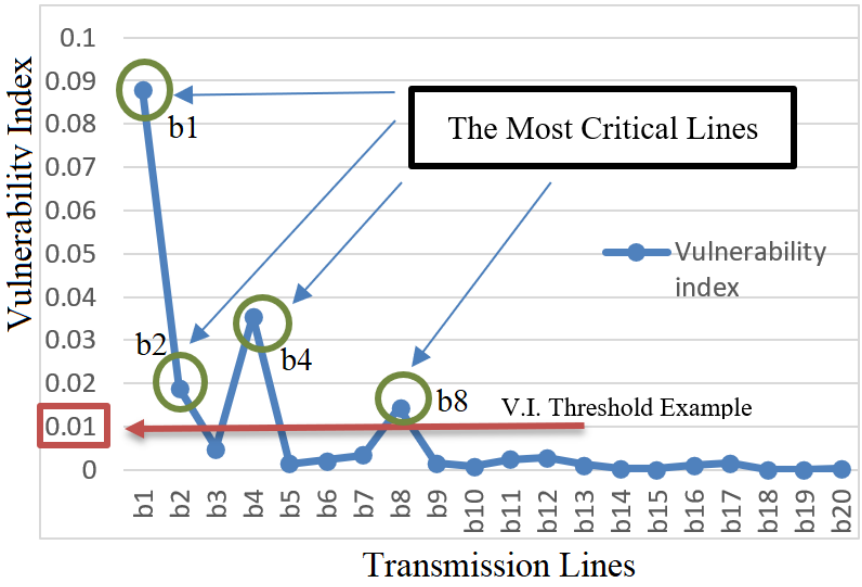

Figure 3.4: Determining the most critical lines when 0.01 is the V.I. threshold.

Some inferences from these three vulnerability rankings are:

- The critical lines vary by selecting a different V.I. threshold.
- The smaller the V.I. threshold the higher the number of lines recognized as critical.
- The highlighted lines b1, b2, b4, and b8 are recognized as the top 25
- The results from the proposed V.I. are more useful in recognizing the critical lines than using fault chains or the power flow method alone.

After setting a sample vulnerability index threshold and obtaining the sensitive lines, these lines must be prioritized in monitoring, operation, and special protection of power system to prevent the cascade failures [19].

3.5 Critical Line Protection and Vulnerability Improvement

The most critical lines and components can be protected by:

- Remedial Action Schemes,

- Improving cybersecurity associated with relays, SCADA, and PMUS related to these lines and components, and
- Improving physical security of substations.

Since the most critical lines are involved in the largest number of fault chains, preventing their failure, dramatically decreases the probability of cascading outages and the whole system vulnerability improves [14, 19].

Assume the influencing factors for simplicity are the same for all segments in fault chains and therefore the probability of an event for all segments $q(T_{(ij)})$ will be the same as well. For example, let the probability of each segment be 0.5. From (3.5), the probability of the i^{th} fault, $q_{\overrightarrow{Li}}$, occurring is obtained and from (6), the cascading outages probability Q_S is calculated as 0.92 (Figure 3.5).

This probability is obtained by considering all the possible fault chains (Table 3.1). However, by applying proper protection and preventing a specific fault chain from occurring, in the cascading outages probability calculation that fault chain will not be involved and consequently, the Q_S probability will be reduced. By providing protection for lines that have higher $q_{\overrightarrow{Li}}$ and more criticality, the outcome Q_S will be less likely and the system is more hardened.

If line b4 or b1 is protected, for instance via RAS, the vulnerability is improved and the cascading outages probability Q_S is decreased by 27.5% (see Figure 3.5). It is noteworthy that the smallest fault chain that contains b4 has 2 lines. There are 3 lines in the smallest fault chain associated with b7 or b2 lines and by protecting these lines the improvement is 11.2%. By protecting lines that are in a fault chain with 4 lines the improvement will be 5%. Therefore, the longer the chain that includes the protected line is, the smaller the vulnerability index improvement will be.

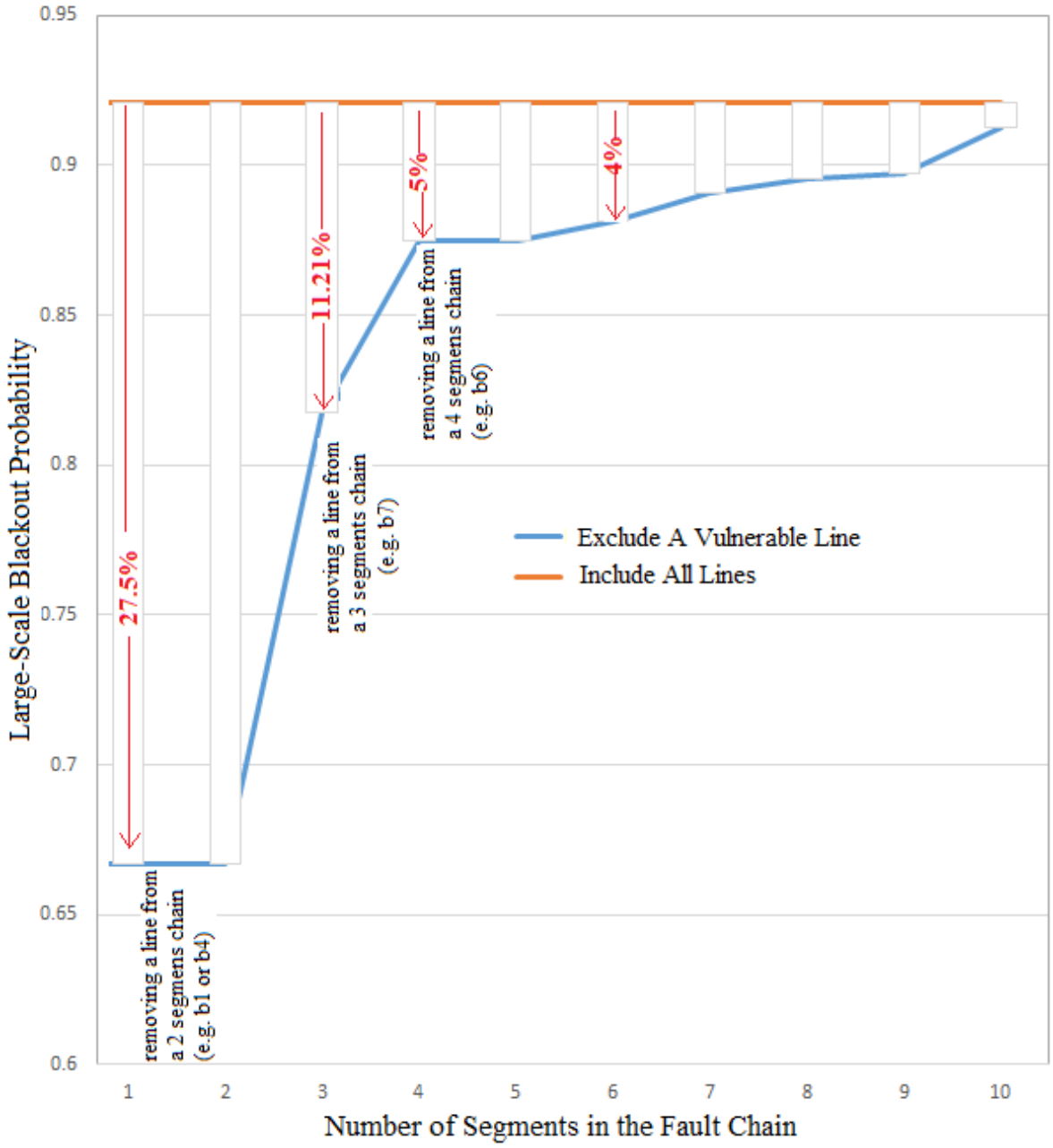

Figure 3.5: Probability of cascading outages and removal of vulnerable transmission line in probability calculations

It is obvious that the system security would be greatly improved if a special protection (e.g. a RAS) is applied to the lines with higher vulnerability indices to better control the system and prevent cascading failures. The procedure for determining critical lines to protect with remedial actions schemes to reduce the system vulnerability can be scaled to

larger systems and will be tested on larger IEEE test cases.

3.6 Conclusion

In this chapter, a new vulnerability indexing approach is proposed to better analyze and determine the critical transmission lines. Vulnerability assessment of the IEEE 14-bus test system is performed by using three different approaches and the results are compared and analyzed. The most critical lines are recognized, and special protection schemes are considered for these lines. The resultant improvement of the system vulnerability is verified by studying the cascading outage probability. By protecting the most critical line with the highest vulnerability, the cascading outage probability is noticeably reduced.

Chapter 4: A New Method of Securing RAS by Detecting False Measurement Using Cause and Effect Analysis and Measurement Consistency

4.1 Introduction

For any power grid, the threat of physical events and cybersecurity events need to be analyzed. In physical security, the goal is to secure the electric grid against physical attacks. Similarly, cybersecurity tries to secure the grid against cyber-attacks. Both security events could lead to disturbances to the electric services and subsequently impact on the public safety and health, economy, and national security.

Up to now, most physical incidents in the United States and Canada have had relatively minor consequences. While, cybersecurity events have been increasing [27]. Physical and cyber threats tend to be different, and demand different approaches to improve, protect and mitigate. In this project, cyber threats are under focus, and the following are of a high importance: system monitoring, state estimation, and defense against bad data injection and false measurement.

Monitoring power grids is necessary to provide system observability. By application of a proper monitoring system, there is sufficient information to reliably operate the system, and take proper corrective actions. These actions are based on the estimated state of the system, which are determined through analyzing measurements and system models. Measurements might be compromised or falsified by failures or by malicious parties. Therefore, false data detection techniques must be utilized to detect and replace the false data and provide reliable information for the RAS and thereby assure a reliable action based upon this data.

A. *System Monitoring*

System monitoring uses the measurements from Phasor Measurement Units (PMUs) and the Supervisory Control And Data Acquisitions (SCADA) system in the power grid to collect

and transfer the required data about the system conditions and thereby assures the reliable operation of the system. The measurements are normally real and reactive power, and bus voltages, which are generally provided and preserved by SCADA, and phase angles, which are estimated or provided by PMUs. This data is used for system analysis and monitoring.

B. *State Estimation*

In state estimation (SE), by analyzing the data and the power system models, the state of the system is estimated, and the unknown variables are evaluated. Contingency analysis uses the SE results and evaluated the possible causes of the operational issues. In order to prevent these issues, some actions may be taken, and the aftereffect of these actions will be analyzed. As an example, when a fault happens (such as isolating a system component or path), the power generation may be increased to maintain the reliable operation of the system [28]. Power flow modeling is the basis of the SE, which is a set of equations that illustrate power flow on each line of a grid. Alternating Current (AC) modeling studies both real and reactive power and formulates them by nonlinear equations. In SE, it is more common to use an approximated Direct Current (DC) power flow model instead of its AC model, since it uses linear equations. Thus, the computational expenses are reduced and a convergence to a solution is guaranteed [28, 29].

C. *False or Compromised Measurement Detection*

To achieve their goals, attackers may directly manipulate the measurements at the substation meters or indirectly at the data collectors or computers that store meter measurements. These bad measurements affect the SE results and reduce the situational awareness. Therefore, the corrective actions based on this information are not reliable and may result in the system instability.

We need to develop techniques to first detect them and then fix them or filter them out.

If the attackers know the exact current configuration of the system at the time of attack, they can bypass almost all existing defense algorithms. Most of these algorithms detect bad measurements when there is a significant difference between estimated and observed

data. To consider the worst case with the most sophisticated attackers, by knowing the system configuration, the attackers can generate bad measurements in a way that the injected difference is not significant enough to be detected and is not an abrupt change to trigger the detection techniques [30][31][32].

However, for the following reasons, it is not easy for attackers to practically launch these attacks. First, because of the regular maintenance and irregular events in power grids, configurations of these systems alter frequently. Moreover, accessing the control center of power companies to access such data is nearly impossible to attackers.

Second, to manipulate a specific value, the attackers need to compromise about 10 meters in most cases in the IEEE 300–bus system [32]. In our work, we use a measurement consistency method on the IEEE 118 bus system. For the area under focus, which only has 10 buses, malicious parties need to compromise at least 50 measurements to inject a single false data, which is a signal of the effectiveness of our approach. The reason for this is explained in Section 4.4.

For a successful attack, a malicious party needs to corrupt the following information and perform the following activities:

- Knowledge of the current system configuration
- Hardware failure or physical attack
- Measurements manipulation
- Communication and data collection interference
- Knowledge of maintenance and operation schedule and procedure
- Knowledge of the most effective parameters to compromise and therefore impose the most negative impacts

In our method of defense, attackers need to accomplish a higher degree of information and compromise more meters, therefore it is more reliable. In this chapter, we assess the

system vulnerability and optimally situate the PMU location using the Unified Approach and a sufficient set of RAS measurements. Further, we detect and fix the false measurement based on the proposed method called False Data Detection and Fixing (FDDF). After fixing measurements, we consider a remedial action scheme (RAS) to reduce the vulnerability of the system and harden the critical components against intentional attacks.

