Spring 2014

Analysis and modeling of resilience for networked systems

Kamlesh Ashok Joshi

ANALYSIS AND MODELING OF RESILIENCE FOR NETWORKED SYSTEMS

by

KAMLESH ASHOK JOSHI

A THESIS

Presented to the Faculty of the Graduate School of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

2014

Approved by

Sahra Sedigh Sarvestani

Minsu Choi

Ali R. Hurson

ABSTRACT

A cyber physical system (CPS) has two main subsystems; a physical infrastructure that is responsible for managing and implementing physical tasks, *e.g.*, generation and distribution of a physical commodity, and a cyber infrastructure that is used to support and enhance these physical operations through computing, communication, and control. Imperfect cyber control can lower the efficacy and even reliability of existing physical infrastructures. As such, justifiable reliance on CPSs requires rigorous investigation of the effect of incorporating cyber infrastructure on functional and non-functional aspects of system performance. One non-functional metric of note is resilience, defined as the ability of a system to “bounce back” from a disrupted state to what is considered as an acceptable performance.

This dissertation proposes a deterministic and non-deterministic model for resilience of networked CPSs. The model is illustrated through application to a nine-bus power grid. Multiple disruptive events are considered, and associated figures of merit are defined, with the overall objective of representing system-level resilience as a function of component restoration time – assumed to be both deterministic and non-deterministic. The proposed technique can also be used to rank components based on their impact on system resilience. The model is validated through discrete event simulation.

ACKNOWLEDGMENTS

This is indeed a great pleasure and moment of immense satisfaction for me to express my sense of profound gratitude towards my thesis advisor, Dr. Sahra Sedigh Sarvestani, whose zeal and enthusiasm was the source of inspiration for me. I am very much thankful to her.

I would also like to thank Dr. Ali Hurson and Dr. Minsu Choi for serving on my committee and taking time to review my thesis.

I would also like to extend my thanks to my Fiancée Snehal, for her endless support, inspiration, and taking care of my needs as demanded. Thanks to all my friends and colleagues especially Raghvendra Kuber, Omkar Ghatpande and Suraj Shet, the social atmosphere is very important for me and I have been provided with good one.

My mother, Pushpalata Joshi (Aai), is the backbone of my entire US journey. Because of her sacrifice and emotional support, it became possible for me to dream about and successfully concluding my Masters. Right from arranging my application packets to packing my bags for my US stay, she was everywhere to fulfill my each and every need. Many thanks to her!

I am also obliged to show gratitude towards my sisters, Tai, Titu and Diku and their family, my maternal uncles and family to provide immense support for my academic excursion in US.

TABLE OF CONTENTS

Page

LIST OF ILLUSTRATIONS

Page

LIST OF TABLES

NOMENCLATURE

Symbol	Description
CEN	Current Evaluation Network
CPS	Cyber Physical Systems
ETN	Electrical Topology Network
FACTS	Flexible Alternating Current Transmission System
FOM	Figure of Merit
GSPN	Generalized Stochastic Petri-Net
IEEE	Institute of Electrical and Electronics Engineer
LESPN	Logical Explicit Stochastic Petri-Net
MIS	Markov Imbeddable Structure
RBD	Reliability Block Diagram
RBTS	Roy Billinton Test System
SMN	Stochastic Model Network
VCPI	Voltage Collapse Proximity Index

1. INTRODUCTION

The pervasive nature of numerous critical infrastructure systems such as smart grid, water distribution, telecommunications and transportation system has impelled many of the researchers across the globe to invest ample amount of time to model, validate and thereby to ensure system reliability, safety and stability. Uncalled disruptive events on such crucial networks, whether man-made or natural causes have coercive effects which often lead to component failures and thereby breaking down the entire system. While many of the studies are actually focused on prevention and protection, novel efforts are put forth, such as resilience and vulnerability analysis to safeguard from malicious or natural disruptions.

The ultimate aim of any power system engineer is to keep the power network stable and protected from any malevolent attacks or natural disasters. The idea of self-healing infrastructure is also finding its own direction to move forward in research and development. In this large and complex world of power infrastructure we cannot guarantee the safe and reliable power supply, although engineers strive very hard to maintain its safety and reliability. Hence a proper research must be undertaken to find the optimal time for a system to recover or “bounce back” from the disruption caused by man-made attacks or natural calamities. The work presented in this thesis provides a step towards focusing on some of the aspects of resilience and vulnerability analysis of power domain. The goal of this work is to lay a new path of research in the direction involving resilience based network component importance technique.

A nine-bus power transmission network has been used to analyze network resilience by defining proper metrics like service function and resilient strategies.

Resilience build up should not be necessarily dealing with complete disruption, instead worst possible scenario according to three line contingency analysis is carried out and disruptive events are decided. A novel way to define figures of merit is implemented to develop resilient strategies for a power transmission network.

The remainder of the thesis is organized as follows: Section 2 provides a varied literature review relevant to the work presented in this thesis. Section 3 presents a brief excursion about the metrics and parameters used in the concept of resilience based network. Section 4 contributes to the detailed modeling and simulation of nine-bus medium voltage power transmission network which is used to analyze the resilience metrics in power domain. Finally the thesis concludes in Section 5 suggesting the futuristic scope of the work put forward.

2. BACKGROUND AND RELATED WORK

The main focus of this thesis is to study resilience behavior of a small power network and also rank component importance as a system vulnerability and resilience point of view. The importance theory was first introduced by Birnbaum in 1969 [1] in which quantitative important measures were proposed. The reason behind this study is the intuitive fact that some components in any system are more important than other in order to provide and maintain continuous operation by the system. Failure detection and correction are some of the features of component importance. The placement of components also plays a vital role in importance analysis. For example, a component placed in series will have higher importance than the same component being placed in parallel system from reliability point of view. Generally, reliability importance is a function of operation time, failure, repair characteristics and system structure. Thus, all reliability importance indices are calculated through combinatorial approaches (such as Reliability Block Diagram (RBD)), or structure function, or Markov Modeling.

Importance theory is a quantitative measure which provides path of actions for reliability improvement or informs about operating and maintaining the system status. These importance measures provide a numerical rank to determine which components are more important to system reliability improvement or more critical to the system failure. The Smart Grid is a self-healing structure and as described earlier, it consists of various cyber and physical components, performing interdependent operations and amalgamating both repairable and non-repairable systems. In such practical applications, we need to address the system failure and restore distributions in addition to the “real world” constraints such as spare component availability and repair response time. Several methods such as importance indices or Markov reward model are used for modeling of such types of complex systems.

The work done in [2] by Fricks and Trivedi was introducing a novel technique of calculating importance measures in a state space dependability model. Markov reward model was specifically used unlike the most common method through combinatorial models. The substantial work was devoted in categorizing the importance measures as: 1) Structural importance - establishes the probability of system failure due to a given component when we consider that all states are equally probable, 2) Birnbaum component importance – deals with the transient measures and 3) Failure Criticality importance - measures the probability of a specific component which is responsible for system failure before time *t.* A specific example of series parallel Reliability Block Diagram was comprehensively elaborated and the relevance of the system components were computed through structure functions, Markov reward rate functions and Birnbaum importance.

Wang, Loman and Vassiliou [3] describes three importance indices such as 1) Failure Criticality Index – describes numerical rank for a particular component for the corresponding system characteristic of interest, 2) Restore Criticality Index – restoration of a system due to restoration of a particular component and 3) Operation Criticality Index – ratio of component downtime to systems downtime. Simulation results were presented with a simple example of series-parallel RBD in order to validate component measures.

Holling [4] introduced resilience to the scientific world through his seminal paper on ‘‘Resilience and Stability of Ecological Systems’’. Subsequently, the concept of resilience developed predominantly and independently in the disciplines like ecology, psychology and physics (specifically in material science).

At the turn of the century, there were a number of different opinions, definitions and classifications of resilience within many disciplines. However, the current interest in resilience of systems and enterprises has been triggered by the events of 9/11 [5].

Resilience based network metrics were discussed by Henry and Ramirez-Marquez in [6]. They proposed a quantifiable model for resilience metrics such as total time to resilience, total time to restoration, etc. It also deals with various system parameters that are necessary to define system resilience such as Figures of Merit, Disruptive Events and Resilience Strategies. The paper proposes that the theory could be applied to any system provided the associated figures of merit and the resilient strategies are properly defined. The defined metrics mostly dealt with the deterministic time approach. Barker, Ramirez-Marquez, et al [7] extended this proposition to amalgamate component importance measures with deterministic and non-deterministic time approach. The importance measures were analyzed using the similar example used in [6]. The importance was ranked according to the component vulnerability which affects the overall system vulnerability. Discrete Event Simulation was used to analyze non-deterministic time approach. Present study utilizes the concepts introduced from [6] and [7] which have provided a sound background of system resilience parameters that are further used to analyze the system resilience in power systems.

In order to extend the resilience theory in power domain, several literatures were found to be of great relevance. The idea behind looking at contingency evaluation of power systems examples was to associate apt figures of merit and resilient strategies.

Moghavvemi and Faruque [8] evaluated real time contingency and ranking measures on IEEE-6 and 24 bus system by defining new real time monitoring indicator known as VCPI (Voltage Collapse Proximity Indicator). This indicator was in fact associated with the voltage collapse which utilizes a basic maximum power transfer theorem. VCPI can be evaluated with different aspects of loading conditions in order to fulfill the demanding increment of load. For the present work the relevant definition for VCPI is given by

$$VCPI = \frac{P_r}{P_{r(max)}} \qquad (1)$$

where,

P_r = real power transferred to the receiving end.

$P_{r(max)}$ = maximum real power that can be transferred.

Crucitti, Latora and Marchiori [9] employed drop in efficiency as their importance measure to locate critical line in the referred network example. They utilized topological properties in graph theory to estimate the drop in efficiency when each link is removed from the network. In other words, the authors carried out vulnerability analysis and also suggested improvements to strengthen the critical link in the network.

Billinton, Allan, et al [10] modeled reliability test system often known as RBTS for academic purposes. They proposed all the reliability parameters that are used to carry out detailed reliability evaluation of distribution systems. Alkuhyali [11], Husshi [12] and Bae, Kim [13] utilizes RBTS and IEEE-6 bus system [21] to evaluate reliability improvement with Microgrids. All the results obtained in the above literature compares the reliability of entire system with and without Microgrids and no conclusion has been drawn towards the component importance of links or nodes that causes reliability improvement.

Petri nets are also widely used for reliability evaluation and hence extensive literature survey has been carried out in the present study for comparing efficiency of working with Petri nets for resilience analysis. Juliano S. A. Carneiro, Luca Ferrarini [14] describes a modeling approach of reliability analysis using Generalized Stochastic Petri nets (GSPN). Basically, the reliability analysis is dealing with the cascading failure events and protection against “hidden failures”. The novel thing they introduced about their model is the way they have defined the structure of a generic power system. They represented their model using three major blocks: 1) Electrical Topology Network (ETN) which represents the physical connectivity of the network, 2) Stochastic Model Network (SMN) which represents the SPN model for various conditions of events and transitions and 3) Current Evaluation Network (CEN) which conditions the firing probability of stochastic transition defined in the SMN according to the current flowing in transmission system. Major drawback is the scalability issue. ETN grows reasonably fast and long if the nodes are increased thereby increasing the reachability graph of SMN.