The rest of this chapter is organized as follows. In Section 4.2, as the primary step, we consider optimizing PMU locations based on Unified Approach [33] and sufficient RAS measurements (the idea of locating PMUs in those areas that makes the RAS hardening possible). In Section 4.3, a new structure for RAS is proposed. The proposed false data detection method is presented in Section 4.4. This section examines and validates the method through simulation using IEEE 118 test systems. Simulation results are provided to demonstrate the success of new securing method in filtering out the compromised data. In Section 4.5, we conclude our work.

4.2 Optimized PMU Location

For better system observability, protection and control in the power grid, PMUs are a promising equipment. PMUs provide important measurements for the system and are beginning to play an important role in system monitoring. Due to the high price of PMUs and their related support systems [34], only specific nodes can be equipped with PMUs. Therefore, it is very important to maximize the system observability with the minimum possible number of PMUs. In this project, the results of the approach used in article [33] are utilized to optimize number and location of PMUs for power system state estimation. This approach considers the impacts of both existing conventional measurements and PMU loss possibility into the decision strategy. The PMU location optimization results come directly from [33].

This approach is called Unified Approach, where the location of PMUs is defined using binary integer linear programming (BILP). Here, the variable is binary and determines the

installation requirement for PMUs at each bus. These placements comply with the goal of maintaining the system observability and minimizing the metering cost.

Using the referred approach, 24 PMUs are required for the IEEE 118 bus system (without considering PMU loss), with two of them in the area under our focus that will be discussed in Section in Section 4.4. The added PMUs are on buses 113 and 22. This number of PMUs make the network observable. A system is observable if the state estimate is able to determine a specific solution for a set of measurements and specify the network topology and measurement locations [33].

Reliable data is a significant requirement for a secured RAS. Therefore, we added two other PMUs to give redundancy for RAS (see Section 4.4). Furthermore, these extra two PMUs provide additional data for the process of false data detecting and fixing.

4.3 Improved RAS

By knowing the vulnerability of a system, proper actions can be created to improve system resilience. An effective resilient system is able to presume, adapt to, and rapidly recover from a disturbing event [5]. One way to accomplish these objectives for a power system is to utilize a RAS. These schemes have been increasingly used by utilities to mitigate stability problems. A RAS prevents the power system from experiencing out-of-step conditions that may result in cascading system-wide outages. The remedial strategies prevent potential cascading events by applying predetermined corrective plans to the most critical lines.

These corrective and remediation actions are taken based on the received measurements. False or compromised data can fake or hide an abnormality in the system and mislead the RAS to take a wrong action and exacerbate a situation with vital failures. Generally, the important components of RAS structure are measurements, arming conditions, RAS logic, and the triggering actions (Figure 4.1).

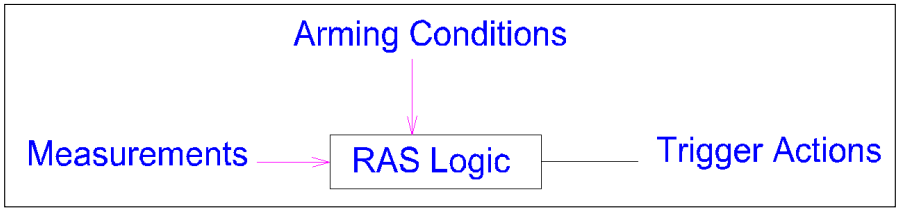

Figure 4.1: RAS structure without detection logic

To insure proper corrective action from RAS, Bad Data Detection (BDD) techniques can be used. These techniques verify the output of RAS prior to trigger the actions. (Figure 4.2).

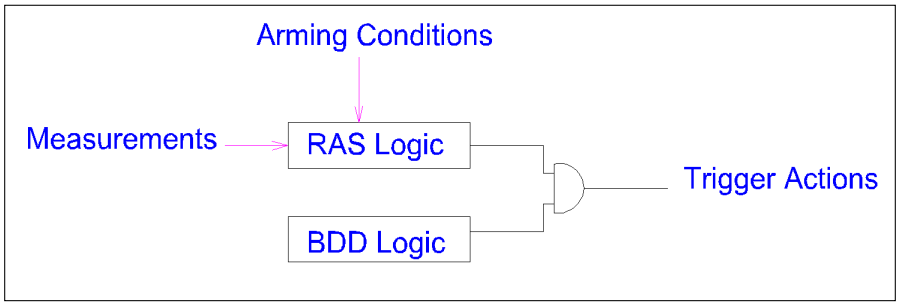

Figure 4.2: RAS structure with bad data detection (BDD) logic

In our approach, the RAS will not be armed unless the FDDF approves the data and validates its accuracy. Therefore, actions taken based on this reliable data are reliable as well. The modified RAS structure is shown in Figure 4.3.

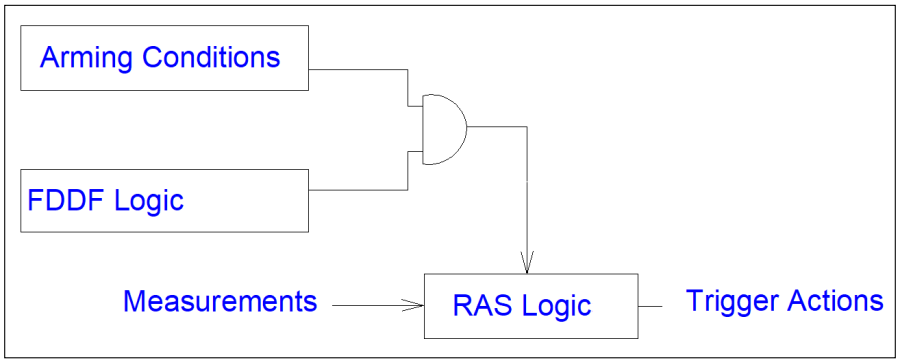

Figure 4.3: The new approach by applying false data and detection logic.

4.4 Proposed False Data Detecting and Fixing Method

This section includes three subjects. First, measurement consistency is discussed, which is fundamental to our method of fixing and detecting false data. Then, a case study with the highlighted zone of focus is presented. The analysis results and extracted logic are included at the end of this section.

A. *Measurement Consistency*

A malicious party might manipulate measurements to bypass the state estimator bad data detection logic or deceive the operators. Here, the measurement consistency check is used to detect and fix the data at the RAS level. To ensure a reliable action taken by RAS, providing reliable data is significantly advantageous. In this method, by using Kirchhoff laws, the measurement from neighborhood buses and lines are used to form a set of logic to verify if the measured value is false or valid. Here, we have simulated our network using Dynamic Security Assessment (DSA) tools [35]. Then, we extracted the logic from our measurements to use it in the process of verifying and fixing false measurements.

B. *Case Study on IEEE 118 Bus Test System*

In this work, the simulation and case study are done on the 118 IEEE bus test system (Figure 4.4). Our focus is on the highlighted part of the network which is expanded in Figure 4.5.

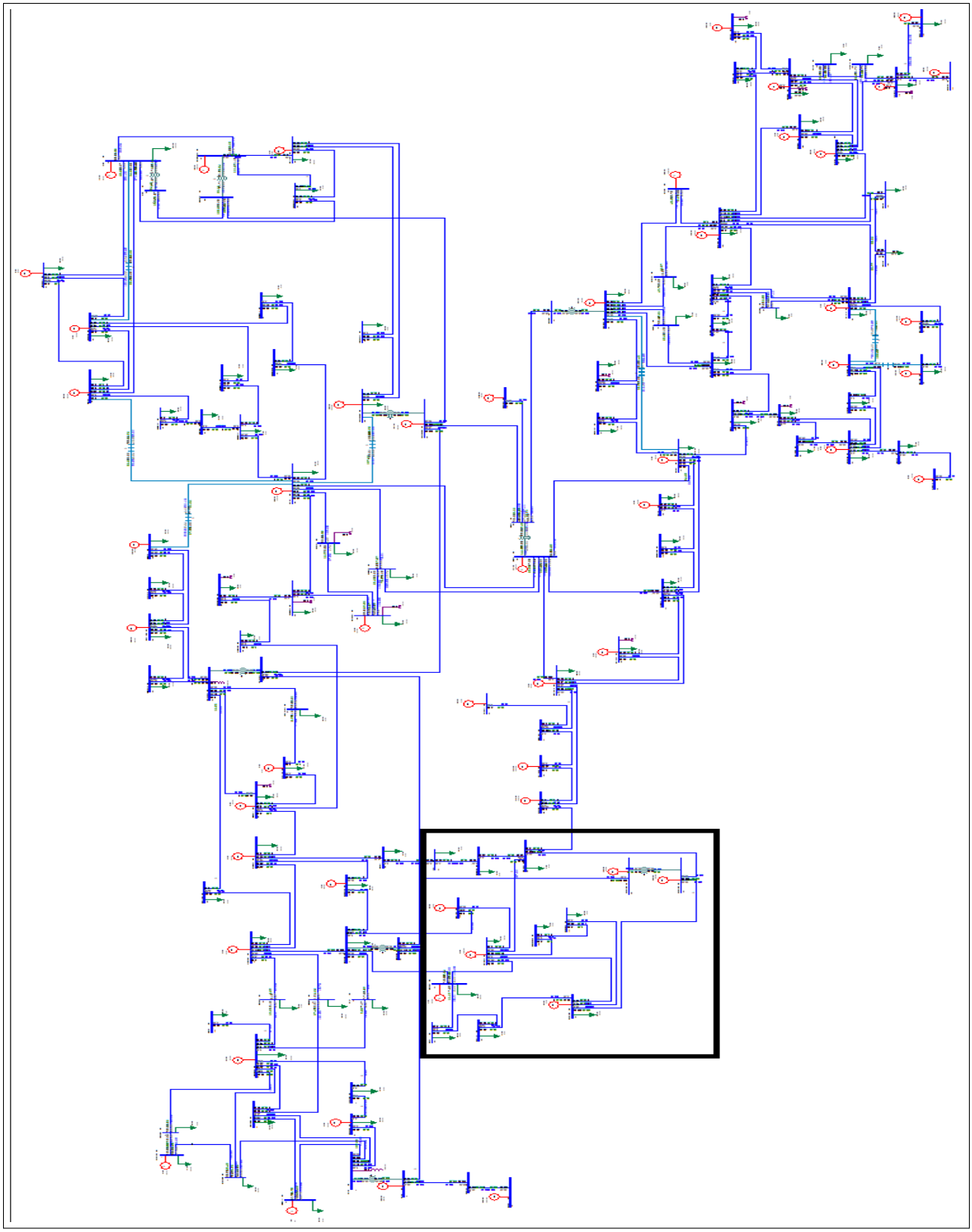

Figure 4.4: Case study IEEE 118 Bus system with the area under focus highlighted.

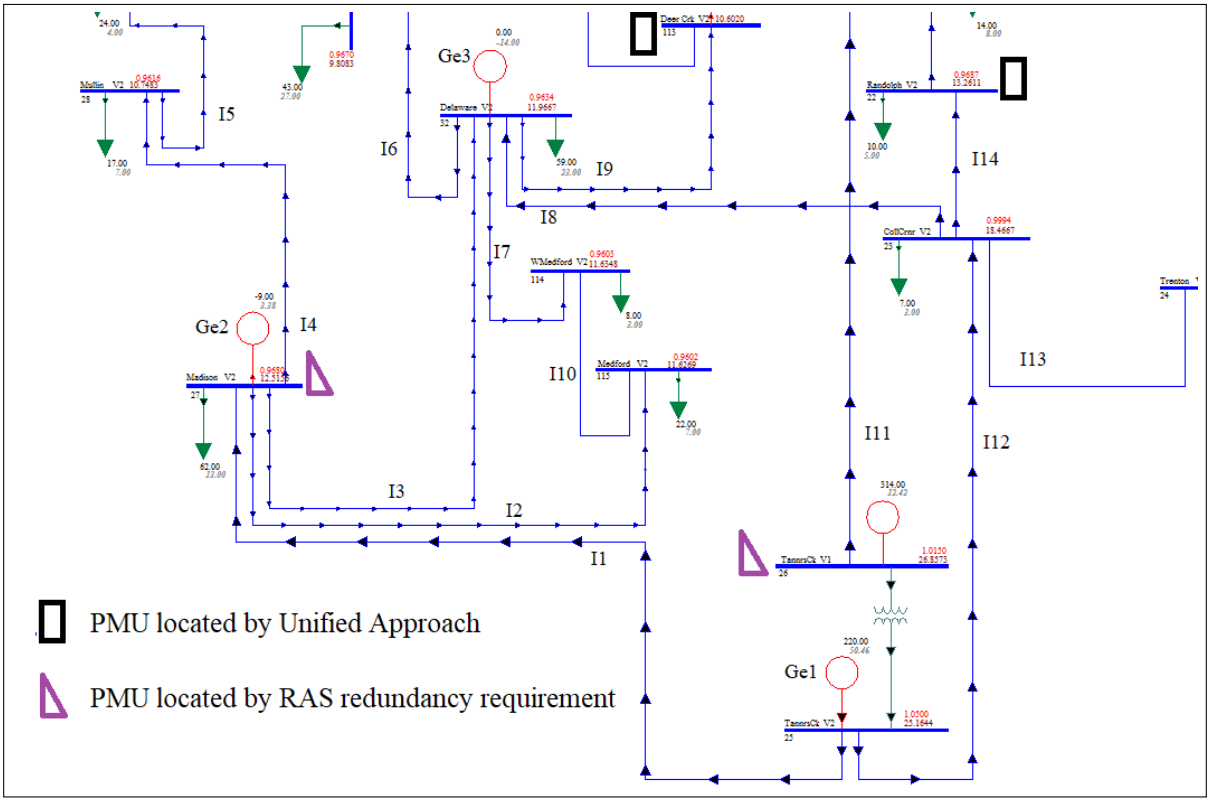

Figure 4.5: The area under focus with 10 buses and 4 PMU locations. Black rectangles indicate PMUs located by Unified Approach, and the purple triangles are located based on the RAS requirement.

C. *Analysis Results*

The DSA tools (including Powerflow and Short circuit Assessment Tool (PSAT) and Voltage Security Assessment Tool (VSAT) packages) are used to apply 43 contingency scenarios on the system and observe the responses and changes on neighborhood buses and lines. The analysis results consist 78 parameters for each of the scenarios. The resultant table includes 3354 (43 x 78) measurements (see Appendix A). Table 4.1 shows a small portion of the analysis results just for explaining purpose. The full results are shown in Appendix A.

As an example, in scenario number 14, Line1 (L1) is assumed to have a failure (originally 144.3 MW, changed to 0 MW) and observe the changes in other measurements on other buses and lines.

D. *FDDF Logic*

FDDF logic is applied to the measurements (in the area under focus) from the simulation

Table 4.1: A Small Part of The Result Matrix Related to 10 scenarios for 20 lines in the Area Under Focus

Parameters				Scenarios										
	From	To	Label	Original	14	15	16	17	18	19	20	21	22	23
Transmission on line active power	25	27	L1	144.31	0	140.37	140.86	136.3	140.32	146.24	143.01	146.09	144.56	111.67
	23	25	L11	-157.58	-238.25	-160.1	-159.77	-159.74	-158.66	-157.05	-154.02	-156.51	-157.43	-106.36
	23	32	L12	97.22	176.26	99.93	99.51	97.31	97.19	97.29	89.91	96.13	97.06	79.53
	32	113	L13	6.42	-22.46	5.05	5.27	9.14	7.79	5.74	14.11	7.04	6.51	-15.84
	22	23	L14	-56.12	-59.29	-56.08	-56.09	-57.33	-56.72	-55.83	-58.01	-56.13	-56.12	-41.07
	21	22	L15	-45.64	-48.75	-45.6	-45.61	-46.83	-46.23	-45.36	-47.49	-45.66	-45.65	-30.85
	26	30	L16	228.15	286.8	229.45	229.31	233.88	231	226.77	233.17	227.49	228.05	313.99
	23	24	L17	-3.91	-5.69	-4.06	-3.98	-3.1	-3.42	-4.21	-2.13	-3.9	-3.91	-21.83
	20	21	L18	-31.44	-34.5	-31.4	-31.41	-32.61	-32.02	-31.16	-33.26	-31.45	-31.44	-16.8
	17	113	L19	-0.22	28.99	1.14	0.92	-2.89	-1.57	0.44	-7.75	-0.84	-0.32	22.13
	27	115	L2	20.72	-17.2	0	27.05	29.89	25.23	18.58	14.66	30.18	22.09	14.04
	17	31	L20	12.38	51.02	12.29	12.27	23.45	17.71	9.93	28.5	12.43	12.39	37.11
	27	32	L3	12.49	-57.88	26.14	0	29.6	20.89	8.51	1.24	6.25	11.58	0
	27	28	L4	33.64	4	37.07	36.62	0	17.07	41.54	49.75	32.05	33.41	22.61
	28	29	L5	16.41	-13.01	19.79	19.35	-17	0	24.16	32.25	14.84	16.18	5.51
	29	31	L6	-7.67	-37.05	-4.32	-4.76	-41.09	-24	0	7.96	-9.22	-7.9	-18.5
	31	32	L7	-31.47	-23.59	-28.22	-28.68	-54.15	-42.58	-26.23	0	-32.98	-31.69	-18.13
	32	114	L8	9.37	47.67	30.16	3.08	0.27	4.89	11.5	15.43	0	8.01	16.05
	114	115	L9	1.36	39.33	22.01	-4.92	-7.73	-3.11	3.48	7.39	-8	0	8.01
Transformer active			L10	85.85	27.22	84.55	84.69	80.12	83	87.23	80.83	86.51	85.85	**0**

results. To make decision based on the measurements, it is crucial to consider the data reliability. Based on the hardware attack or failure possibilities, two different sets of logic are applied.

Without considering hardware attack or failure, the logic is shown in Figure 4.6. Here, we are assuming the measurements as reliable and every single of them can be used to verify the event. Therefore, the malicious party needs to compromised more measurements to inject a false event.

For example, suppose that a false measurement is received showing an abnormal voltage decline on Bus 27. Assume that the malicious purpose is to hide a failure on Generator 1 by compromising the data to show a voltage decline on Bus 27. As it is shown in Figure 4.6, to inject this false data, malicious party must compromise 4 different measurements. In this example, voltage on Bus 27, power of Line 12 and Line 15, and the voltage on Generator 1 bus must be compromised.

By compromising only 3 of these 4 measurements, the attackers will fail. Here, the injected data (B27-Vdrop) is detected and the real failure (Ge1-Vdrop) is extracted. Furthermore, an alarm will be sent to operators to inform them of the compromised data and as well as the real event.

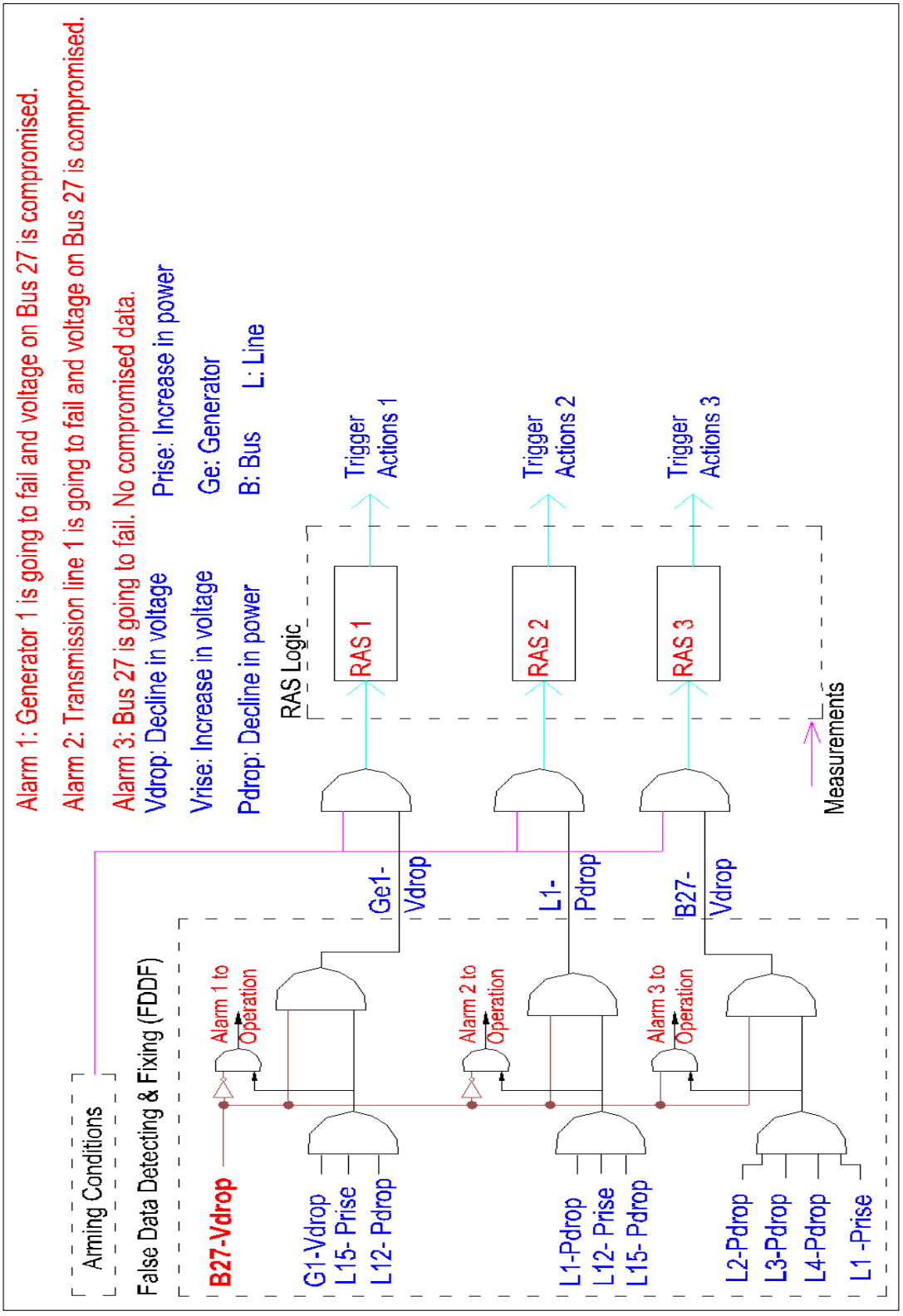

Figure 4.6: Extracted logic for three measurements without considering physical failure or attacks

If there is a hardware failure or attack on measurements, the measurements are less reliable. Thus, a false event can be injected by compromising fewer measurements. In this case, instead of allowing a single measurement to change the decision results, only a set of measurements can impact the decision. Thus, a voting strategy can be used to decrease the impact of the false data. In our example, two out of three measurements must verify the event to allow any decision. Therefore, compromising a single measurement cannot change the decision. In addition, to inject a specific false input, 3 measurements have to be compromised.

The voting strategies for two out of three, three out of four, and four out of five are shown in Figure 4.7, respectively in Part b, Part c, and Part d. Part a is the logic gates related to a simple voting scheme for two of three. Part b, c, and d, show a representative symbol for voting logic for simplicity.

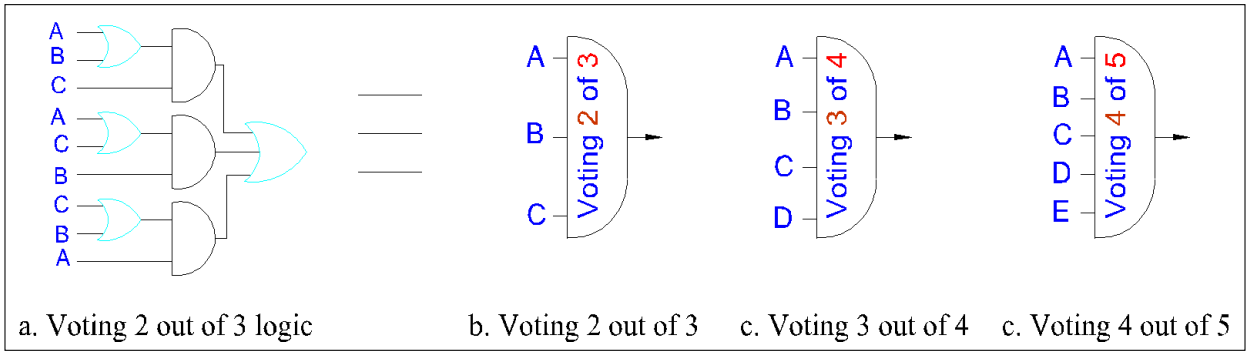

Figure 4.7: Voting logic for two of three, three of four, and four out of five measurements. Part a is the logic gates and Part b, c, and d are representative symbols.

For the same example, suppose that a false measurement is received indicating a decline in voltage on Bus 27. Assume that the malicious purpose is to hide a failure on Generator 1 by compromising the measurements to show a voltage decline on Bus 27. As shown in Figure 4.6, to inject this false data, malicious party must compromise three different measurements. In this example, three of the following must be compromised to inject a false measurement; voltage on Bus 27, power of Line 12 and Line 15, and the voltage on Generator1.

By compromising only two of these four measurements, the attackers will fail. Here,

the injected data (B27-Vdrop) is detected and the real failure (Ge1-Vdrop) is extracted. Furthermore, an alarm will be sent to operators to inform them of the compromised data as well as the real event.

4.5 Conclusion

In this chapter, state estimation and bad data detection are briefly reviewed, and two types of remedial action scheme structures are listed and a new structure is presented. A false data detection and correction method is proposed, and it is tested on the IEEE 118 bus system. The system is simulated using DSA tools and the results are used to extract the required logic for new detection method. The false data is detected and fixed. Furthermore, in case of detecting a false measurement, the operators are informed about the injected data and the real event.