Mariana Dumitrescu [15] proposed a methodology that describes the dependability analysis of power systems, encompassing the modeling approach using Colored and Stochastic Petri nets simultaneously. The author named the Petri net as Logical Explicit Stochastic Petri Nets (LESPN).

White and Sedigh [16] modeled a small part of the security of a computer memory chip using attack graph and classical Petri net**.** Attack tree has provided the decision power in only four categories, whereas PN provided with fourteen categories. But there is always a tradeoff between modeling power and decision power**.**

Faza [17], presented a mathematical model based on knowledge of reliability estimates for individual components of the power grid to predict its overall system reliability. The model utilizes MIS (Markov Imbeddable Structure) technique which provides the way through which the reliability of power grid can be predicted at the system level. This information can help in determining the expected frequency of failures. It also aids in identification of areas of the system where adding redundancy will have the greatest impact on prevention of cascading failures. [18], [19] were mainly related to the deterministic approaches such as line and load contingency analysis and voltage stability. Optimal placement of FACTS (Flexible Alternating Current Transmission System) devices and analysis of max-flow algorithm were used to determine the value of power flow in FACTS settings.

The topics in the thesis have utilized the concepts studied from the above literatures to build and analyze the simulation results of the system examples. Contingency analysis was carried out in Power World Simulation 17 software [20] for the purpose of finding figures of merit and worst system disruptions. Analysis of resilience networks in power domain put forward in the present work provides a unique opportunity of research in power systems.

3. SYSTEM RESILIENCE: METRICS AND QUANTITATIVE APPROACHES

3.1. GENERAL INTRODUCTION

As described earlier, System Resilience is defined as an ability of a system to *“bounce back”* to an acceptable capable state from a defined disruptive state. The sections ahead describe the quantifiable metrics for developing the formula and computation of system resilience [4].

3.2. INITIAL FORMULATION

Let $R_F(t)$ be defined as a resilience of a system at time *t*. $R_F(t)$ is defined as a ratio of recovery time *t* to the loss suffered in time t_d as shown in Eq.(2)

$$R_F(t) = \frac{\text{Recovery}(t)}{\text{Loss}(t_d)} \tag{2}$$

Where, t_d is the instant at which system is reached to its worst disruption.

From Eq. (2) it can be understood that if the recovery time is equal to the loss time, then the system is completely resilient; and if there is no recovery or in other words system is unable to bounce back to its original service capability then the system is having no resilience. This is very crude definition and there is a need for a fundamental generic quantitative approach that will be omnipresent in the development of resilient strategies of the systems.

3.3. SYSTEM OF INTEREST

We will define a new system of interest *S* considering through resilience point of view. The system S is experiencing three distinct states: 1) Original state, S_0, 2) Disrupted state, S_d, and 3) Recovered state S_f; and two distinct transitions: 1) System disruption (from S_0 to S_d) and 2) System recovery (from S_d to S_f). There are two events that fire the transitions from one state to another, 1) Disruptive event and 2) Resilient action. Figure 3.1 illustrates the above states and respective transitions due to firing of subsequent events.

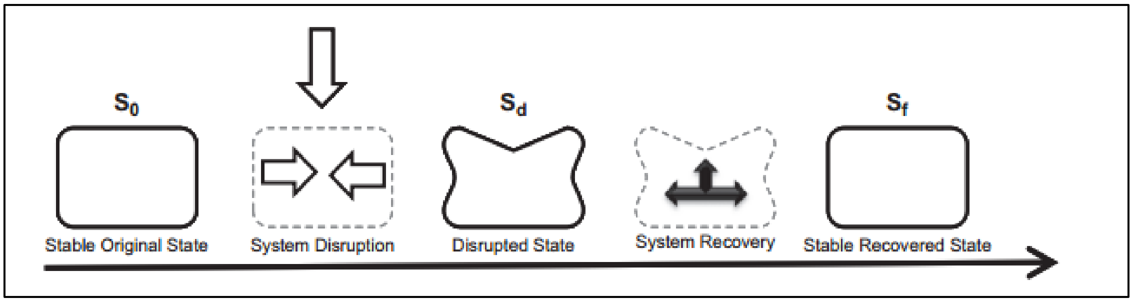

Figure 3.1 System function transition with respect to time [6]

Initially when there is no disruptive event, system is working in a reliable condition S_0 till time t_0. A disruptive event occurs that triggers the system disruption and the system enters into a disrupted state S_d. As a result of responsive measure of resilient action the system recovers back to its recovered state S_f. It could be noted that S_f could be the same or at different state that from S_0.

3.4. SYSTEM FUNCTION OR FIGURES- OF- MERIT (FOM)

The figure-of-merit, F(t), is basis of the resilience metric computation. FOM can be network, connectivity, flow, etc. depending upon the considered system of interest. The F(t) is directly associated with the state of the system. For example, corresponding to state S_0, the service function associated to the original state could be denoted as $F(t_0)$. Similarly, $F(t_d)$ and $F(t_f)$ are associated with states S_d and S_f respectively.

Figure 3.2 illustrates the FOM as a function of time. Computation of resilience affecting the system is synonymous to unambiguous identification of a quantifiable and time-dependent system level service function or associated FOM.

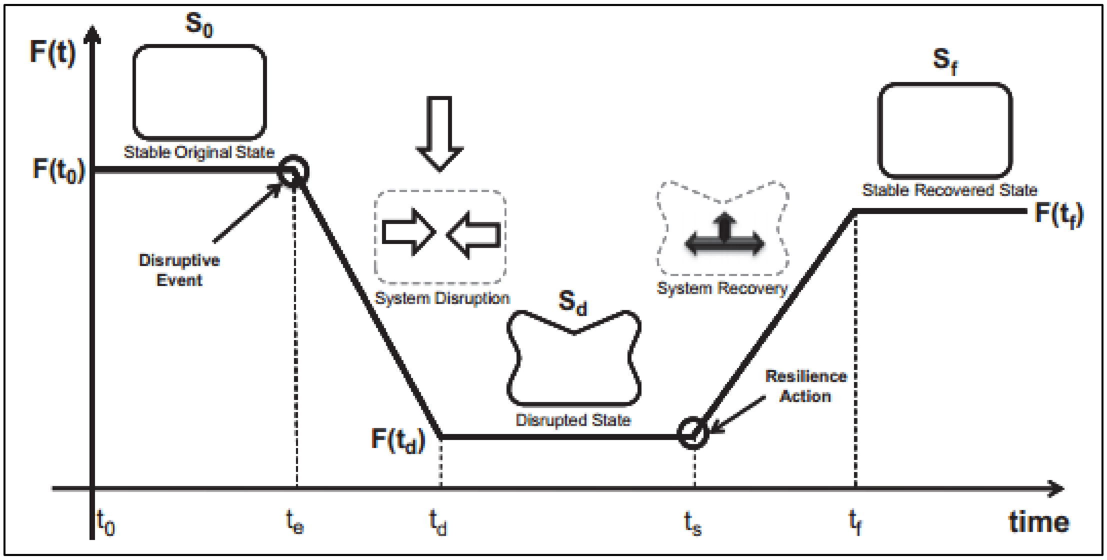

Figure 3.2 Service function as a function of time [7]

It must also be noted that the two events that transition the system disruption and system recovery need not be a single step action. The events could be a function of time and therefore the resulting transitions may also vary with time and not necessarily linearly. It could also be understood that in many cases, the system disruption will continue until the resilience action is triggered. From Figure 3.2 the time incidents t_d and t_s may coincide with no threshold and steady disrupted state.

3.5. DISRUPTIVE EVENTS

An event is considered to be disruptive if and only if it affects the system S in such a way that the corresponding values of the associated FOM are reduced. From Figure 3.1 and Figure 3.2, a disruptive event is one that affects S such that $F(t_d) < F(t_0)$. In actual system under study there can be multiple disruptive events which may or may not associate certain FOM with respect to other disruptive events. Mathematically, let E represents set of all events, $E = \{e_1, e_2, ..., e_m\}$. Then, the set of disruptive events D can be defined as

$$D = \{e_j \in E \mid F(t_d \mid e_j) < F(t_0) \qquad (3)$$

3.6. SYSTEM RESILIENCE ACTION AS A FUNCTION OF TIME

At this stage, system resilience can be defined with all the parameters stated in the above discussion. A successful resilience action is the one that restores the system to stable state S_f from a disrupted state S_d by increasing the value of associated FOM.

Based on the earlier discussion, the value of resilience $R_F(t_r \mid e_j)$ corresponding a specific FOM $F(t_r \mid e_j)$ evaluated for time t_r (where, $t_r \in (t_d, t_s)$) under the disruptive event e_j can be formulated as

$$R_F(t_r \mid e_j) = \frac{F(t_r \mid e_j) - F(t_d \mid e_j)}{F(t_0) - F(t_d \mid e_j)} \quad \forall e_j \in D \qquad (4)$$

3.7. ILLUSTRATIVE EXAMPLE (SEERVADA NATIONAL PARK PROBLEM)

This section will illustrate a simple example that will be used to describe the applicability and usefulness of the quantitative approach to resilience. The example presented will serve as representation for many infrastructure systems considered as system study.

3.7.1. Problem Setup. The Seervada Park Problem is used by Hillier and Lieberman [6] as an example to discuss the shortest-path, minimum spanning tree and maximum flow problems in Operations Management. This problem is modified here, to illustrate the quantitative framework to resilience. Figure 3.3 depicts the road network of the Seervada Park (i.e. the system of interest being considered for resilience analysis). Node O is the entrance to the park, and there is a scenic wonder at node T. Nodes A through E are ranger stations that serve as connection nodes for the road network. The park operates trams for visitors to reach the scenic wonder from the park entrance. The distance and maximum daily capacity of trams is provided for each road segment (between a pair of nodes). The arrows point to the direction in which trams ply while transporting passengers from the park entrance to the scenic wonder. The maximum daily capacity of trams includes return trips back to the park entrance.

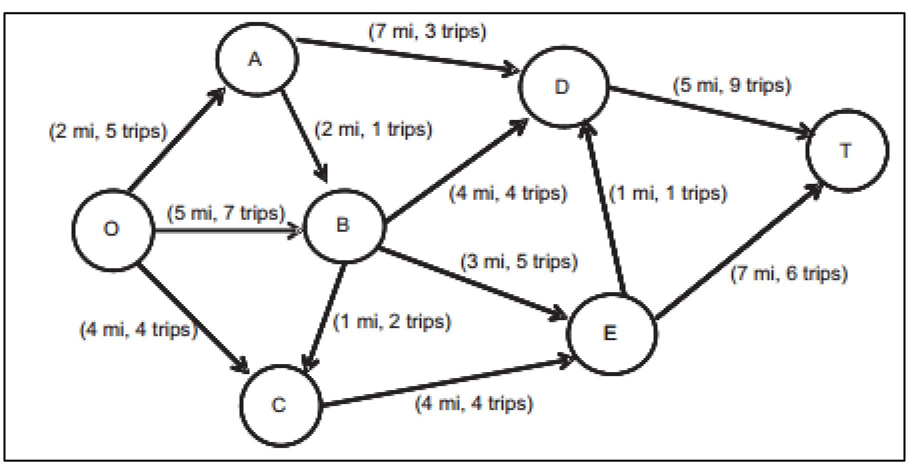

Figure 3.3 Seervada National Park Problem Network[5]

3.7.2. Associated FOM. Here, Three figure-of-merits are considered for the problem.

FOM 1: Shortest path from origin O to sink T

It describes the lowest preferable value. Any disruption will actually cause to yield a higher value. For the problem the shortest distance, FOM 1 = 13 units at t_0.