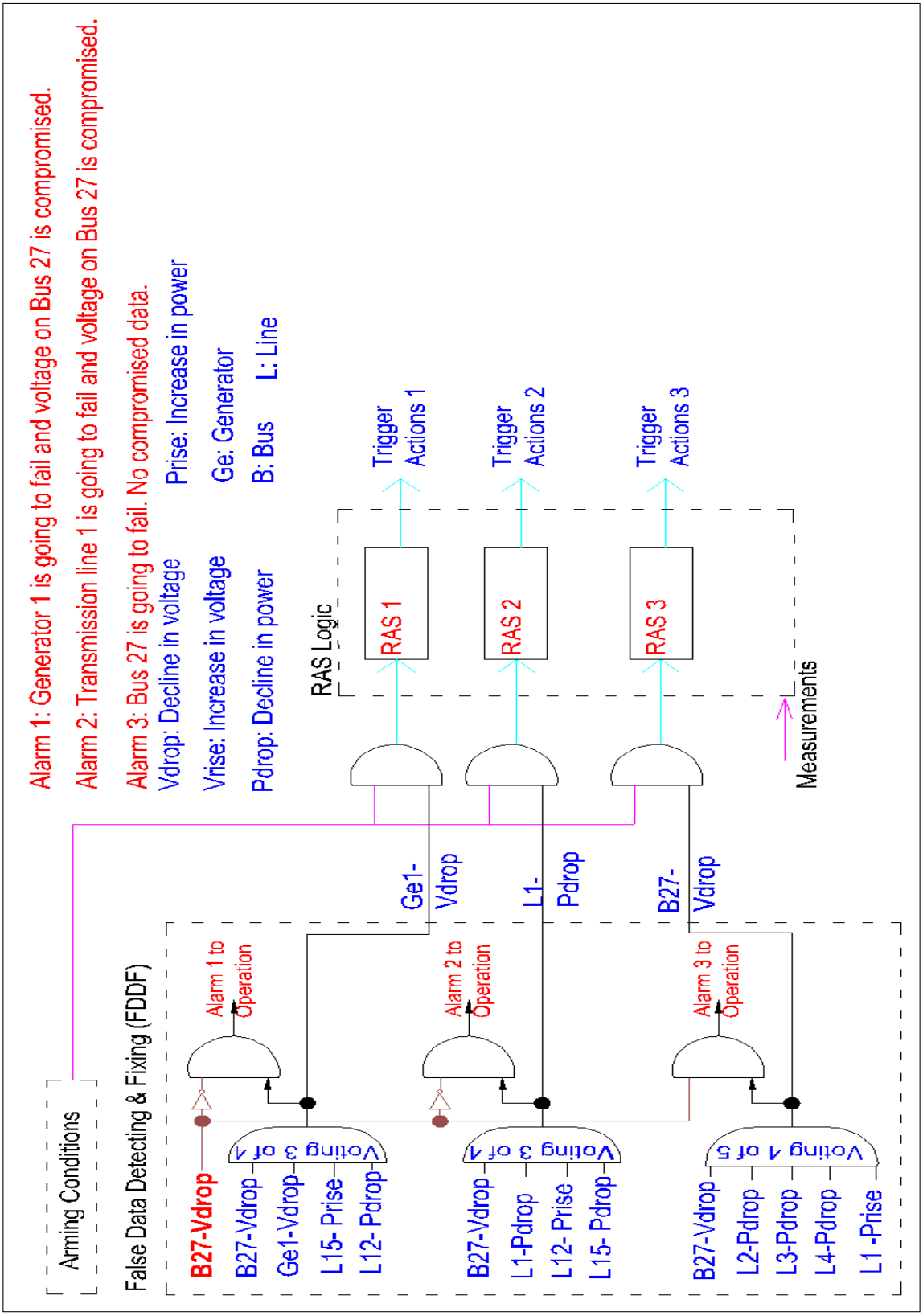

Figure 4.8: Extracted logic for on measurement with considering physical failure or attacks.

Chapter 5: Summary, Conclusions, and Future work

5.1 Summary

The risk of cascading outages and cascading failures in power grids can arise due to vulnerable transmission lines and lack of proper remediation techniques after recognizing the failures. Therefore, under fault conditions, other disturbances, and cyber or physical attacks, the resiliency of the power grid could be severely jeopardized.

A commonly used solution to improve operational security is to recognize the critical lines or generators and use remedial action schemes to reduce vulnerability and maintain the system operational security.

The RAS takes corrective actions based on the input data. As a result, these data need to be very reliable. One way to insure the data is not false or compromised is to detect bad data and fix it.

In our work, we used power flow–based method and fault chain theory to determine the critical lines. Furthermore, a new vulnerability index is presented to identify the most critical lines more efficiently. We consider applying RAS on these critical lines and measure the improvement in vulnerability after applying the RAS. The effectiveness of the new index and the impact of the applied RAS is illustrated on the IEEE 14 bus and IEEE 9 bus systems. Moreover, the probability of large–scale blackout before and after applying RAS is calculated and the improvement is showed. To verify the measurement to RAS and insure its right corrective action, a new false data detection and fixing (FDDF) method is proposed. The method is examined by IEEE 118 bus system and the results are demonstrated.

5.2 Conclusions

In this thesis, the accomplishments can be outlined as the followings:

- Assessed the system vulnerability before and after applying RAS
- Demonstrated resiliency improvement (40%) by considering a simple RAS

- Proposed a way to assess vulnerability indices to better recognition of critical lines
- Analyzed effects of applying RAS on these lines
- Illustrated resulting decline (27.5%) in the probability of a failure cascading to a black-out
- Analyzed the IEEE 118 bus system for 43 contingency scenarios and for 87 parameters
- Offered FDDF, which is a new method of detecting and fixing false data

5.3 Future work

Some topics meriting further study are listed below, and a short description is provided for each suggestion.

A. *Compare additional vulnerability analysis methods and try to rank and categorize the methods.*

There are several assessment methods available to assess the power system vulnerability. For a given power system, each approach has its own criticality ranking and determines a specific set of components as critical. This is confusing and causes researchers or power system planners to mistake the criticality ranking of system components. Therefore, study of all available common vulnerability assessment approaches and comparing them would be useful in determining the best assessment method for each application. Having a list of methods with their limits and merits can a valuable guidance to select the proper method of analysis.

B. *Integrate the fault chain theory with the false data detection.*

The fault chain theory determines the next line with the highest probability to fail. Thus, the measurement of the next line to fail can be used to verify if the previous line is actually failed or the data was compromised. This is another level of detection logic that can be

integrated with the bad data detection logic to further validate the results of the detection methods.

C. *Define Proper RAS schemes related to the extracted fixed data from FDDF.*

A new detecting and fixing method was proposed to provide more reliable data as RAS input. The RAS related to each scenario can be defined and the number of RAS schemes can be optimized by finding the common action requirements in each scenario.

D. *Evaluate the FDDF by applying random contingencies and observe the results.*

To evaluate the False Data Detecting and Fixing (FDDF) method, random contingencies can be applied to the logic and observe the final output of the FDDF. Then, compare the result and the applied contingency to verify if they are the same. If they are not, the FDDF is not properly built and the logic must be modified.

E. *Extract the FDDF logic for the whole IEEE 118 bus system.*

The case study in Chapter 4 was on the IEEE 118 bus system. We focused on an area with 10 buses and recorded the results for this area. The extracted logic is also related to the focus area. The same method can be applied to the whole 118 bus system and try to optimize the detecting and fixing logic and minimize the RAS actions needed to secure the system and reduce the cost and complexity.

Bibliography

[1] I. Dobson, B. A. Carreras, and D. E. Newman, "A loading-dependent model of probabilistic cascading failure," *Probability in the Engineering and Informational Sciences*, vol. 19, no. 1, pp. 15–32, 2005.

[2] P. Khaledian, B. K. Johnson, and S. Hemati, "Power grid resiliency improvement through remedial action schemes," in *Industrial Electronics Conference*, pp. 1–6, IEEE, 2018.

[3] L. Zongxiang, M. Zhongwei, and Z. Shuangxi, "Cascading failure analysis of bulk power system using small-world network model," in *Probabilistic Methods Applied to Power Systems. 2004 International Conference on*, pp. 635–640, IEEE, 2004.

[4] I. Dobson and D. E. Newman, "Cascading blackout overall structure and some implications for sampling and mitigation," *International Journal of Electrical Power & Energy Systems*, vol. 86, pp. 29–32, 2017.

[5] K. Eshghi, B. Johnson, and C. Rieger, "Metrics required for power system resilient operations and protection," in *Resilience Week (RWS). 2016*, pp. 200–203, IEEE, 2016.

[6] P. Khaledian, B. K. Johnson, and S. Hemati, "Power grid security improvement by remedial action schemes using vulnerability assessment based on fault chains and power flow," in *Probabilistic Methods Applied to Power Systems, IEEE International Conference*, pp. 1–6, IEEE, 2018.

[7] R. Ramanathan, B. Tuck, and J. O'Brien, "BPA's experience of implementing remedial action schemes in power flow for operation studies," in *Power and Energy Society General Meeting (PES), 2013 IEEE*, pp. 1–5, IEEE, 2013.

[8] "Special protection systems (SPS) / remedial action schemes (RAS): Assessment of definition, regional practices, and application of related standards," *North American Electric Reliability Corporation (NERC)*, 2013.

[9] B. Heap, "Remedial action schemes (RAS)," in *Hands-On Relay School*, Washington State University, 2014.

[10] M. Vaughn, R. Schloss, S. Manson, S. Raghupathula, and T. Maier, "Idaho power RAS: A dynamic remedial action case study," in *Proceedings of the 64th Annual Georgia Tech Protective Relaying Conference, Atlanta, GA*, 2010.

[11] "Remedial action scheme design guide," *Western Electricity Coordinating Council (WECC)*, 2006.

[12] "Remedial action scheme," *North American Electric Reliability Corporation (NERC)*, 2014.

[13] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, and P. Zhang, "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Transactions on Power Systems*, vol. 27, no. 2, p. 631, 2012.

[14] S. Eftekharnejad, "Selection of multiple credible contingencies for real time contingency analysis," in *Power & Energy Society General Meeting, 2015 IEEE*, pp. 1–5, IEEE, 2015.

[15] K. Morison, L. Wang, and P. Kundur, "Power system security assessment," *IEEE Power and Energy Magazine*, vol. 2, no. 5, pp. 30–39, 2004.

[16] A. Atputharajah and T. K. Saha, "Power system blackouts-literature review," in *Industrial and Information Systems (ICIIS), 2009 International Conference on*, pp. 460–465, IEEE, 2009.

[17] A. Dwivedi and X. Yu, "A maximum-flow-based complex network approach for power system vulnerability analysis," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 81–88, 2013.

[18] Z. Wang, G. Chen, D. J. Hill, and Z. Y. Dong, "A power flow based model for the analysis of vulnerability in power networks," *Physica A: Statistical Mechanics and its Applications*, vol. 460, pp. 105–115, 2016.

[19] M. Vaiman, P. Hines, J. Jiang, S. Norris, M. Papic, A. Pitto, Y. Wang, and G. Zweigle, "Mitigation and prevention of cascading outages: Methodologies and practical applications," in *Power and Energy Society General Meeting (PES), 2013 IEEE*, pp. 1–5, IEEE, 2013.

[20] J. M. Arroyo and F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem," *IEEE transactions on Power Systems*, vol. 20, no. 2, pp. 789–797, 2005.

[21] A. M. Rushdi and O. M. Ba-Rukab, "Fault-tree modelling of computer system security," *International Journal of Computer Mathematics*, vol. 82, no. 7, pp. 805–819, 2005.

[22] A. Wang, Y. Luo, G. Tu, and P. Liu, "Vulnerability assessment scheme for power system transmission networks based on the fault chain theory," *IEEE Transactions on power systems*, vol. 26, no. 1, pp. 442–450, 2011.

[23] J. Yang and K. Jiang, "The sensitive line identification in resilient power system based on fault chain model," *International Journal of Electrical Power & Energy Systems*, vol. 92, pp. 212–220, 2017.

[24] J. Lu, Y. Chen, and Y. Zhu, "Identification of cascading failures based on overload character of transmission lines," in *Electric Utility Deregulation and Restructuring and Power Technologies, 2008. DRPT 2008. Third International Conference on*, pp. 1030–1033, IEEE, 2008.

[25] B.-H. Zhang, F. Yao, D.-C. Zhou, L.-Y. Wang, and B.-G. Zou, "Study on security protection of transmission section and its key technologies," *Proceedings of the CSEE*, vol. 26, no. 21, pp. 1–7, 2006.

[26] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[27] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 741–749, 2011.

[28] Q. Li, R. Negi, and M. D. Ilić, "Phasor measurement units placement for power system state estimation: A greedy approach," in *Power and Energy Society General Meeting, 2011 IEEE*, pp. 1–8, IEEE, 2011.

[29] D. Van Hertem, J. Verboomen, K. Purchala, R. Belmans, and W. Kling, "Usefulness of DC power flow for active power flow analysis with flow controlling devices," *8th IEE International Conference on AC and DC Power Transmission (ACDC)*, pp. 58–62, 2006.

[30] Y. Chakhchoukh and H. Ishii, "Coordinated cyber-attacks on the measurement function in hybrid state estimation," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2487–2497, 2015.

[31] T. JiWei, W. BuHong, S. FuTe, and L. Shuaiqi, "Stealthy false data injection attacks using matrix recovery and independent component analysis in smart grid," in *IOP Conference Series: Materials Science and Engineering*, vol. 199, p. 012034, IOP Publishing, 2017.

[32] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[33] N. H. Abbasy and H. M. Ismail, "A unified approach for the optimal PMU location for power system state estimation," *IEEE Transactions on power systems*, vol. 24, no. 2, pp. 806–813, 2009.

[34] M. S. Shahriar, I. O. Habiballah, and H. Hussein, "Optimization of phasor measurement unit (pmu) placement in supervisory control and data acquisition (scada)-based power system for better state-estimation performance," *Energies*, vol. 11, no. 3, p. 570, 2018.

[35] PowerTech Lab Inc., "Dynamic Security Assessment (DSA) tools," 2017. Available: http://www.dsatools.com/.

Appendix A: The full results from DSA tools for IEEE 118 bus system

The results are specific to the area under the focus of this project. It includes 43 scenarios for 78 parameters.

Parameters						Scenarios												
Parameters					Orignal	Scenarios												
	No.	From	To	Label		1	2	3	4	5	6	7	8	9	10	11	12	13
Generator active	1			Ge1	220	0	220	220	220	220	220	330	220	220	220	220	220	220
	2			Ge2	-9	-9	0	-9	-9	-9	-9	-9	-13.5	-9	-9	-9	-9	-9
	3			Ge3	7	7	7	0	7	7	7	7	7	10.5	7	7	7	7
	4			Ge4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	5			Ge5	314	314	314	314	314	0	314	314	314	314	314	417	314	314
	6			Ge6	-6	-6	-6	-6	-6	-6	0	-6	-6	-6	-6	-6	-9	-6
Generator reactive	7			Ge1	50.46	0	50.46	50.46	50.46	50.46	50.46	49.08	50.62	50.38	50.46	51.35	50.52	72.06
	8			Ge2	8.29	8.29	0	8.29	8.29	8.29	8.29	7.59	4.82	3.15	8.29	5.9	3.45	-2.95
	9			Ge3	33.23	33.23	33.23	0	33.23	33.23	33.23	33.11	32.47	31.27	33.23	32.82	32.44	32.79
	10			Ge4	-11.9	-11.9	-11.9	-11.9	0	-11.9	-11.9	-14	-14	-14	-11.9	-14	-14	-14
	11			Ge5	52.61	52.61	52.61	52.61	52.61	0	52.61	18.86	12.36	12.43	52.61	23.65	12.49	8.38
	12			Ge6	7.02	7.02	7.02	7.02	7.02	7.02	0	9.92	7.81	7.91	7.02	9.62	8.73	8.65
transmission line active power	13	25	27	L1	144.31	108	141.15	145.7	144.2	108.36	144	162.24	145.87	143.64	144.31	156.36	144.5	111.67
	14	23	25	L11	-157.58	-70	-158.6	-157	-157.8	-55.86	-158	-200.21	-157.1	-157.81	-157.58	-190.34	-157.29	-106.36
	15	23	32	L12	97.22	96.07	94.67	99.2	97.42	104.26	96.28	97.64	98.5	96.22	97.22	95.06	97.7	79.53
	16	32	113	L13	6.42	-9.65	8.03	5.67	6.5	-5.77	5.44	14.13	5.61	6.87	6.42	10.48	6.91	-15.84
	17	22	23	L14	-56.12	-45.9	-56.43	-56.1	-56.11	-48.87	-55.9	-60.92	-55.97	-56.15	-56.12	-58.52	-56.23	-41.07
	18	21	22	L15	-45.64	-35.7	-45.94	-45.6	-45.64	-38.53	-45.5	-50.34	-45.5	-45.68	-45.64	-47.99	-45.75	-30.85
	19	26	30	L16	228.15	135.1	230.27	227.3	228.1	54.86	227.9	275.24	227.09	228.57	228.15	284.61	228.26	313.99
	20	23	24	L17	-3.91	-79.8	-0.69	-6.35	-3.92	-105.15	-2.17	33.28	-5.53	-2.71	-3.91	28.5	-4.79	-21.83
	21	20	21	L18	-31.44	-21.6	-31.73	-31.4	-31.44	-24.41	-31.2	-36.07	-31.29	-31.47	-31.44	-33.75	-31.54	-16.8
	22	17	113	L19	-0.22	15.82	-1.82	0.61	-0.31	11.9	-5.24	-7.79	0.58	-0.66	-0.22	-4.22	2.27	22.13
	23	27	115	L2	20.72	12.4	22.36	20.69	20.78	12.08	20.64	24.76	19.91	20.73	20.72	23.55	20.76	14.04
	24	17	31	L20	12.38	30.9	10.39	15.65	12.31	26.86	12.59	3.65	13.39	10.84	12.38	7.62	12.26	37.11
	25	27	32	L3	12.49	-2.97	15.52	12.46	12.32	-3.55	12.36	20.03	10.97	12.5	12.49	17.77	12.56	0
	26	27	28	L4	33.64	23.85	35.05	34.71	33.59	24.98	33.54	38.39	32.93	32.99	33.64	36.51	33.7	22.61
	27	28	29	L5	16.41	6.73	17.79	17.46	16.36	7.86	16.31	21.08	15.71	15.77	16.41	19.24	16.46	5.51
	28	29	31	L6	-7.67	-17.3	-6.3	-6.64	-7.72	-16.16	-7.77	-3.04	-8.36	-8.3	-7.67	-4.87	-7.61	-18.5
	29	31	32	L7	-31.47	-22.9	-32.08	-34.4	-31.66	-25.73	-31.4	-35.53	-31.16	-30.14	-31.47	-33.39	-31.54	-18.13
	30	32	114	L8	9.37	17.69	7.75	9.41	9.31	18	9.45	5.36	10.19	9.36	9.37	6.56	9.34	16.05
	31	114	115	L9	1.36	9.64	-0.26	1.39	1.3	9.95	1.44	-2.64	2.17	1.35	1.36	-1.45	1.32	8.01
transformer active	32			L10	85.85	178.9	83.73	86.76	85.93	-54.86	86.15	38.74	86.73	85.43	85.85	132.21	85.74	0
transmission line reactive power	33	25	27	L1	30.08	20.53	30.16	30.12	30.08	30.12	30.07	30.85	30.12	30.06	30.08	30.54	30.08	30.03
	34	23	25	L11	-27.9	-38.5	-27.55	-28.2	-27.02	-56.57	-27.7	-14.81	-28.09	-27.79	-27.9	-17.71	-28.02	-41.02
	35	23	32	L12	3.94	0.94	4.41	3.86	1.53	2.69	4.28	3.15	3.75	4.09	3.94	3.81	3.86	7.84
	36	32	113	L13	-18.26	-13.7	-18.73	-18.2	-16.69	-14.86	-17	-20.46	-18.05	-18.37	-18.26	-19.41	-18.4	-11.16
	37	22	23	L14	-5.97	-6.93	-5.92	-5.95	-6.11	-7.16	-6	-4.96	-5.99	-5.97	-5.97	-5.44	-5.95	-9.01
	38	21	22	L15	-1.05	-2.86	-0.97	-1.03	-1.19	-2.88	-1.1	0.46	-1.08	-1.04	-1.05	-0.28	-1.02	-5.3
	39	26	30	L16	-9.02	-14.9	-8.82	-8.54	-9.04	-15.05	-8.82	-1.58	-9.12	-9.01	-9.02	0.45	-8.96	8.38
	40	23	24	L17	13.54	27.88	12.7	13.95	14.94	43.57	13.03	1.24	13.94	13.27	13.54	3.5	13.74	22.23
	41	20	21	L18	5.93	3.61	6.02	5.95	5.78	3.71	5.87	7.76	5.89	5.94	5.93	6.86	5.97	0.97
	42	17	113	L19	5.33	1.49	5.67	1.48	5.35	1.03	11.88	6.01	5.14	5.41	5.33	4.96	4.63	-2.34
	43	27	115	L2	4.79	6.78	4.33	5.07	2.44	6.82	4.97	4.2	4.98	4.76	4.79	4.3	4.79	5.71
	44	17	31	L20	11.96	7.13	12.51	21.57	11.98	7.85	11.37	14.23	11.68	12.4	11.96	13.04	12.01	5.21
	45	27	32	L3	1.26	6.42	0.11	1.78	-3.18	6.55	1.6	-0.53	1.75	1.2	1.26	-0.15	1.26	4.12
	46	27	28	L4	-0.73	1.21	-1.11	7.13	-0.73	0.97	-0.72	-1.59	-0.6	-0.62	-0.73	-1.26	-0.75	1.46
	47	28	29	L5	-6.76	-4.31	-7.22	0.97	-6.74	-4.59	-6.73	-7.92	-6.58	-6.6	-6.76	-7.46	-6.77	-3.99
	48	29	31	L6	-8.86	-6.16	-9.38	-1.2	-8.84	-6.46	-8.83	-10.22	-8.66	-8.67	-8.86	-9.68	-8.88	-5.82
	49	31	32	L7	12.55	10.06	12.81	-3.4	9.13	10.96	12.75	14.26	12.48	12.05	12.55	13.31	12.59	7.4
	50	32	114	L8	2.04	0.01	2.54	1.77	4.38	-0.03	1.87	2.74	1.84	2.07	2.04	2.61	2.04	1.06
	51	114	115	L9	0.49	-1.69	1	0.21	2.82	-1.73	0.31	1.22	0.27	0.51	0.49	1.08	0.48	-0.6

Parameters					Scenarios												
Parameters				Orignal	Scenarios												
	No.	From	To	Label	1	2	3	4	5	6	7	8	9	10	11	12	13
transformer reactive	52			L10	21.45	67.5	21.39	21.48	21.45	15.05	21.46	20.44	21.48	21.44	21.45	23.19	21.45	0
voltage magnitude	53			21	0.9578	0.958	0.9577	0.958	0.958	0.9589	0.958	0.9559	0.9578	0.9578	0.9578	0.9568	0.9577	0.9616
	54			22	0.9687	0.968	0.9687	0.969	0.969	0.9698	0.969	0.9667	0.9688	0.9687	0.9687	0.9677	0.9687	0.973
	55			23	0.9994	0.995	0.9994	0.999	1	0.9988	0.999	0.9982	0.9993	0.9994	0.9994	0.9987	0.9993	1.0011
	56			25	1.05	1.035	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05
	57			26	1.015	1.015	1.015	1.015	1.015	1.013	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015
	58			27	0.968	0.968	0.9677	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968
	59			28	0.9616	0.962	0.9614	0.954	0.962	0.9616	0.962	0.9615	0.9616	0.9616	0.9616	0.9615	0.9616	0.9615
	60			29	0.9632	0.963	0.9632	0.948	0.963	0.9631	0.963	0.9633	0.9632	0.9632	0.9632	0.9633	0.9632	0.963
	61			31	0.967	0.967	0.967	0.949	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967
	62			32	0.9634	0.963	0.9634	0.963	0.967	0.963	0.963	0.9631	0.9634	0.9634	0.9634	0.9633	0.9634	0.9641
	63			113	0.993	0.993	0.993	0.993	0.993	0.993	0.991	0.993	0.993	0.993	0.993	0.993	0.993	0.993
	64			114	0.9603	0.96	0.9602	0.96	0.962	0.9601	0.96	0.9601	0.9603	0.9604	0.9603	0.9603	0.9603	0.9607
	65			115	0.9602	0.96	0.9601	0.96	0.962	0.9601	0.96	0.9601	0.9602	0.9602	0.9602	0.9602	0.9602	0.9606
voltage angle	66			21	10.5247	-3.71	11.13	10.03	10.53	-9.8183	10.91	17.21	10.221	10.764	10.5247	16.6624	10.3288	9.3604
	67			22	13.2609	-1.6	13.885	12.76	13.26	-7.5376	13.64	20.259	12.948	13.5023	13.2609	19.5553	13.0722	11.1401
	68			23	18.4665	2.649	19.121	17.97	18.45	-3.0434	18.82	25.958	18.139	18.711	18.4665	25.0078	18.2889	14.8406
	69			25	25.1642	5.466	25.865	24.65	25.16	-1.047	25.55	34.658	24.813	25.4198	25.1642	33.2416	24.9732	19.1707
	70			26	26.8571	9.047	27.516	26.36	26.86	-2.1307	27.25	35.422	26.527	27.1043	26.8571	35.8529	26.6639	33.3933
	71			27	12.5154	-4.1	13.511	11.87	12.52	-10.33	12.93	20.329	12.018	12.8341	12.5154	19.4638	12.3067	9.5775
	72			28	10.7481	-5.33	11.665	10.12	10.76	-11.622	11.17	18.301	10.289	11.102	10.7481	17.539	10.5362	8.4166
	73			29	9.7081	-5.77	10.537	9.113	9.723	-12.131	10.13	16.971	9.292	10.1014	9.7081	16.3234	9.4926	8.0528
	74			31	9.808	-5.46	10.605	9.247	9.824	-11.843	10.24	16.968	9.4072	10.2153	9.808	16.3608	9.5912	8.3934
	75			32	11.9665	-3.86	12.806	11.33	11.92	-10.061	12.39	19.405	11.546	12.2837	11.9665	18.6499	11.7544	9.6483
	76			113	10.6018	-3.1	11.228	10.05	10.61	-9.8185	11.19	17.02	10.287	10.861	10.6018	16.7485	10.3247	11.2514
	77			114	11.6346	-4.52	12.54	10.99	11.61	-10.737	12.06	19.231	11.182	11.9525	11.6346	18.4295	11.4239	9.056
	78			115	11.6267	-4.59	12.543	10.98	11.61	-10.804	12.05	19.25	11.168	11.9447	11.6267	18.4406	11.4163	9.0037