FOM 2: Max Flow between O and T

It describes the maximum daily capacity of trips from O and T. The FOM 2 calculated is 14 at t_0.

FOM 3: Overall Health of the network

FOM 3 is calculated as computed length of usable roads/total length of roads. Hence, at t_0, FOM 3 = 1. Now it may be noted that a certain disruptive event may affect FOM 3 but not other FOMs. For instance, certain disruption of a road may or may not be in the shortest path.

3.7.3. Disruptive Events. The problem assumes two disruptive events.

1) A rock slides results into outage of roads OA, OB, OC, AB and BC

2) Flood water runs over roads AD, BD, BE and CE

3.7.4. Resilient Strategies and Analysis. The resilient action is carried out in a *queue* as stated in the disruptive events and one at a time.

3.7.4.1 Deterministic time approach. The repair time of each link is assumed to be deterministic and the repair time of each link is assumed to be 20 units. Note that the disruption starts at t_d and the resilience action begins from t_s. t_1 to t_f are repair time for the respective link repair in a queue. Two strategies are defined: 1) Link repair occurs in a similar fashion as of disruption and 2) Link repair occurs in a reverse direction.

Table 3.1 will illustrate the network behavior under 1st disruptive event. Strategy 1 is first adopted to illustrate the resilience action for this particular event.

Table 3.1 Network behavior under Disruption 1 - Strategy 1

Road Segment	Network Status							
	t_0	t_d	t_s	t_1	t_2	t_3	t_4	t_f
OA	1	0	0	1	1	1	1	1
OB	1	0	0	0	1	1	1	1
OC	1	0	0	0	0	1	1	1
AB	1	0	0	0	0	0	1	1
BC	1	0	0	0	0	0	0	1
AD	1	1	1	1	1	1	1	1
BD	1	1	1	1	1	1	1	1
BE	1	1	1	1	1	1	1	1
CE	1	1	1	1	1	1	1	1
DT	1	1	1	1	1	1	1	1
ED	1	1	1	1	1	1	1	1
ET	1	1	1	1	1	1	1	1

Based upon this network behavior, resilience action is carried out and the respective FOMs are calculated at different disrupted conditions. Finally the resilience formula is implemented according to (3) to calculate the system resilience for the respective FOMs. Table 3.2 elaborates the resilience computations for considered FOMs for Disruption1 and implemented Strategy 1.

Table 3.2 Resilience computations for Disruption 1 - Strategy 1

Time	Network Status							
	t_0	t_d	t_s	t_1	t_2	t_3	t_4	t_f
FOM 1	13	-	-	14	14	14	13	13
Rf1	-	0	0	0.93	0.93	0.93	1	1
FOM 2	14	0	0	3	10	14	14	14
Rf2	-	0	0	0.214	0.714	1	1	1
FOM 3	1	0.689	0.689	0.734	0.845	0.934	0.978	1
Rf3	-	0	0	0.144	0.501	0.787	0.929	1

Similarly, the tables are developed for Disruption 1–Strategy 2, Disruption 2–Strategy 1 and Disruption 2–Strategy 2. As discussed earlier, unlike Strategy 1, Strategy 2 occurs in the reverse direction for both of the resilience actions. Disruption 2 deals with the link AD, BD, BE and CE failing together and disrupting all the FOMs to zero value (complete disruption). Following tables will demonstrate the network behavior and resilience computations for the respective disruptive events and implemented strategies for the respective FOMs.

Table 3.3 Network behavior under Disruption 1 - Strategy 2

Road Segment	Network Status							
	t_0	t_d	t_s	t_1	t_2	t_3	t_4	t_f
OA	1	0	0	0	0	0	0	1
OB	1	0	0	0	0	0	1	1
OC	1	0	0	0	0	1	1	1
AB	1	0	0	0	1	1	1	1
BC	1	0	0	1	1	1	1	1
AD	1	1	1	1	1	1	1	1
BD	1	1	1	1	1	1	1	1
BE	1	1	1	1	1	1	1	1
CE	1	1	1	1	1	1	1	1
DT	1	1	1	1	1	1	1	1
ED	1	1	1	1	1	1	1	1
ET	1	1	1	1	1	1	1	1

Table 3.4 Resilience computations for Disruption 1 - Strategy 2

Time	Network Status							
	t_0	t_d	t_s	t_1	t_2	t_3	t_4	t_f
FOM 1	13	-	-	-	-	14	14	13
Rf1	-	0	0			0.93	0.93	1
FOM 2	14	0	0	0	0	4	9	14
Rf2	-	0	0	0	0	0.285	0.642	1
FOM 3	1	0.689	0.689	0.712	0.755	0.845	0.956	1
Rf3	-	0	0	0.074	0.212	0.501	0.858	1

2^{nd} disruptive event doesn't deal with source or sink node. It deals with the intermediate links. The two strategies are implemented similarly as in case of 1^{st} disruptive event and the resilience calculations are carried out. The links which are not failed in this disruption are removed from Table 3.5. and Table 3.7 in order to avoid redundancy.

Table 3.5 Network behavior under Disruption 2 - Strategy 1

Road Segment	Network Status							
	t_0	t_d	t_s	t_1	t_2	t_3	t_4	t_f
AD	1	0	0	1	1	1	1	1
BD	1	0	0	0	1	1	1	1
BE	1	0	0	0	0	1	1	1
CE	1	0	0	0	0	0	1	1

Table 3.6 Resilience computations for Disruption 2 - Strategy 1

Time	Network Status							
	t_0	t_d	t_s	t_1	t_2	t_3	t_4	t_f
FOM 1	13	-	-	14	13	13	13	13
Rf1	-	0	0	0.93	1	1	1	1
FOM 2	14	0	0	3	7	11	14	14
Rf2	-	0	0	0.214	0.5	0.782	1	1
FOM 3	1	0.6	0.6	0.75	0.844	0.912	1	1
Rf3	-	0	0	0.375	0.61	0.78	1	1

Table 3.7 Network behavior under Disruption 2 - Strategy 2

Road Segment	Network Status							
	t_0	t_d	t_s	t_1	t_2	t_3	t_4	t_f
AD	1	0	0	0	0	0	1	1
BD	1	0	0	0	0	1	1	1
BE	1	0	0	0	1	1	1	1
CE	1	0	0	1	1	1	1	1

Table 3.8 Resilience computations for Disruption 2 - Strategy 2

Time	Network Status							
	t_0	t_d	t_s	t_1	t_2	t_3	t_4	t_f
FOM 1	13	-	-	14	14	13	13	13
Rf1	-	0	0	0.93	0.93	1	1	1
FOM 2	14	0	0	4	7	11	14	14
Rf2	-	0	0	0.2857	0.5	0.785	1	1
FOM 3	1	0.6	0.6	0.78	0.847	0.934	1	1
Rf3	-	0	0	0.375	0.6175	0.835	1	1

3.7.4.2 Non-deterministic time approach. The link recovery time for each link is assumed to be a uniform time distribution between (8, 12). A MATLAB program is developed considering discrete event simulation for 1000 iterations. Simulation is carried out for 1st disruptive event and Strategy 1. It is noticed that full network resilience occurred after the first three recovery activities (Link OA, OB and OC). Hence a discrete time event is bounded by the interval (24, 36). Approximate probability distribution and cumulative distribution function representations are plotted for resilience action as a function of non-deterministic time.

Furthermore probabilistic vulnerability analysis is carried out for system vulnerability as a function of component survivability to rank the component importance.

3.8. DETERMINISTIC AND NON DETERMINISTIC SIMULATION RESULTS AND DISCUSSIONS (SERVADA NATIONAL PARK PROBLEM)

Based on the tables of FOMs and respective resilience calculations, different plots are developed to analyze the strategy to find out optimal resilience methodology.

3.8.1. Deterministic Time Resilience Analysis. Figure 3.4 illustrates the effect of Strategy 1 applied on 1st disruptive event. From the graph it is evident that the network resilience builds up quite rapidly for FOM 1 when strategy 1 is implemented and the first link is restored. Although it requires another 3 links to reach complete network restoration. Figure 3.4 will not give the exact explanation for which strategy is better for which FOM unless we have an individual comparison for different FOMs considering both the strategies together. Subsequent figures will discuss different strategies and their effects will be analyzed on the network resilience build up.

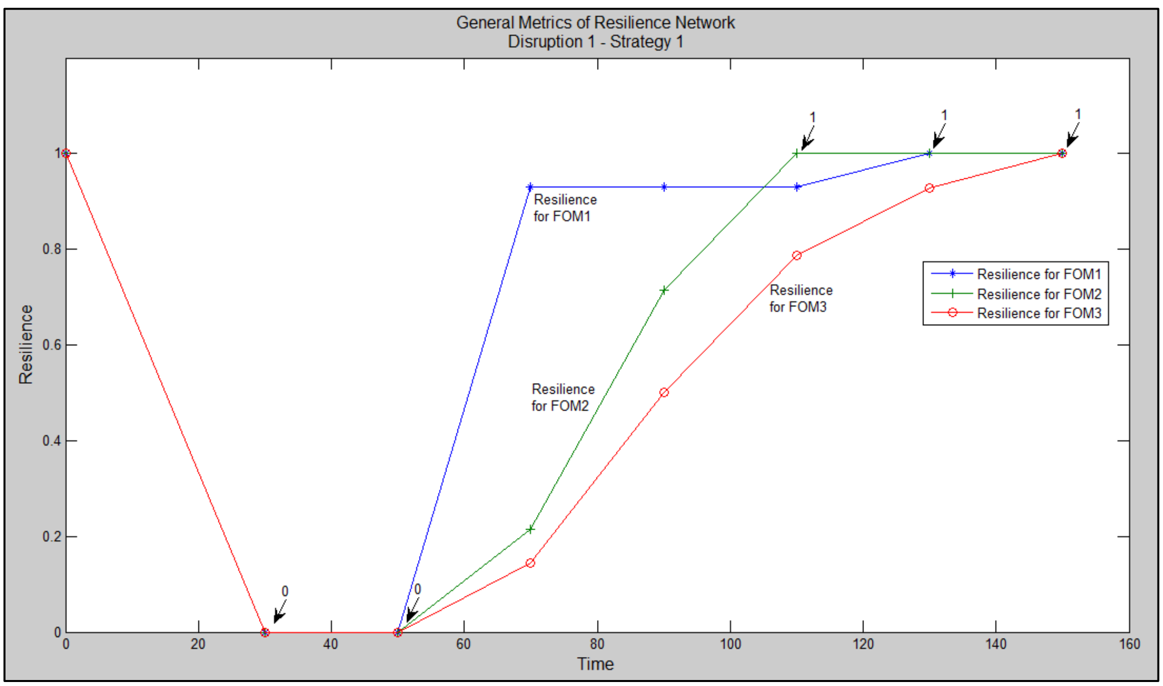

Figure 3.4 Resilience action for Disruption 1 – Strategy 1

As we discussed earlier in section 3.7, Strategy 2 for 1st disruptive event occurs in reverse order link recovery time. Figure 3.5 illustrates the network resilience build up for Strategy 2 – Disruption 1. It is now vaguely clear that Strategy 1 is better for FOM 1 than

Strategy 2. It will be tough to conclude about FOM 3, since both strategies are following similar trends. Hence it will be too early to conclude about which strategy will be better to implement for optimal network resilience build up. Figure 3.6, 3.7 and 3.8 will discuss the applicability of implementing the strategies based upon minimal network resilience and total restoration time for 1st disruption.