Parameters						Scenarios									
Parameters					Orignal	14	15	16	17	18	19	20	21	22	23
	No.	From	To	Label											
Generator active	1			Ge1	220	220	220	220	220	220	220	220	220	220	220
	2			Ge2	-9	-9	-9	-9	-9	-9	-9	-9	-9	-9	-9
	3			Ge3	7	7	7	7	7	7	7	7	7	7	7
	4			Ge4	0	0	0	0	0	0	0	0	0	0	0
	5			Ge5	314	314	314	314	314	314	314	314	314	314	314
	6			Ge6	-6	-6	-6	-6	-6	-6	-6	-6	-6	-6	-6
Generator reactive	7			Ge1	50.46	22.04	50.36	50.39	50.18	50.29	50.57	50.55	50.19	50.41	72.06
	8			Ge2	8.29	57.6	-7	-0.76	-5.15	4.72	15.65	5.58	8.26	4.24	-2.95
	9			Ge3	33.23	36.18	32.66	32.68	45.33	33.41	21.73	29.96	31.04	32.16	32.79
	10			Ge4	-11.9	6.18	-1.71	-8.75	-14	-14	-14	-11.2	-14	-14	-14
	11			Ge5	52.61	22.89	12.6	12.58	13.24	12.82	12.24	13.16	12.34	12.41	8.38
	12			Ge6	7.02	8.57	8.01	8.02	8.02	7.92	7.86	8.34	7.15	7.73	8.65
transmission line active power	13	25	27	L1	144.31	0	140.37	140.86	136.3	140.32	146.24	143.01	146.09	144.56	111.67
	14	23	25	L11	-157.58	-238.25	-160.1	-159.77	-159.74	-158.66	-157.05	-154.02	-156.51	-157.43	-106.36
	15	23	32	L12	97.22	176.26	99.93	99.51	97.31	97.19	97.29	89.91	96.13	97.06	79.53
	16	32	113	L13	6.42	-22.46	5.05	5.27	9.14	7.79	5.74	14.11	7.04	6.51	-15.84
	17	22	23	L14	-56.12	-59.29	-56.08	-56.09	-57.33	-56.72	-55.83	-58.01	-56.13	-56.12	-41.07
	18	21	22	L15	-45.64	-48.75	-45.6	-45.61	-46.83	-46.23	-45.36	-47.49	-45.66	-45.65	-30.85
	19	26	30	L16	228.15	286.8	229.45	229.31	233.88	231	226.77	233.17	227.49	228.05	313.99
	20	23	24	L17	-3.91	-5.69	-4.06	-3.98	-3.1	-3.42	-4.21	-2.13	-3.9	-3.91	-21.83
	21	20	21	L18	-31.44	-34.5	-31.4	-31.41	-32.61	-32.02	-31.16	-33.26	-31.45	-31.44	-16.8
	22	17	113	L19	-0.22	28.99	1.14	0.92	-2.89	-1.57	0.44	-7.75	-0.84	-0.32	22.13
	23	27	115	L2	20.72	-17.2	0	27.05	29.89	25.23	18.58	14.66	30.18	22.09	14.04
	24	17	31	L20	12.38	51.02	12.29	12.27	23.45	17.71	9.93	28.5	12.43	12.39	37.11
	25	27	32	L3	12.49	-57.88	26.14	0	29.6	20.89	8.51	1.24	6.25	11.58	0
	26	27	28	L4	33.64	4	37.07	36.62	0	17.07	41.54	49.75	32.05	33.41	22.61
	27	28	29	L5	16.41	-13.01	19.79	19.35	-17	0	24.16	32.25	14.84	16.18	5.51
	28	29	31	L6	-7.67	-37.05	-4.32	-4.76	-41.09	-24	0	7.96	-9.22	-7.9	-18.5
	29	31	32	L7	-31.47	-23.59	-28.22	-28.68	-54.15	-42.58	-26.23	0	-32.98	-31.69	-18.13
	30	32	114	L8	9.37	47.67	30.16	3.08	0.27	4.89	11.5	15.43	0	8.01	16.05
	31	114	115	L9	1.36	39.33	22.01	-4.92	-7.73	-3.11	3.48	7.39	-8	0	8.01
transformer active	32			L10	85.85	27.22	84.55	84.69	80.12	83	87.23	80.83	86.51	85.85	0
transmission line reactive power	33	25	27	L1	30.08	0	29.98	29.99	29.91	29.98	30.14	30.04	30.13	30.09	30.03
	34	23	25	L11	-27.9	-5.14	-27.31	-27.4	-27.41	-27.64	-28.03	-29.01	-27.84	-27.87	-41.02
	35	23	32	L12	3.94	-8.2	3.71	3.79	4.01	3.96	3.93	5.47	3.13	3.78	7.84
	36	32	113	L13	-18.26	-9.39	-18.06	-18.12	-19.13	-18.68	-18.06	-20.5	-17.75	-18.16	-11.16
	37	22	23	L14	-5.97	-4.45	-5.94	-5.94	-5.74	-5.86	-6.02	-5.67	-6.04	-5.98	-9.01
	38	21	22	L15	-1.05	0.82	-1.02	-1.02	-0.7	-0.88	-1.13	-0.56	-1.12	-1.06	-5.3
	39	26	30	L16	-9.02	2.58	-8.81	-8.84	-8.04	-8.55	-9.25	-8.14	-9.13	-9.04	8.38
	40	23	24	L17	13.54	3.75	13.21	13.22	12.97	13.25	13.68	13.08	14.23	13.67	22.23
	41	20	21	L18	5.93	8.04	5.96	5.96	6.36	6.14	5.83	6.54	5.86	5.92	0.97
	42	17	113	L19	5.33	-3.39	4.93	4.99	6.2	5.77	5.1	7.64	5.51	5.36	-2.34
	43	27	115	L2	4.79	13.88	0	3.83	3.22	3.97	5.21	6.31	8.73	5.61	5.71
	44	17	31	L20	11.96	2.2	11.99	11.99	8.89	10.45	12.67	7.55	11.94	11.96	5.21
	45	27	32	L3	1.26	24.81	-2.14	0	-3.26	-1.04	2.4	5.13	1.18	1.16	4.12
	46	27	28	L4	-0.73	5.89	-1.36	-1.28	0	5.32	9.2	-3.41	-0.44	-0.69	1.46
	47	28	29	L5	-6.76	0.85	-7.6	-7.49	-6.98	0	2.51	-10.66	-6.36	-6.7	-3.99
	48	29	31	L6	-8.86	-1.13	-9.84	-9.71	-9.17	-3.97	0	-13.61	-8.41	-8.79	-5.82
	49	31	32	L7	12.55	10.28	11.84	11.99	20.97	16.55	10.74	0	11.58	12.34	7.4
	50	32	114	L8	2.04	-5.37	8.98	3.19	3.93	2.98	1.59	0.49	0	1.53	1.06
	51	114	115	L9	0.49	-8.38	6.81	1.68	2.42	1.46	0.01	-1.17	-3	0	-0.6

Parameters					Orignal	Scenarios									
Parameters						14	15	16	17	18	19	20	21	22	23
	No.	From	To	Label											
transformer reactive	52			L10	21.45	20.31	21.41	21.42	21.29	21.37	21.49	21.31	21.47	21.45	0
voltage magnitude	53			21	0.9578	0.9543	0.9577	0.9577	0.9573	0.9576	0.9578	0.9573	0.9579	0.9578	0.9616
	54			22	0.9687	0.9643	0.9686	0.9686	0.9683	0.9685	0.9688	0.9683	0.969	0.9688	0.973
	55			23	0.9994	0.9943	0.9992	0.9992	0.9992	0.9993	0.9994	0.9994	0.9997	0.9994	1.0011
	56			25	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05
	57			26	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015
	58			27	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968
	59			28	0.9616	0.9611	0.9615	0.9615	0.949	0.9591	0.9514	0.9613	0.9616	0.9616	0.9615
	60			29	0.9632	0.9625	0.9633	0.9633	0.9593	0.963	0.9421	0.9633	0.9632	0.9632	0.963
	61			31	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967
	62			32	0.9634	0.963	0.963	0.963	0.9631	0.9633	0.9634	0.963	0.9649	0.9637	0.9641
	63			113	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.993
	64			114	0.9603	0.9597	0.9528	0.9601	0.9601	0.9603	0.9603	0.9601	0.9552	0.9611	0.9607
	65			115	0.9602	0.9597	0.9515	0.96	0.96	0.9602	0.9603	0.96	0.9557	0.9594	0.9606
voltage angle	66			21	10.5247	9.6241	10.5014	10.516	10.4875	10.525	10.5122	10.5734	10.5255	10.5253	9.3604
	67			22	13.2609	12.5952	13.2361	13.2513	13.3019	13.2998	13.23	13.4298	13.2605	13.2612	11.1401
	68			23	18.4665	18.1854	18.4398	18.456	18.6301	18.5658	18.4068	18.8225	18.4628	18.4662	14.8406
	69			25	25.1642	28.6969	25.2546	25.2553	25.4283	25.3139	25.08	25.3541	25.1117	25.157	19.1707
	70			26	26.8571	29.2336	26.9218	26.9253	27.008	26.9504	26.8001	26.9479	26.8175	26.8518	33.3933
	71			27	12.5154	2.8355	12.975	12.9299	13.5289	13.0385	12.2504	12.8266	12.2957	12.4843	9.5775
	72			28	10.7481	2.7064	11.0194	10.999	6.73	12.2126	10.1619	10.1782	10.6153	10.7296	8.4166
	73			29	9.7081	3.4948	9.7696	9.7766	7.6508	8.6968	8.7595	8.1561	9.6722	9.7038	8.0528
	74			31	9.808	4.2448	9.7948	9.8115	8.4322	9.1617	10.0946	7.9063	9.8067	9.8087	8.3934
	75			32	11.9665	5.8847	11.7443	11.7914	12.1223	12.0674	11.9022	12.8539	12.0353	11.9762	9.6483
	76			113	10.6018	8.3594	10.5531	10.5715	10.3944	10.52	10.6271	10.4695	10.617	10.6046	11.2514
	77			114	11.6346	4.0373	10.6736	11.7075	12.1513	11.9131	11.4858	12.2793	10.9606	11.692	9.056
	78			115	11.6267	3.7711	10.539	11.7419	12.2049	11.9355	11.4635	12.23	11.0087	11.5403	9.0037

Parameters	Parameters				Orignal	Scenarios									
	No.	From	To	Label		24	25	26	27	28	29	30	31	32	33
Generator active	1			Ge1	220	220	220	220	220	220	220	220	220	220	220
	2			Ge2	-9	-9	-9	-9	-9	-9	-9	-9	-9	-9	-9
	3			Ge3	7	7	7	7	7	7	7	7	7	7	7
	4			Ge4	0	0	0	0	0	0	0	0	0	0	0
	5			Ge5	314	314	314	314	314	314	314	314	314	314	314
	6			Ge6	-6	-6	-6	-6	-6	-6	-6	-6	-6	-6	-6
Generator reactive	7			Ge1	50.46	16.89	50.45	50.5	45.49	46.21	84	42.18	49.17	50.46	50.72
	8			Ge2	8.29	23.07	14.64	3.97	3.56	3.45	29.54	0.78	3.92	3.36	4.64
	9			Ge3	33.23	32.79	33.03	32.88	32.59	32.49	41.85	31.15	32.7	31.92	51.86
	10			Ge4	-11.9	-3.07	16.56	0.77	-14	-14	6.23	-14	-14	-14	-14
	11			Ge5	52.61	28.35	15.75	12.75	16.2	15.47	37.21	12.26	14.4	12.07	11.04
	12			Ge6	7.02	9.37	7.6	-4.26	9.32	8.99	31.88	7.16	8.73	13.87	2.3
transmission line active power	13	25	27	L1	144.31	220.05	192.88	142.79	147.58	146.98	233.58	143.83	146.22	144.22	148.03
	14	23	25	L11	-157.58	0	-91.79	-156.77	-132.31	-136.83	-287.27	-160.25	-143.02	-157.51	-158.5
	15	23	32	L12	97.22	3.17	0	94.81	119	115.1	147.29	96.5	109.47	97.12	101.2
	16	32	113	L13	6.42	-7.69	-20.07	0	17.85	15.81	65.75	5.85	12.87	6.19	1.18
	17	22	23	L14	-56.12	-27.5	-71.85	-56.87	0	-10	-94.43	-55.66	-24.03	-56.13	-54.62
	18	21	22	L15	-45.64	-17.43	-60.99	-46.38	10.02	0	-82.72	-45.22	-14.09	-45.65	-44.18
	19	26	30	L16	228.15	313.95	247.86	230.51	251.3	247.2	0	225.97	241.45	228.3	223.45
	20	23	24	L17	-3.91	-37.96	11.06	-3.1	6.31	4.69	35.06	0	2.38	-3.89	-5.42
	21	20	21	L18	-31.44	-3.42	-46.54	-32.16	24.18	14.05	-67.67	-31.02	0	-31.44	-29.99
	22	17	113	L19	-0.22	13.85	26.46	6	-11.4	-9.41	-56.04	0.35	-6.6	0	5.07
	23	27	115	L2	20.72	42.03	36.23	20.01	20.48	20.52	38.12	20.68	20.59	20.69	20.54
	24	17	31	L20	12.38	22.65	37	9.67	0.76	2.83	-49.42	12.99	5.78	12.35	0
	25	27	32	L3	12.49	52.24	41.43	11.2	12.02	12.09	44.94	12.3	12.25	12.44	12.17
	26	27	28	L4	33.64	40.17	32.92	34.22	37.34	36.67	62.94	33.39	35.74	33.64	37.53
	27	28	29	L5	16.41	22.85	15.7	16.98	20.05	19.4	45.13	16.16	18.47	16.41	20.24
	28	29	31	L6	-7.67	-1.3	-8.37	-7.1	-4.06	-4.71	20.56	-7.92	-5.63	-7.67	-3.88
	29	31	32	L7	-31.47	-14.98	-8.11	-33.62	-39.45	-38.03	-66.73	-31.16	-35.96	-31.52	-39.69
	30	32	114	L8	9.37	-11.68	-5.99	10.08	9.61	9.57	-7.84	9.42	9.5	9.4	9.55
	31	114	115	L9	1.36	-19.71	-14	2.07	1.6	1.56	-15.85	1.4	1.49	1.39	1.54
transformer active	32			L10	85.85	0.06	66.14	83.49	62.69	66.8	314.16	88.08	72.56	85.69	90.55
transmission line reactive power	33	25	27	L1	30.08	36.93	33.38	30.04	30.18	30.16	39.17	30.06	30.13	30.08	30.19
	34	23	25	L11	-27.9	0	-37.96	-28.23	-29.43	-29.09	10.56	-19.75	-30.29	-27.92	-27.67
	35	23	32	L12	3.94	7.84	0	4.61	4.99	4.81	-9.49	8.16	3.68	3.96	3.43
	36	32	113	L13	-18.26	-14.29	-10.22	0	-21.12	-20.61	-30.65	-17.52	-20.01	-18.2	-16.85
	37	22	23	L14	-5.97	-7.42	-5.2	-5.84	0	-5	0.75	-7.29	-10.95	-5.97	-6.2
	38	21	22	L15	-1.05	-4.33	1.47	-0.84	3.06	0	11.28	-2.44	-8.01	-1.05	-1.42
	39	26	30	L16	-9.02	8.17	-5.19	-8.63	-4.64	-5.48	0	-9.28	-6.61	-9.35	-10.54
	40	23	24	L17	13.54	-15.82	24.96	13.19	21.44	20.14	-15.33	0	15.51	13.54	13.86
	41	20	21	L18	5.93	1.72	9.61	6.18	9.89	6.34	22.25	4.48	0	5.93	5.47
	42	17	113	L19	5.33	-0.3	-1.87	3.52	7.6	7.22	5.25	5.23	6.66	0	9.12
	43	27	115	L2	4.79	1.2	2.17	5.2	4.61	4.62	1.85	3.94	4.83	4.79	4.94
	44	17	31	L20	11.96	8.82	5.57	12.76	15.22	14.63	30.07	11.8	13.79	12.48	0
	45	27	32	L3	1.26	-9.12	-6.31	2.15	0.96	0.97	-7.23	-0.33	1.35	1.27	1.58
	46	27	28	L4	-0.73	-1.9	-0.6	-0.84	-1.41	-1.29	-5.12	-0.69	-1.12	-0.73	-1.44
	47	28	29	L5	-6.76	-8.36	-6.58	-6.9	-7.67	-7.5	-13.74	-6.69	-7.27	-6.76	-7.71
	48	29	31	L6	-8.86	-10.74	-8.65	-9.02	-9.92	-9.73	-17.78	-8.79	-9.46	-8.86	-9.97
	49	31	32	L7	12.55	7.45	5.26	13.69	15	14.52	25.92	11.16	14.13	12.56	15.6
	50	32	114	L8	2.04	6.79	5.35	1.62	2.22	2.21	5.82	2.88	2	2.04	1.89
	51	114	115	L9	0.49	5.17	3.81	0.06	0.66	0.65	4.25	1.32	0.45	0.48	0.33

Parameters					Orignal	Scenarios									
Parameters						24	25	26	27	28	29	30	31	32	33
	No.	From	To	Label											
transformer reactive	52			L10	21.45	20.18	20.93	21.38	20.86	20.95	37.21	21.52	21.09	21.44	21.59
voltage magnitude	53			21	0.9578	0.9527	0.9567	0.9575	0.9205	0.9335	0.9377	0.9609	0.9674	0.9578	0.9581
	54			22	0.9687	0.9599	0.9694	0.9685	0.9139	0.9954	0.9475	0.9731	0.9774	0.9687	0.9691
	55			23	0.9994	0.9799	1.0069	0.9993	1.0046	1.0037	0.9902	1.0054	1.0012	0.9994	0.9993
	56			25	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05
	57			26	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015
	58			27	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968
	59			28	0.9616	0.9615	0.9616	0.9616	0.9615	0.9615	0.9608	0.9616	0.9616	0.9616	0.9615
	60			29	0.9632	0.9633	0.9632	0.9632	0.9633	0.9633	0.9633	0.9632	0.9633	0.9632	0.9633
	61			31	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967
	62			32	0.9634	0.963	0.963	0.963	0.9637	0.9637	0.963	0.9647	0.9634	0.9634	0.9632
	63			113	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.993
	64			114	0.9603	0.9599	0.96	0.9601	0.9605	0.9605	0.9599	0.9611	0.9603	0.9603	0.9602
	65			115	0.9602	0.9598	0.9599	0.96	0.9604	0.9604	0.9598	0.9609	0.9602	0.9602	0.9601
voltage angle	66			21	10.5247	8.3126	10.9566	10.5664	1.0355	2.7873	11.6443	10.0726	16.8722	10.5293	10.4675
	67			22	13.2609	9.3296	14.6482	13.3506	0.4318	19.2483	16.993	12.7445	17.6136	13.2659	13.1092
	68			23	18.4665	11.8779	21.3026	18.6312	20.4048	20.1013	26.2558	17.8258	19.6705	18.4721	18.1664
	69			25	25.1642	34.2295	25.0005	25.2909	25.9506	25.8521	39.1565	24.6698	25.6969	25.1665	24.9071
	70			26	26.8571	34.2306	26.3046	26.9371	27.1866	27.1691	45.3623	26.4065	27.1276	26.8561	26.6925
	71			27	12.5154	14.456	7.793	12.7842	12.9952	12.9535	18.1	12.066	12.8694	12.5258	11.9101
	72			28	10.7481	12.3306	6.0652	10.985	11.0249	11.0196	14.7344	10.3125	10.9869	10.7583	9.9291
	73			29	9.7081	10.8914	5.0692	9.9095	9.7586	9.794	11.9133	9.2878	9.8187	9.7182	8.6513
	74			31	9.808	10.8491	5.1847	9.9967	9.778	9.8278	11.3791	9.3931	9.8731	9.818	8.6667
	75			32	11.9665	11.9151	5.7942	12.3074	12.4642	12.4192	15.9249	11.5043	12.3327	11.9795	11.3802
	76			113	10.6018	12.4125	7.9475	10.3965	9.6042	9.8268	6.8491	10.2377	10.1184	10.6446	10.7041
	77			114	11.6346	12.4214	6.0723	11.945	12.1249	12.0813	16.2773	11.1785	11.9956	11.6465	11.0402
	78			115	11.6267	12.5564	6.1685	11.9319	12.1157	12.0723	16.3861	11.1715	11.9868	11.6384	11.031

Parameters					Orignal	Scenarios									
Parameters						34	35	36	37	38	39	40	41	42	43
	No.	From	To	Label											
Generator active	1			Ge1	220	220	220	220	220	220	220	220	220	220	220
	2			Ge2	-9	-9	-9	-9	-9	-9	-9	-9	-9	-9	-9
	3			Ge3	7	7	7	7	7	7	7	7	7	7	7
	4			Ge4	0	0	0	0	0	0	0	0	0	0	0
	5			Ge5	314	314	314	314	314	314	314	314	314	314	314
	6			Ge6	-6	-6	-6	-6	-6	-6	-6	-6	-6	-6	-6
Generator reactive	7			Ge1	50.46	48.99	49.98	49.87	49.49	46.72	50.04	49.42	48.3	48.64	49.13
	8			Ge2	8.29	-28.36	-5.18	-0.22	0.77	-18.43	-0.83	-7.73	2.72	2.87	3.03
	9			Ge3	33.23	32.39	27.4	22.59	-8.01	22.82	31.61	30.63	32.12	32.19	32.26
	10			Ge4	-11.9	-14	-14	-14	-14	-14	-14	-14	-14	-14	-14
	11			Ge5	52.61	13.57	12.59	12.5	12.5	13.1	12.52	12.71	12.36	12.48	12.56
	12			Ge6	7.02	9.11	8.12	8.22	8.59	4.45	7.62	7.38	7.74	7.8	7.86
transmission line active power	13	25	27	L1	144.31	122.89	139.47	139.14	136.15	131.91	142.14	138.18	144.07	144.23	144.37
	14	23	25	L11	-157.58	-164.33	-159.15	-159.34	-160.43	-159.2	-158.08	-159.07	-156.81	-156.28	-155.8
	15	23	32	L12	97.22	79.74	92.37	90.38	85.04	75.38	94.53	89.97	97.78	98.28	98.69
	16	32	113	L13	6.42	17.52	9.11	9.65	11.82	20.14	8.11	10.97	6.57	6.87	7.13
	17	22	23	L14	-56.12	-58.21	-56.53	-56.45	-56.55	-58.19	-56.4	-56.88	-50.2	-50.25	-56.9
	18	21	22	L15	-45.64	-47.68	-46.05	-45.97	-46.06	-47.68	-45.92	-46.39	-39.87	-49.74	-46.35
	19	26	30	L16	228.15	242.55	231.35	231.48	233.34	238.89	229.79	232.74	229.24	229.62	229.96
	20	23	24	L17	-3.91	18.14	2.08	4.36	10.69	17.39	-1.01	4.04	0.93	-0.16	-0.98
	21	20	21	L18	-31.44	-33.44	-31.83	-31.75	-31.85	-33.44	-31.71	-32.17	-39.6	-35.48	-32.15
	22	17	113	L19	-0.22	-11.21	-2.9	-3.45	-5.62	-13.71	-1.9	-4.73	-0.37	-0.67	-0.93
	23	27	115	L2	20.72	31.96	22.57	21.45	20.84	16.36	17.61	10.98	20.65	20.66	20.67
	24	17	31	L20	12.38	-1.29	7.1	2.7	-6.25	-0.63	10.59	7.5	12.25	11.93	11.66
	25	27	32	L3	12.49	33.39	15.92	13.83	12.68	3.53	12.92	14.4	12.33	12.36	12.38
	26	27	28	L4	33.64	43.33	23.84	26.79	25.85	35.53	34.32	35.7	33.64	33.75	33.84
	27	28	29	L5	16.41	25.93	23.76	9.65	8.73	18.27	17.08	18.43	16.41	16.52	16.61
	28	29	31	L6	-7.67	1.72	-0.39	9.64	-15.28	-5.82	-7.01	-5.67	-7.67	-7.56	-7.47
	29	31	32	L7	-31.47	-35.64	-29.53	-24.06	-15.25	-42.63	-32.59	-34.35	-31.61	-31.82	-31.98
	30	32	114	L8	9.37	-1.77	7.53	8.64	9.25	13.73	4.45	-2.98	9.45	9.43	9.42
	31	114	115	L9	1.36	-9.77	-0.48	0.63	1.24	5.69	4.44	-10.98	1.43	1.42	1.41
transformer active	32			L10	85.85	71.45	82.65	82.52	80.66	75.11	84.21	81.27	84.8	84.4	84.02
transmission line reactive power	33	25	27	L1	30.08	29.85	29.96	29.95	29.9	29.86	30.02	29.94	30.07	30.08	30.08
	34	23	25	L11	-27.9	-25.41	-27.26	-27.11	-26.58	-24.5	-27.48	-26.82	-26.2	-26.63	-27.14
	35	23	32	L12	3.94	6.8	4.68	5	5.88	0.93	3.82	3.91	4.97	4.75	4.5
	36	32	113	L13	-18.26	-21.03	-18.93	-19.03	-19.54	-17.16	-18.34	-18.63	-18.16	-18.27	-18.37
	37	22	23	L14	-5.97	-5.68	-5.92	-5.95	-5.96	-6.12	-5.97	-5.94	-2.49	-3.25	-6.07
	38	21	22	L15	-1.05	-0.55	-0.96	-1	-1	-1	-1.02	-0.95	1.8	-2.98	-1.08
	39	26	30	L16	-9.02	-7.45	-8.77	-8.85	-8.8	-8.05	-8.88	-8.61	-9.09	-8.94	-8.83
	40	23	24	L17	13.54	8.07	12.12	11.65	10.22	12.64	13.18	12.37	15.52	15.38	14.99
	41	20	21	L18	5.93	6.56	6.04	6	6.01	6.09	5.97	6.07	1.2	4.2	5.94
	42	17	113	L19	5.33	7.57	5.85	5.85	6.05	8.35	5.71	6.33	5.34	5.41	5.47
	43	27	115	L2	4.79	2.43	4.32	4.48	4.5	-1.22	2.81	-0.38	4.59	4.63	4.68
	44	17	31	L20	11.96	15.87	13.45	14.75	17.49	15.66	12.45	13.32	11.99	12.08	12.15
	45	27	32	L3	1.26	-5.1	0.06	0.55	0.68	-9.32	0.03	-1.75	0.89	0.96	1.05
	46	27	28	L4	-0.73	-2.42	-5.55	-1.25	0.79	-1.08	-0.86	-1.11	-0.73	-0.76	-0.77
	47	28	29	L5	-6.76	-9.12	-4.06	-6.89	-4.82	-7.22	-6.92	-7.26	-6.76	-6.78	-6.81
	48	29	31	L6	-8.86	-11.67	-6.42	-4.8	-6.7	-9.4	-9.05	-9.44	-8.86	-8.89	-8.92
	49	31	32	L7	12.55	13.65	11.73	9.79	6.73	6.16	12.08	11.64	12.28	12.41	12.54
	50	32	114	L8	2.04	4.83	2.55	2.36	2.34	7.98	0.86	-0.12	2.24	2.2	2.16
	51	114	115	L9	0.49	3.31	1.02	0.82	0.78	6.34	2.36	-1.61	0.68	0.65	0.6