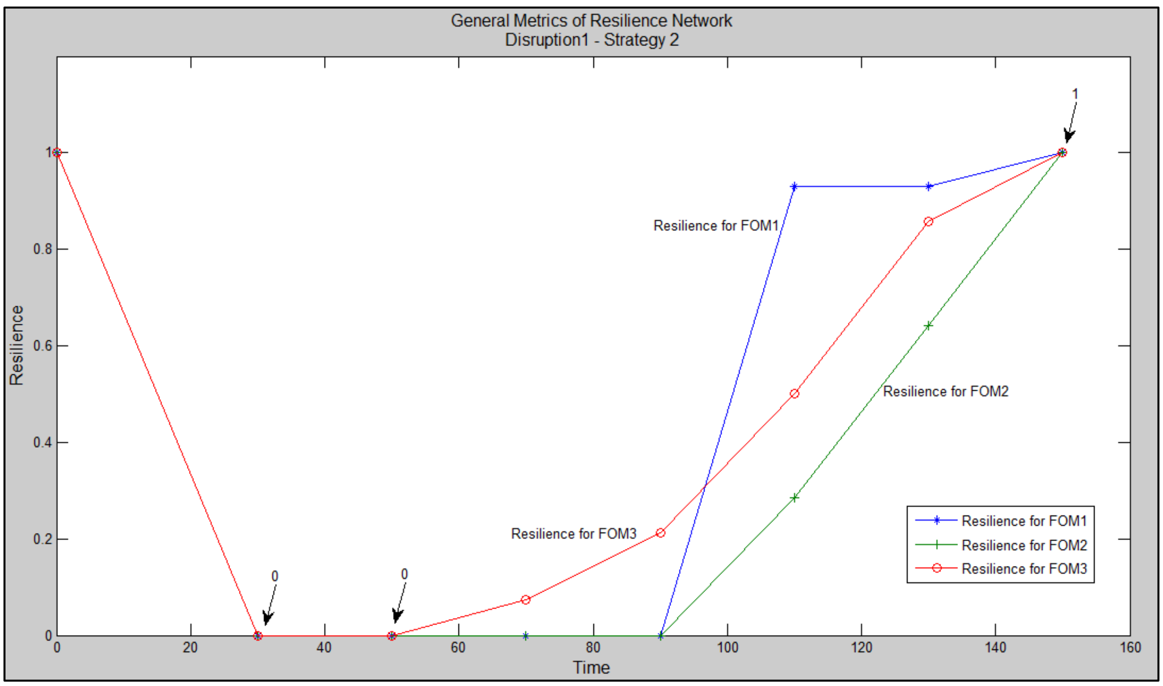

Figure 3.5 Resilience action for Disruption 1 – Strategy 2

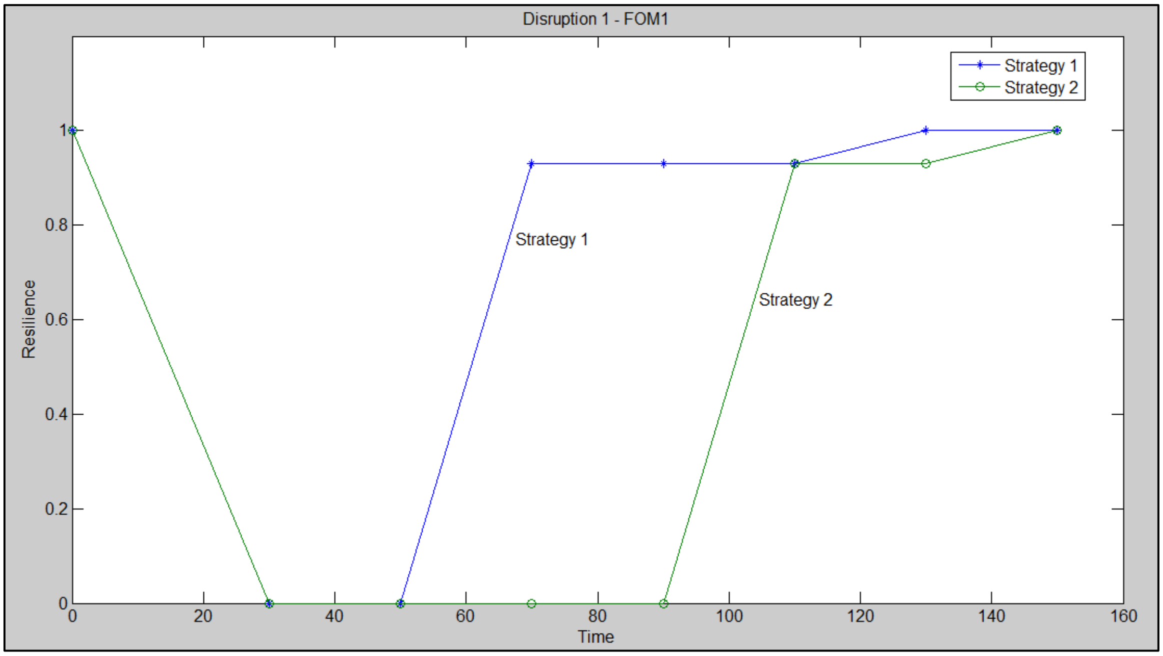

Figure 3.6 Comparing Strategies for 1st disruptive event: FOM 1

Now it is clear from Figure 3.6 that resilience action and network restoration is better when Strategy 1 is applied for FOM 1 than Strategy 2. The network resilience is not only faster as compared to Strategy 2 but also it starts at very early time when Strategy 1 is implemented.

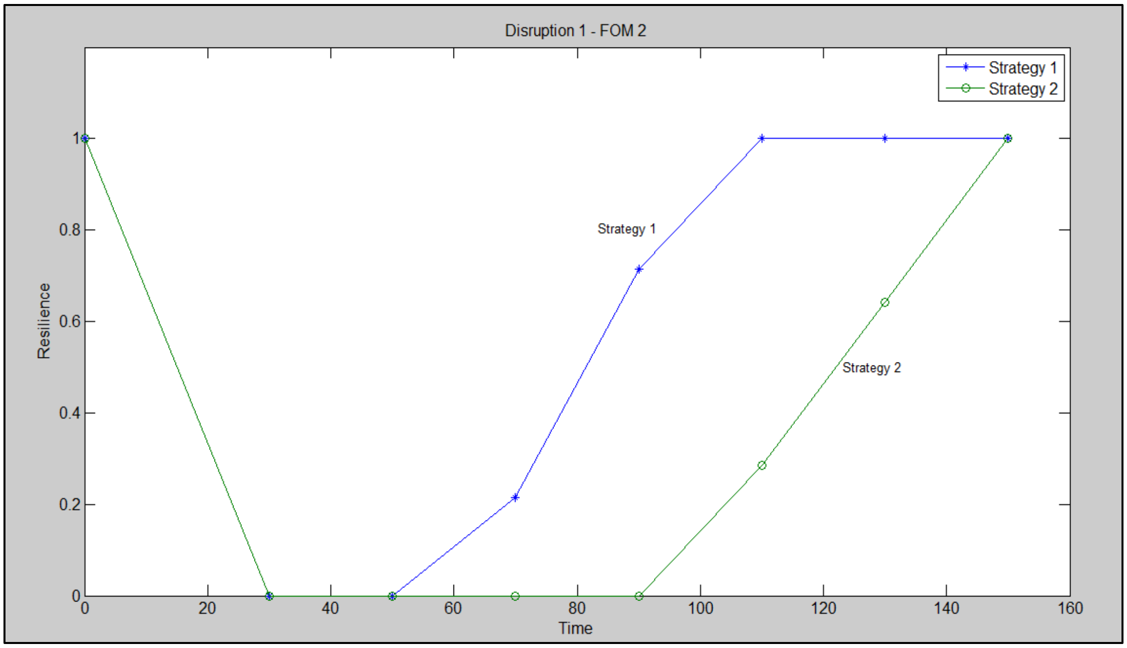

Figure 3.7 Comparing Strategies for 1st disruptive event: FOM 2

Again Strategy 1 is proving to be efficient and faster with respect to Strategy 2, regarding network resilience and full network restoration. In fact, when Strategy 1 is implemented for FOM 2 which is maximum flow, the network resilience and full service capability are achieved after three links are recovered. While for Strategy 2 it requires complete 5 links to recover to the full service capacity and the time required for network resilience build up is also too long.

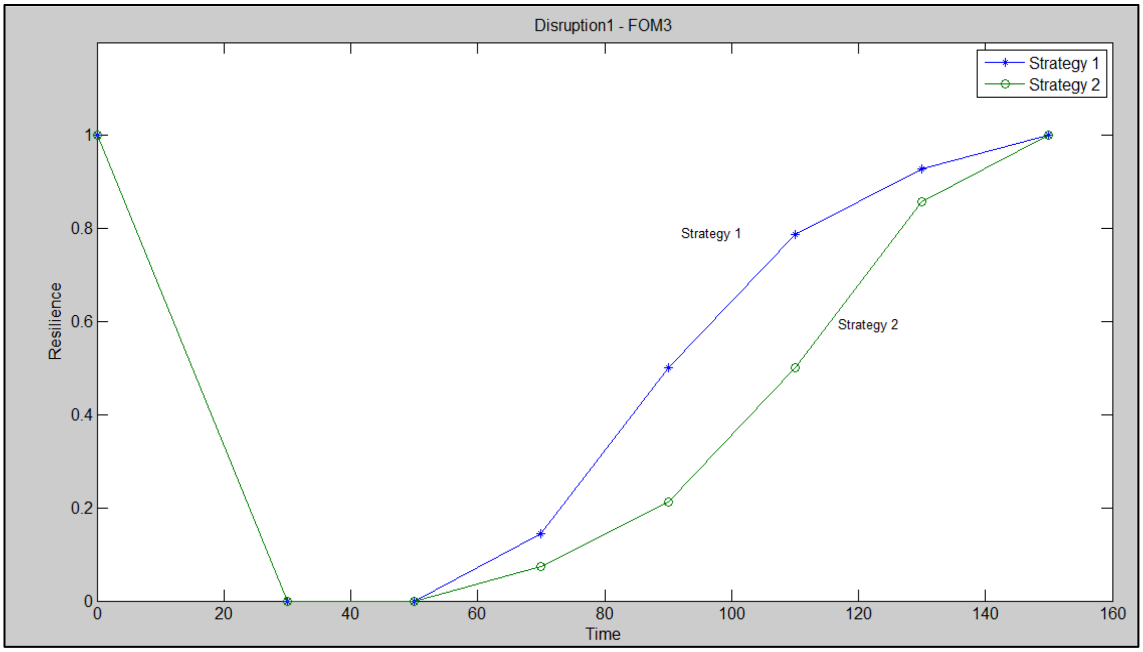

Figure 3.8 Comparing Strategies for 1st disruptive event: FOM 3

In Figure 3.8 both strategies are utilizing the same amount of time for network resilience build up. However, if "bounce back" ability of the system is a concern, Strategy 1 will be better for FOM 3 in 1^{st} disruptive event.

Similarly, following the procedure that has been implemented to analyze two strategies for 1^{st} disruptive event, graphs are obtained for 2^{nd} disruptive event with the same strategies. The strategies are, Strategy 1: Link recovery time is assumed in a queue as of the failures in disruptive event and Strategy 2: Link recovery time is assumed to be in reverse direction as of the failures. Figure 3.9, 3.10 and 3.11 are comparing the results obtained after implementing both strategies for FOM 1, FOM 2 and FOM 3 in 2^{nd} disruptive event.

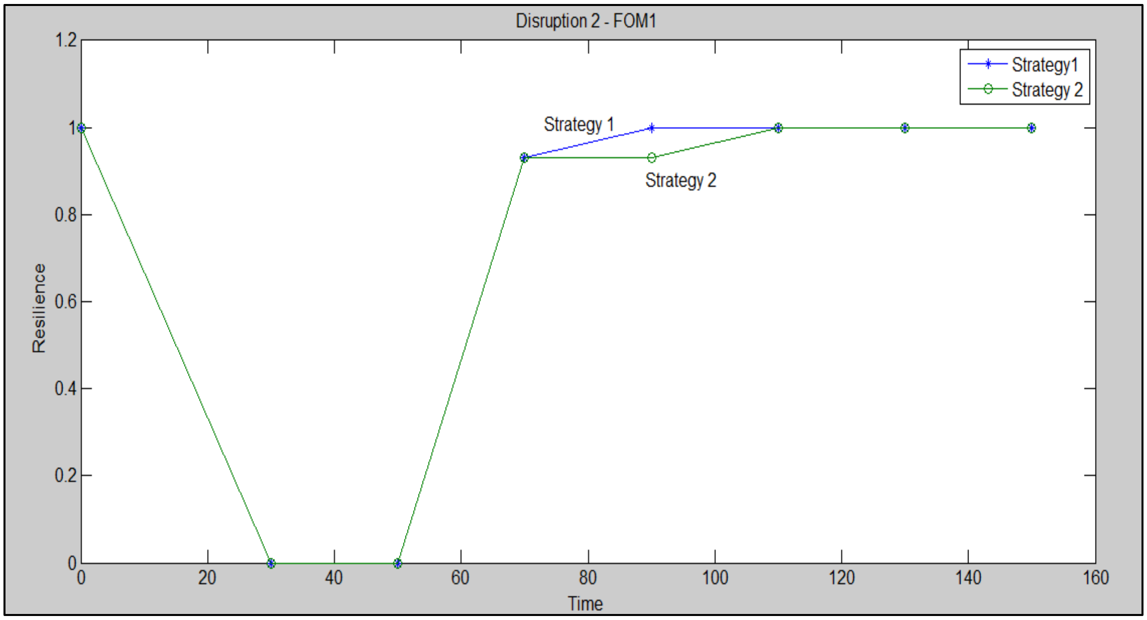

Figure 3.9 Comparing Strategies for 2nd disruptive event: FOM 1

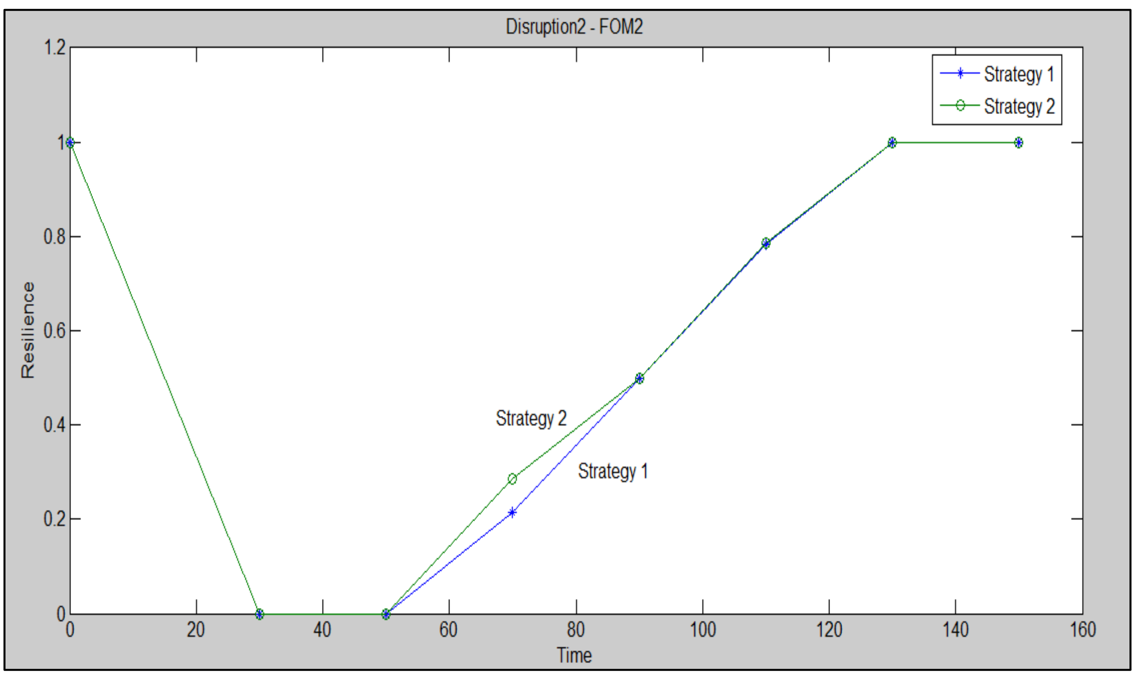

Figure 3.10 Comparing Strategies for 2nd disruptive event: FOM 2

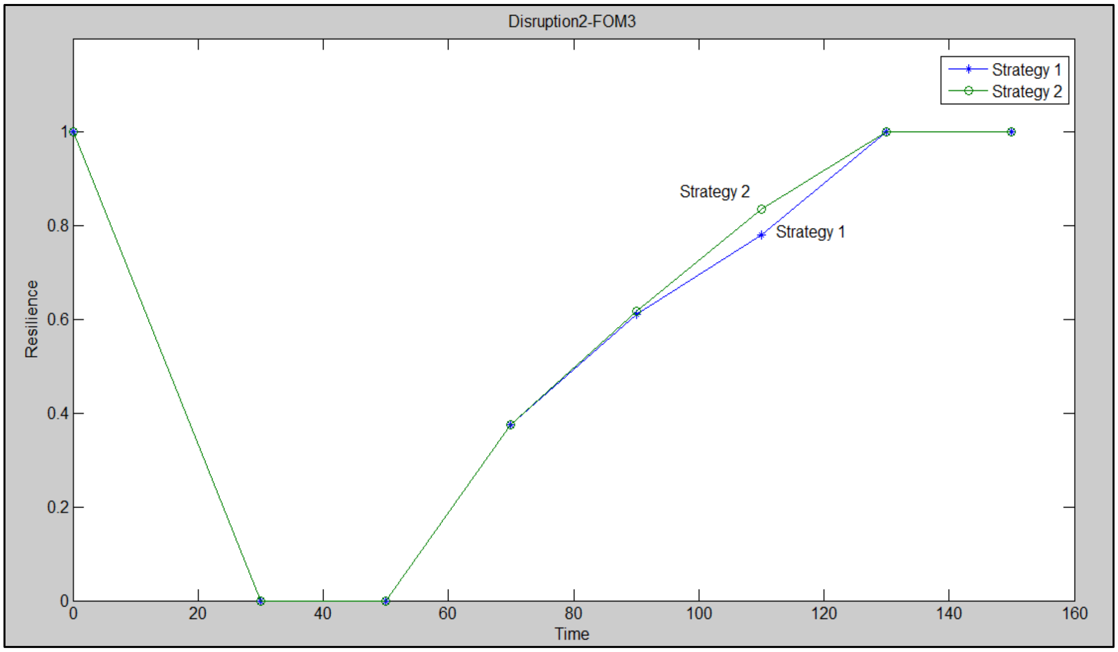

Figure 3.11 Comparing Strategies for 2nd disruptive event: FOM 3

In 2nd disruptive event, both strategies follow very similar trend for each of the considered FOMs. One reason might be the fact that this disruption does not include source and sink. The complete disruption occurs when all the FOMs reaches the worst case scenario at t_d . But all the links are having equal importance. In this case, the failure order queue or reverse order queue does not matter. Strategy 2 is better for FOM 3, since network resilience builds up a bit faster than Strategy 1.

3.8.2. Non-deterministic Time Resilience Analysis. 1000 iteration discrete event simulation is performed while considering uniform time distribution between (8, 12) as individual arc recovery time. It is observed that first three links are responsible for full network service capability. Hence total time span for simulation is in the range of (24, 36). Figure 3.12 illustrates the approximate pdf and figure 3.12 explains cdf of the simulation. The service function or Figure of Merit is maximum flow and 1st disruptive event implementing Strategy 1 is taken into consideration while obtaining the results.

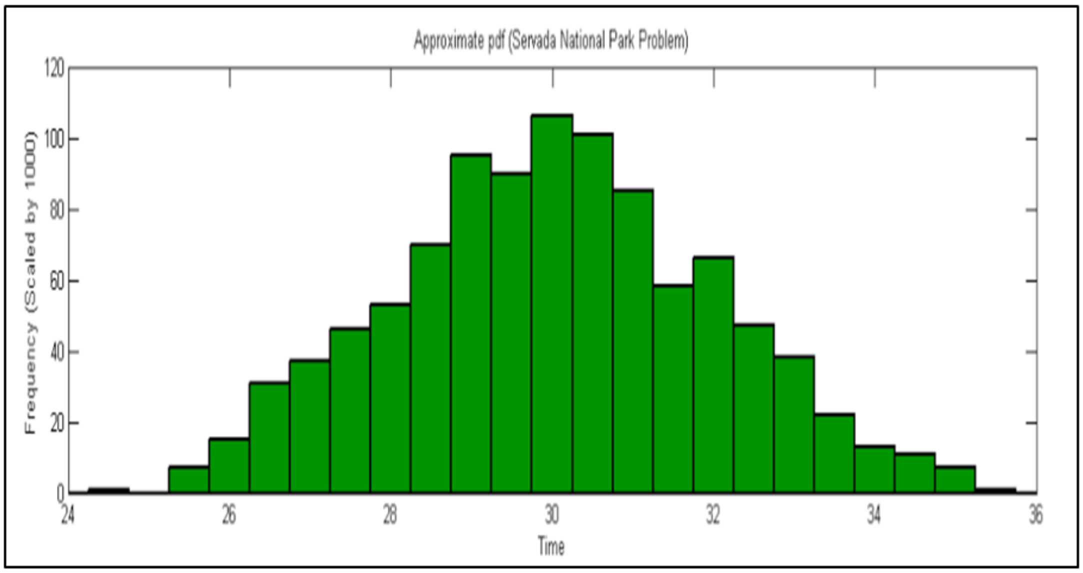

Figure 3.12 Probability distribution histogram

Note that the time to full network resilience is not equal to the time to full network restoration. 36 units indicate recovery of three links which denotes that the system resilience is fully functional. Whereas the complete capacity of the system will be achieved when all the 5 links will be recovered from disruption.