Parameters					Orignal	Scenarios									
Parameters						34	35	36	37	38	39	40	41	42	43
	No.	From	To	Label											
transformer reactive	52			L10	21.45	21.06	21.36	21.35	21.3	21.15	21.4	21.32	21.42	21.41	21.4
voltage magnitude	53			21	0.9578	0.9574	0.9577	0.9578	0.9578	0.9584	0.9578	0.9578	0.9728	0.9638	0.9581
	54			22	0.9687	0.9684	0.9687	0.9688	0.9689	0.9699	0.9688	0.9689	0.9792	0.9777	0.9693
	55			23	0.9994	0.9996	0.9995	0.9995	0.9997	1.0018	0.9996	0.9999	1.001	1.0008	1.0005
	56			25	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05	1.05
	57			26	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015	1.015
	58			27	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968	0.968
	59			28	0.9616	0.9615	0.9675	0.9632	0.9616	0.9616	0.9616	0.9616	0.9616	0.9616	0.9616
	60			29	0.9632	0.9633	0.9649	0.9666	0.9631	0.9632	0.9632	0.9633	0.9632	0.9632	0.9632
	61			31	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967	0.967
	62			32	0.9634	0.9638	0.9636	0.9636	0.9638	0.9737	0.9643	0.9653	0.9637	0.9637	0.9636
	63			113	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.993	0.993
	64			114	0.9603	0.9605	0.9604	0.9605	0.9606	0.9664	0.9626	0.9653	0.9605	0.9605	0.9604
	65			115	0.9602	0.9603	0.9603	0.9604	0.9604	0.9655	0.9622	0.9658	0.9604	0.9604	0.9603
voltage angle	66			21	10.5247	14.6399	11.6748	12.1492	13.4129	14.4941	11.071	12.0131	12.3959	11.6324	11.0002
	67			22	13.2609	17.5065	14.4363	14.9052	16.1743	17.3472	13.8236	14.7945	14.7602	14.5435	13.7759
	68			23	18.4665	22.9158	19.6812	20.1411	21.4185	22.7264	19.0539	20.069	19.4195	19.2011	19.044
	69			25	25.1642	29.9299	26.4527	26.922	28.2508	29.5085	25.776	26.8382	26.087	25.8432	25.6628
	70			26	26.8571	31.3387	28.0824	28.549	29.8413	30.9894	27.4364	28.4407	27.759	27.5075	27.3196
	71			27	12.5154	19.2866	14.2566	14.7572	16.3658	18.021	13.3305	14.7628	13.4604	13.2015	13.0086
	72			28	10.7481	16.989	12.9564	13.3469	15.0263	16.1498	11.5258	12.8826	11.6929	11.4279	11.23
	73			29	9.7081	15.3586	11.5384	12.7026	14.4627	14.994	10.4442	11.7168	10.6526	10.381	10.1774
	74			31	9.808	15.2485	11.5063	12.4778	14.7319	15.0527	10.5292	11.772	10.7524	10.4784	10.2728
	75			32	11.9665	17.679	13.5318	14.1361	15.8001	17.7419	12.7448	14.084	12.9139	12.6547	12.4617
	76			113	10.6018	14.8623	11.8154	12.3504	13.7323	14.7819	11.173	12.1563	11.5351	11.2348	11.0066
	77			114	11.6346	17.7927	13.274	13.8347	15.4755	17.3022	12.5903	14.2015	12.5811	12.322	12.129
	78			115	11.6267	17.8607	13.2787	13.832	15.4687	17.275	12.5653	14.2696	12.573	12.3139	12.121

Appendix B: IEEE Copyright for PMAPS Conference Paper

IEEE COPYRIGHT AND CONSENT FORM

To ensure uniformity of treatment among all contributors, other forms may not be substituted for this form, nor may any wording of the form be changed. This form is intended for original material submitted to the IEEE and must accompany any such material in order to be published by the IEEE. Please read the form carefully and keep a copy for your files.

Power Grid Security Improvement by Remedial Action Schemes Using Vulnerability Assessment Based on Fault Chains and Power Flow
Parviz Khaledian, Brian Johnson and Saied Hemati
2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)

COPYRIGHT TRANSFER

The undersigned hereby assigns to The Institute of Electrical and Electronics Engineers, Incorporated (the "IEEE") all rights under copyright that may exist in and to: (a) the Work, including any revised or expanded derivative works submitted to the IEEE by the undersigned based on the Work; and (b) any associated written or multimedia components or other enhancements accompanying the Work.

GENERAL TERMS

1. The undersigned represents that he/she has the power and authority to make and execute this form.
2. The undersigned agrees to indemnify and hold harmless the IEEE from any damage or expense that may arise in the event of a breach of any of the warranties set forth above.
3. The undersigned agrees that publication with IEEE is subject to the policies and procedures of the IEEE PSPB Operations Manual.
4. In the event the above work is not accepted and published by the IEEE or is withdrawn by the author(s) before acceptance by the IEEE, the foregoing copyright transfer shall be null and void. In this case, IEEE will retain a copy of the manuscript for internal administrative/record-keeping purposes.
5. For jointly authored Works, all joint authors should sign, or one of the authors should sign as authorized agent for the others.
6. The author hereby warrants that the Work and Presentation (collectively, the "Materials") are original and that he/she is the author of the Materials. To the extent the Materials incorporate text passages, figures, data or other material from the works of others, the author has obtained any necessary permissions. Where necessary, the author has obtained all third party permissions and consents to grant the license above and has provided copies of such permissions and consents to IEEE

You have indicated that you DO wish to have video/audio recordings made of your conference presentation under terms and conditions set forth in "Consent and Release."

CONSENT AND RELEASE

1. In the event the author makes a presentation based upon the Work at a conference hosted or sponsored in whole or in part by the IEEE, the author, in consideration for his/her participation in the conference, hereby grants the IEEE the unlimited, worldwide, irrevocable permission to use, distribute, publish, license, exhibit, record, digitize, broadcast, reproduce and archive, in any format or medium, whether now known or hereafter developed: (a) his/her presentation and comments at the conference; (b) any written materials or multimedia files used in connection with his/her presentation; and (c) any recorded interviews of him/her (collectively, the "Presentation"). The permission granted includes the transcription and reproduction of the Presentation for inclusion in products sold or distributed by IEEE and live or recorded broadcast of the Presentation during or after the conference.
2. In connection with the permission granted in Section 1, the author hereby grants IEEE the unlimited, worldwide, irrevocable right to use his/her name, picture, likeness, voice and biographical information as part of the advertisement, distribution and sale of products incorporating the Work or Presentation, and releases IEEE from any claim based on

right of privacy or publicity.

BY TYPING IN YOUR FULL NAME BELOW AND CLICKING THE SUBMIT BUTTON, YOU CERTIFY THAT SUCH ACTION CONSTITUTES YOUR ELECTRONIC SIGNATURE TO THIS FORM IN ACCORDANCE WITH UNITED STATES LAW, WHICH AUTHORIZES ELECTRONIC SIGNATURE BY AUTHENTICATED REQUEST FROM A USER OVER THE INTERNET AS A VALID SUBSTITUTE FOR A WRITTEN SIGNATURE.

Parviz Khaledian 

Signature

21-03-2018

Date (dd-mm-yyyy)

Information for Authors

AUTHOR RESPONSIBILITIES

The IEEE distributes its technical publications throughout the world and wants to ensure that the material submitted to its publications is properly available to the readership of those publications. Authors must ensure that their Work meets the requirements as stated in section 8.2.1 of the IEEE PSPB Operations Manual, including provisions covering originality, authorship, author responsibilities and author misconduct. More information on IEEE's publishing policies may be found at http://www.ieee.org/publications_standards/publications/rights/authorrightsresponsibilities.html Authors are advised especially of IEEE PSPB Operations Manual section 8.2.1.B12: "It is the responsibility of the authors, not the IEEE, to determine whether disclosure of their material requires the prior consent of other parties and, if so, to obtain it." Authors are also advised of IEEE PSPB Operations Manual section 8.1.1B: "Statements and opinions given in work published by the IEEE are the expression of the authors."

RETAINED RIGHTS/TERMS AND CONDITIONS

- Authors/employers retain all proprietary rights in any process, procedure, or article of manufacture described in the Work.
- Authors/employers may reproduce or authorize others to reproduce the Work, material extracted verbatim from the Work, or derivative works for the author's personal use or for company use, provided that the source and the IEEE copyright notice are indicated, the copies are not used in any way that implies IEEE endorsement of a product or service of any employer, and the copies themselves are not offered for sale.
- Although authors are permitted to re-use all or portions of the Work in other works, this does not include granting third-party requests for reprinting, republishing, or other types of re-use.The IEEE Intellectual Property Rights office must handle all such third-party requests.
- Authors whose work was performed under a grant from a government funding agency are free to fulfill any deposit mandates from that funding agency.

AUTHOR ONLINE USE

- **Personal Servers**. Authors and/or their employers shall have the right to post the accepted version of IEEE-copyrighted articles on their own personal servers or the servers of their institutions or employers without permission from IEEE, provided that the posted version includes a prominently displayed IEEE copyright notice and, when published, a full citation to the original IEEE publication, including a link to the article abstract in IEEE Xplore. Authors shall not post the final, published versions of their papers.
- **Classroom or Internal Training Use.** An author is expressly permitted to post any portion of the accepted version of his/her own IEEE-copyrighted articles on the author's personal web site or the servers of the author's institution or company in connection with the author's teaching, training, or work responsibilities, provided that the appropriate copyright, credit, and reuse notices appear prominently with the posted material. Examples of permitted uses are lecture materials, course packs, e-reserves, conference presentations, or in-house training courses.
- **Electronic Preprints.** Before submitting an article to an IEEE publication, authors frequently post their manuscripts to their own web site, their employer's site, or to another server that invites constructive comment from colleagues. Upon submission of an article to IEEE, an author is required to transfer copyright in the article to IEEE, and the author must update any