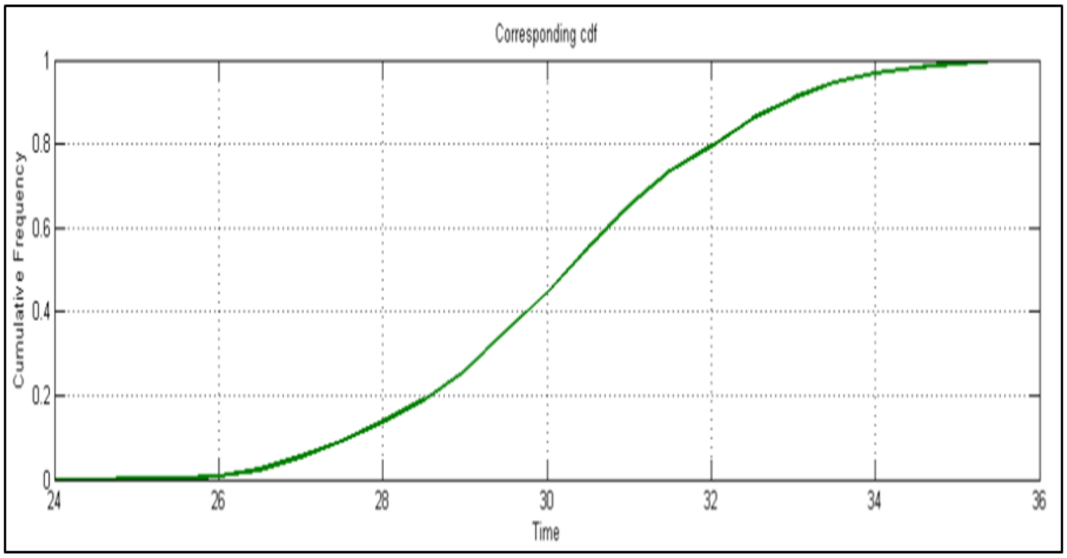

Figure 3.13 Approximate cumulative distribution function

3.8.3. Vulnerability Analysis for Component Importance Ranking. 1st disruptive event is used to analyze component importance. MATLAB program is developed to rank component importance according to system vulnerability against component or link survivability. Maximum flow is considered as FOM. Modifications have been done to implement maximum flow in a uniformly increasing manner. For example, link OA has a flow rate of 7. When the disruption occurs, it is assumed that at a particular instance only one link is completely failed in a uniformly distributed manner. The system vulnerability is calculated by the following equation:

$$V_j^s = \frac{M - D}{M} \qquad (5)$$

where,

V_j^s represents system vulnerability due to j^{th} disruptive event.

M represents FOM at initial state (undisrupted state).

D represents disrupted FOM due to the component failure.

Instead of considering direct FAIL/STABLE (0/1) state, the disrupted FOM (D) will increase uniformly as we uniformly increase the link capacity, Figure 3.14 illustrates the flow reduction of the system as a function of link survivability.

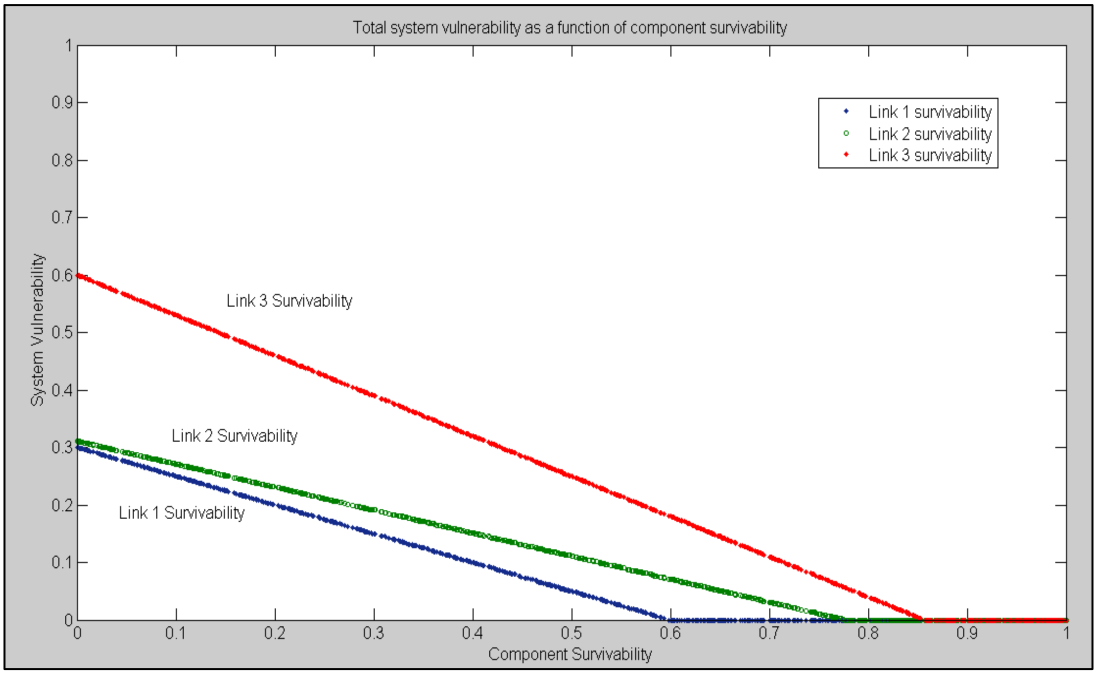

Figure 3.14 Total system vulnerability as a function of individual component survivability

This particular graph on Figure 3.14 is appealing for analysis. Y coordinate represents system vulnerability and X coordinate represents decreasing order of component vulnerability. Figure 3.14 indicates that link 3 produces largest loss of functionality or vulnerability. Here, although link 1 and 2 have low initial loss, but the system resilience recovers faster as the link is getting back to its original state, whereas, link 3 is not contributing to system network resilience. Hence the ranking should be prioritized according to the need and application, and the prudent choices are faster network resilience or lesser system vulnerability.

4. POWER SYSTEM RESILIENCE SIMULATION AND ANALYSIS

A nine-bus power system network of an electrical utility is shown in Figure 4.1. The load data is tabulated in Table 4.1. Voltage magnitude, generation schedule, the reactive power limits for the regulated buses and impedance line data are also shown in Table 4.2, and Table 4.3. Bus 1 is taken as the slack/reference bus.

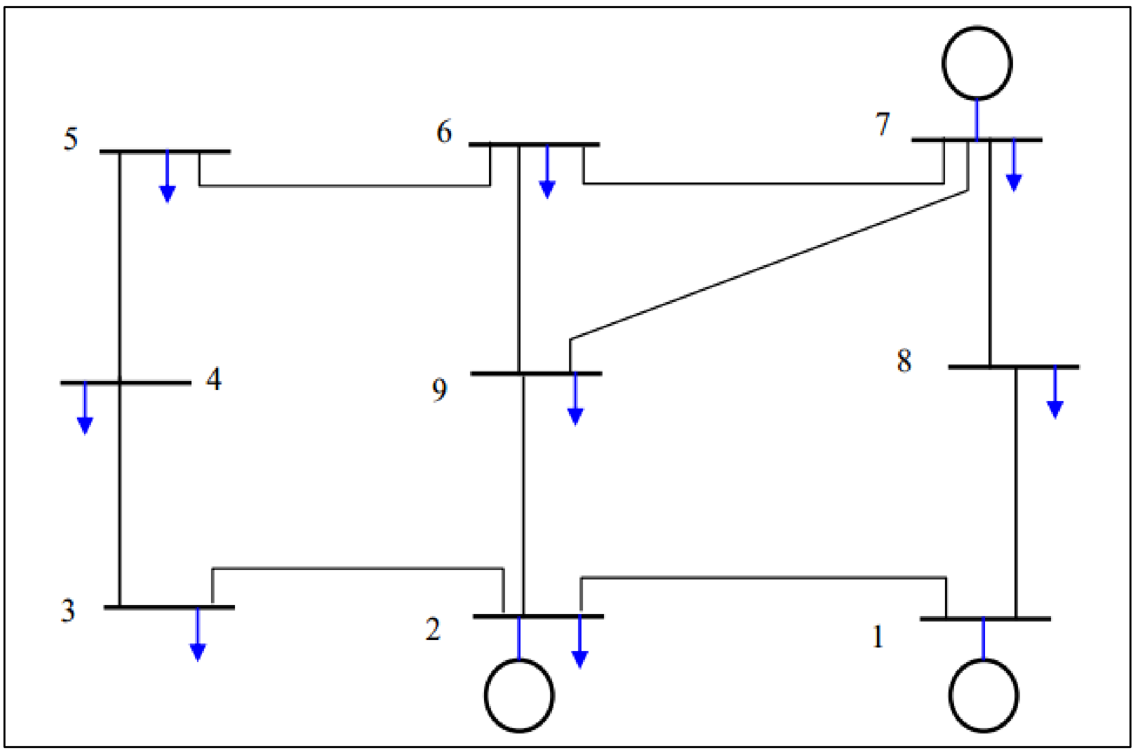

Figure 4.1 Nine-bus power system network of an electric utility

Power World Simulator 17 software [20] is used to carry out power flow analysis which is used to decide the figures of merit and resilient strategies. Contingency analysis is carried out with a combination of three transmission lines failure on a common bus to observe the maximum violations considering the worst disruptive event. In three-line contingency analysis there were some other combinations of three line outages, but the violations were less and the intensity of violations in line limits and drop in bus voltages were severe in case of only both considered disruptive events. With the reference of results obtained in three-line contingency analysis, following two disruptive events are decided.

1) Open line 1-2, 2-3 and 2-9 resulting into 11 violations (7 voltage and 4 power flow)
2) Open line 1-2, 1-8 and 2-9 resulting into 10 violations (6 Voltage and 4 power flow)

Table 4.1 Load data of nine-bus power system example

Load Data		
	Load	
Bus #	MW	Mvar
1	0	0
2	20	10
3	25	15
4	10	5
5	40	20
6	60	40
7	10	5
8	80	60
9	100	80

Table 4.2 Generation data and reactive power limits of voltage regulated and slack bus

Generation Data				
Bus #	|V| pu	P_G (MW)	Q_{min} (Mvar)	Q_{max} (Mvar)
1	1.03		-150	300
2	1.04	80	0	250
7	1.01	120	0	100

Table 4.3 Line data of nine-bus power system example

Line Data				
From	**To**	**R**	**X**	**B**
Bus	**Bus**	**pu**	**pu**	**pu**
1	2	0.018	0.054	0.0090
1	8	0.014	0.036	0.0060
2	9	0.006	0.030	0.0056
2	3	0.013	0.036	0.0060
3	4	0.010	0.050	0.0000
4	5	0.018	0.056	0.0000
5	6	0.020	0.060	0.0000
6	7	0.015	0.045	0.0076
6	9	0.002	0.066	0.0000
7	8	0.032	0.076	0.0000
7	9	0.022	0.065	0.0000

4.1. ASSOCIATED FOM AND RESILIENCE STRATEGIES

As discussed earlier for the considered disruptive events, though we have 11 and 10 violations, they are only used to decide the disruptive events and not the FOM. The violations are bus voltage and transmission line flow. Hence the maximum violation in line flow and maximum violation in bus voltage are assumed FOMs. For 1st disruptive event, FOM 1 is line flow from bus 1 to bus 8. Since, the results in contingency analysis showed that for three-line disruptions, the maximum line flow violation occurs at line 1-8 with 307 % exceeding the rated apparent power limit of 120MVA. FOM 2 is considered as a low bus voltage at bus 9. Bus 9 consists of maximum load and line 2-9 is considered in both the disruptive events. Also, line 2-9 is a part of maximum violations in three-line contingency. Low bus voltage at bus 9 is 0.6p.u during three-line disruptions for 1st disruptive event.

Two strategies are considered to carry out the resilience action.

1) Recovery of lines 2-9, 2-3 and 1-2 in a queue
2) Recovery of lines 2-9, 2-3 and 3-4 in a queue

Eqn. (4) is used to calculate both FOMs. FOM 1 at reliable state is 81% of rated transmission flow in line and FOM 2 at reliable state is 1.0p.u voltage at bus 9, i.e. 138kV nominal voltage.

4.2. DETERMINISTIC TIME RESILIENCE EVALUATION

Table 4-3 describes network behavior under 1st disruptive event – strategy 1 and Table 4.4 illustrates the calculations of associated FOMs at different time. Since the MVA limit for every line is constant (120 MVA), the recovery time is assumed to be equal which is 10 units for the considered open lines.

Table 4.4 Transmission line behavior under Disruption 1 - Strategy 1

Transmission line	Network Status					
	t_0	t_d	t_s	t_1	t_2	t_f
2-9	1	0	0	1	1	1
2-3	1	0	0	0	1	1
1-2	1	0	0	0	0	1

Table 4.5 utilizes the similar approach of finding out associated FOMs as described in chapter 3. Provided all the FOMs are properly defined as per the resilience theory, we can use similar resilient strategies.

Table 4.5 Resilience computations of power network for Disruption 1 - Strategy 1

Time	Network Status					
	t_0	t_d	t_s	t_1	t_2	t_f
FOM 1	81	307	307	133	131	81
Rf1	1	0	0	0.7699	0.7789	1
FOM 2	1	0.6	0.6	1	1	1
Rf2	1	0	0	1	1	1

Similarly, Strategy 2 is developed and resilience calculations are tabulated in table 4.6 and 4.7 respectively.

Table 4.6 Transmission line behavior under Disruption 1 - Strategy 2

Transmission line	Network Status					
	t_0	t_d	t_s	t_1	t_2	t_f
2-9	1	0	0	1	1	1
1-2	1	0	0	0	1	1
2-3	1	0	0	0	0	1

Table 4.7 Resilience computations of power network for Disruption 1 - Strategy 2

Time	Network Status					
	t_0	t_d	t_s	t_1	t_2	t_f
FOM 1	81	307	307	133	90	81
Rf1	1	0	0	0.7699	0.96	1
FOM 2	1	0.6	0.6	1	1	1
Rf2	1	0	0	1	1	1

2nd disruptive event, as discussed earlier, is complete outage of line 2-9, 2-3 and 3-4. Again FOM 1 is considered as line flow in line 1-8 and FOM 2 is low bus voltage at bus 9 for the same reason justified at the time of 1st disruptive event. Following resilient strategies are decided for resilience build up:

1) Recovery of lines 2-9, 2-3 and 3-4.

2) Reverse order recovery.

FOM 1 at 2nd disruptive event is 244% of MVA rating for line 1-8 and FOM 2 is 0.71p.u. The reliable states for FOM 1 and FOM 2 are 81% are 1p.u respectively. Table 4.8 describes network behavior under 2st disruptive event – Strategy 1 and Table 4.9 illustrates the calculations of associated FOMs at different time. Again recovery of 10 units is assumed for deterministic resilience calculations.

Table 4.8 Transmission line behavior under Disruption 2 - Strategy 1

Transmission line	Network Status					
	t_0	t_d	t_s	t_1	t_2	t_f
2-9	1	0	0	1	1	1
2-3	1	0	0	0	1	1
3-4	1	0	0	0	0	1

Table 4.9 Resilience computations of power network for Disruption 2 - Strategy 1

Time	Network Status					
	t_0	t_d	t_s	t_1	t_2	t_f
FOM 1	81	244	244	82	86	81
Rf1	1	0	0	0.9938	0.969	1
FOM 2	1	0.71	0.71	1	1	1
Rf2	1	0	0	1	1	1

Similarly Table 4.10 represents network behavior for 2nd strategy and Table 4.11 represents resilient computations.

Table 4.10 Transmission line behavior under Disruption 2 - Strategy 2

Transmission line	Network Status					
	t_0	t_d	t_s	t_1	t_2	t_f
3-4	1	0	0	1	1	1
2-3	1	0	0	0	1	1
2-9	1	0	0	0	0	1

Table 4.11 Resilience computations of power network for Disruption 2 - Strategy 2

Time	Network Status					
	t_0	t_d	t_s	t_1	t_2	t_f
FOM 1	81	244	244	240	127	81
Rf1	1	0	0	0.0243	0.7171	1
FOM 2	1	0.71	0.71	0.78	0.9	1
Rf2	1	0	0	0.241	0.655	1

4.3. NONDETERMINISTIC TIME RESILIENCE EVALUATION

As described in section 3.7.4.2, 10000 events Discrete Event Simulation is programmed in MATLAB. Uniform distribution between time (6, 14) is considered as link recovery time for disrupted transmission lines. The recovery time is uniformly distributed for the same time period because of the same MVA rating. Again for the sake of avoiding redundancy in the results, 1st disruptive event and Strategy 1 is simulated. Approximate probability distribution and cumulative distribution function are plotted for resilience action as function of probabilistic time.

4.4. SIMULATION RESULTS AND ANALYSIS

The calculated tables of resilience actions for deterministic approach and both strategies are compared to analyze which strategy is better for a particular disruptive event.

4.4.1. Deterministic Time Resilience Power Network Analysis. Figure 4.2 illustrates the effect of implementing Strategy 1 and Strategy 2 for 1st disruptive event.

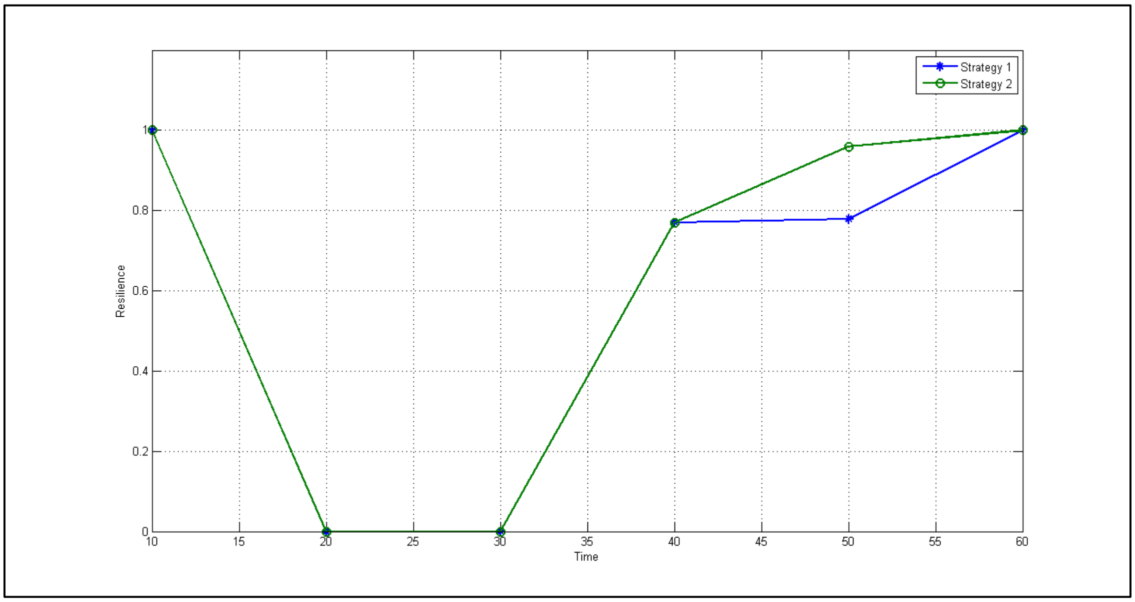

Figure 4.2 Comparing strategies of power network for FOM 1: 1st disruptive event

From the graph it is clear that when both the strategies are implemented, line 2-9 recovery is very crucial in resilience action for FOM 1. Strategy 2 proves to be a better option for resilience build up. After line 2-9 is recovered the line limit in 1-8 drops down to 133% from 307%, giving the resilience value of 0.8 approximately.

Figure 4.3 describes comparison of both strategies for FOM 2 in 1st disruptive event.

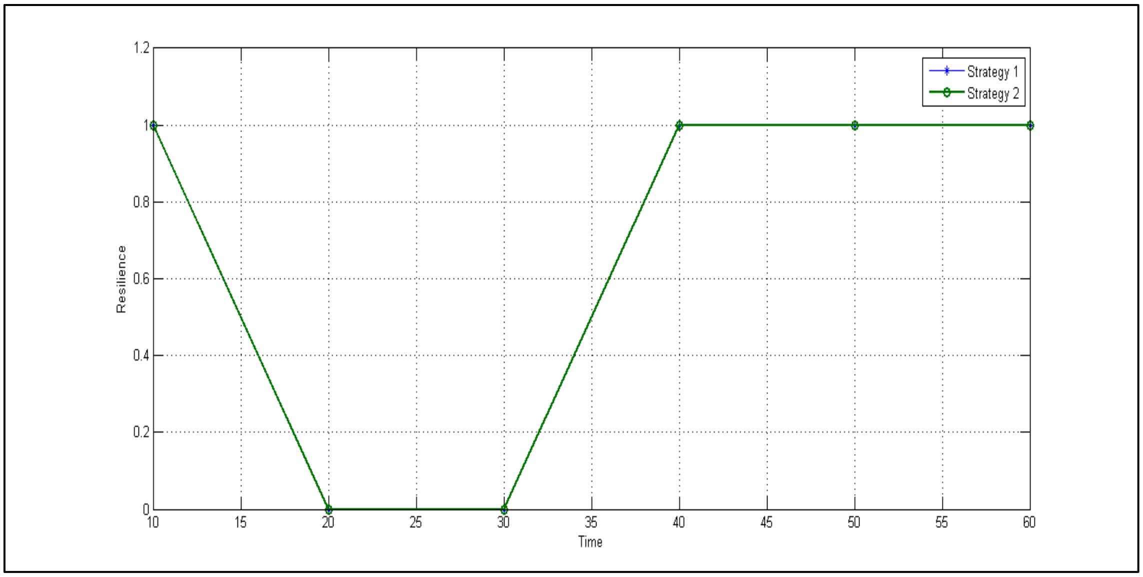

Figure 4.3 Comparing strategies of power network for FOM 2: 1st disruptive event

Both the strategies are behaving in the same form for resilience build up. Hence, one thing is concluded that line 2-9 is crucially important when both of the strategies are implemented and line 2-3 and 1-2 are both equally important for FOM 2. But at the time of disruption, both FOMs are disrupted with equal significance. Hence, Strategy 2 proves to be a better option for 1st disruptive event.

Similar results were depicted in Figure 4.4 and Figure 4.5 for 2nd disruptive event and two defined strategies.

.

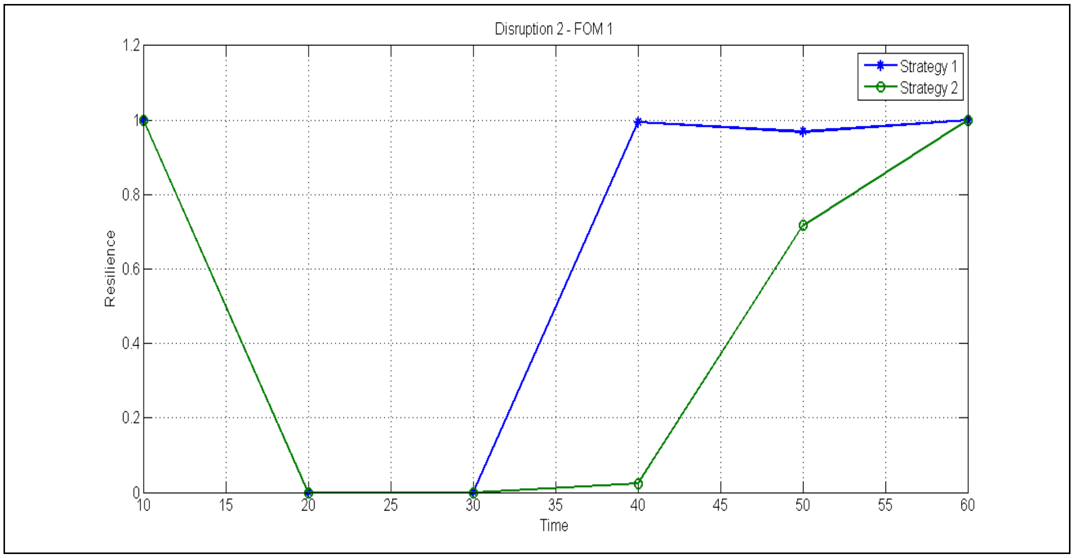

Figure 4.4 Comparing strategies of power network for FOM 1: 2nd disruptive event

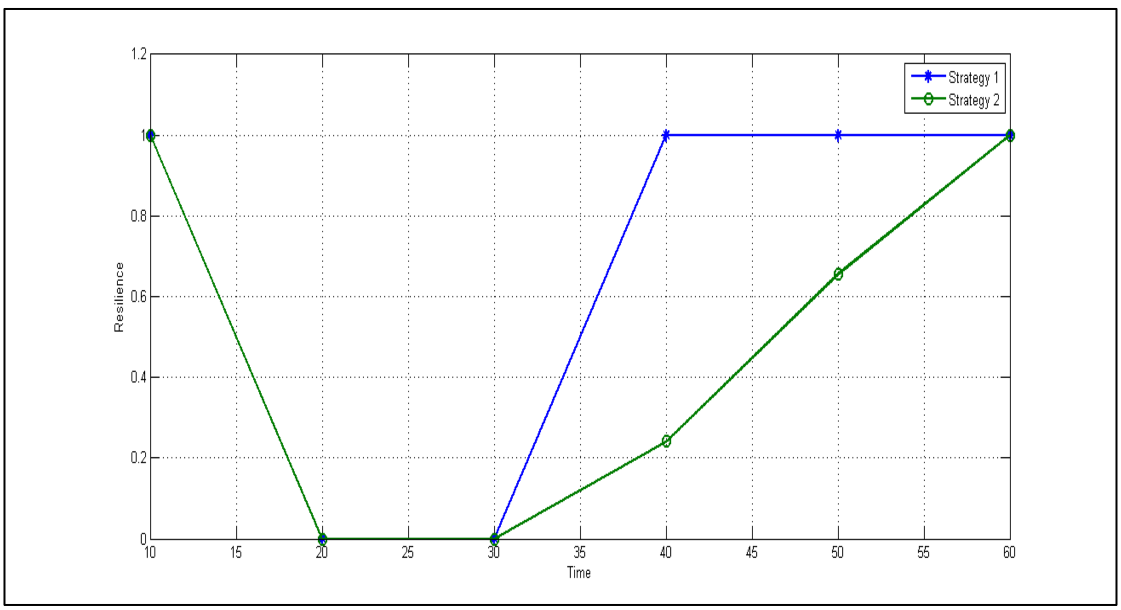

Figure 4.5 Comparing strategies of power network for FOM 2: 2nd disruptive event

Figure 4.4 and Figure 4.5 gives a clear indication of the fact that strategy 1 implemented for 2nd disruptive event is better than strategy 2. Note that in strategy 1, initial recovery of line 2-9 is the cause to build resilience faster. In strategy 2, initial recovery of line 2-9 is not accounted, which is the reason for slower resilience build up as compared to strategy 1.

4.4.2. Nondeterministic Time Resilience Power Network Analysis. 10000 events discrete event simulation is carried out in MATLAB to plot the probability distribution function and cumulative distribution function for network resilience. The total time to resilience is equal to total time to restoration which is bounded in (18, 42). Figure 4.6 and Figure 4.7 describes the pdf and cdf of the network resilience build up as a function of nondeterministic time. The assumed service function to plot these curves is line limit of 1-8 for first disruptive event.

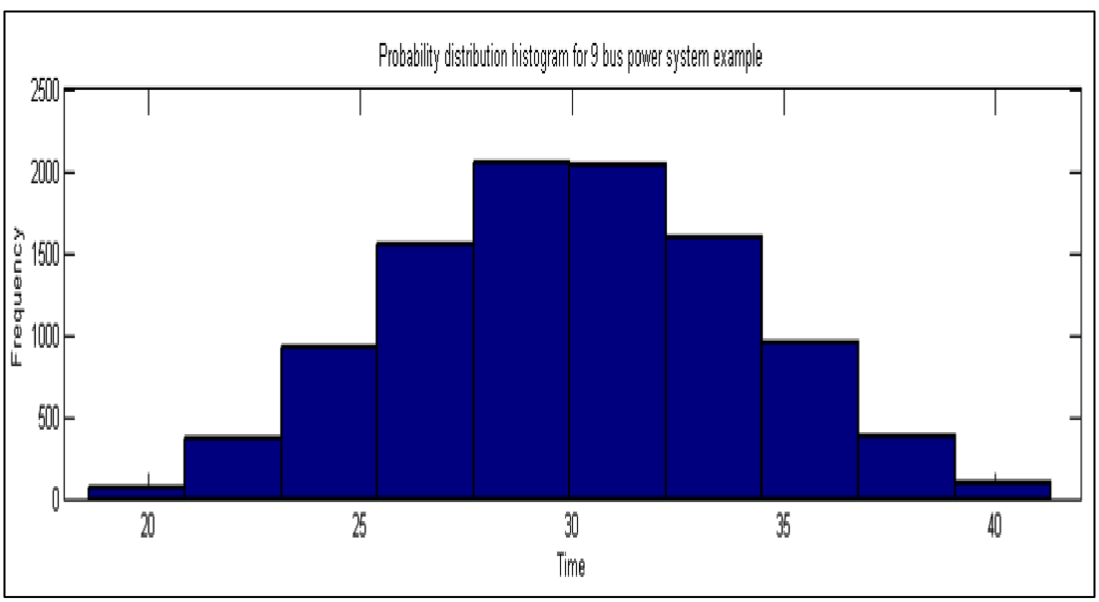

Figure 4.6 Probability distribution histogram for nine-bus power system example

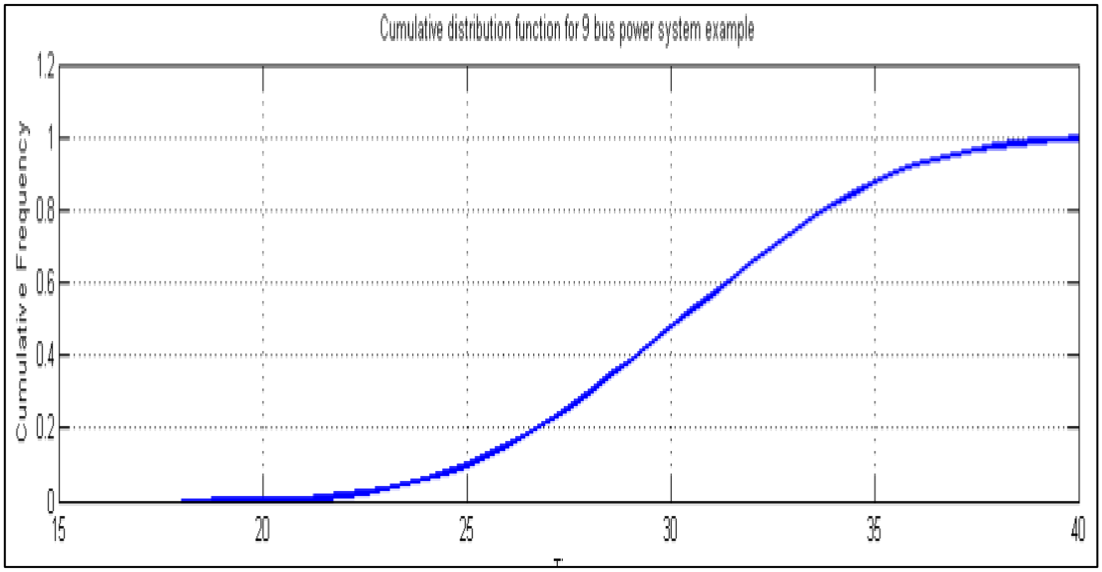

Figure 4.7 Cumulative distribution histogram for nine-bus power system example

5. CONCLUSIONS AND FUTURE SCOPE

The research presented in the thesis provides a background for the consideration of network resilience, which is against the conventional reliability and network protection and disruption prevention studies. Network resilience analysis is crucial to assurance of critical infrastructure systems and hence there is a need to address the concern of ability of a system to “bounce back” from the disruption to its full service capability.

In this thesis, resilience metrics is discussed in detail to provide a theoretical background for the application of these metrics in power systems resilience analysis. Initial studies in network resilience deal with the theoretical aspects and not the applications. One of the future works of these studies is to apply concepts of network resilience in any considered domain provided proper service function or figure of merits and resilient strategies are defined. A nine-bus power system transmission and large load network is used to determine the recovery of the system from worst disruption. Deterministic and nondeterministic approaches are considered to recover the transmission links. One of the major contributions of the thesis is the importance measure according to strategies adopted for network resilience. Once the strategies of a particular disruptive event and service function is decided, then the recovery time for faster resilience build up can determine the strategy which should be adopted for a particular service function.

Several restoration strategies are considered and compared. New technique of vulnerability analysis to rank component importance paved a way for importance measure. For this purpose, instead of conventional 0 and 1 as fail and restore scenario, the thesis proposes to gradually increase the link recoverability. The system vulnerability is calculated as a function of stochastic link survivability. Due to each single line recovery, the link or component importance has been weighted according to the faster system recoverability.

Important future work as an extension to the present work will be including FACTS devices at the most vulnerable node. In resilient point of view, it will be the node with the worst disruption. Hence if the links at vulnerable node is causing an adverse effect on system vulnerability, FACTS devices will help to recover the system disruption and thereby improving network resilience with or without recovering a particular transmission line. Hence ranking FACTS devices according to component importance measure will be a significant advancement of the current work. A more complex approach may be implemented to amalgamate FACTS devices to a higher level power system in order to give practical orientation in complement with the present work.

Another important extension to the work may include cost assessment of losses due to system deterioration. Proper allocation of resources may help to build network resilience faster and thus reducing system vulnerability. As described in present work, the network resilience approach can be applied to any domain including telecommunication networks, intelligent water distribution networks and power line communication networks; provided proper figures of merit, disruptive events and resilient strategies are developed.

Power outages and disruptions in complex systems are not completely eradicated and steps must be undertaken to analyze recoverability after such disruptions. This thesis is a step towards explaining and implementing most of the resilience metrics in power domain. The proposed analysis provides a framework for decision support in fortification and restoration efforts.

BIBLIOGRAPHY

[1] Z. W. Birnbaum, "On the importance of different components in a multicomponent system," *In P. R. Krishnaiah, editor,Multivariate Analysis -II*, pp. 581-592, 1969.

[2] R. M. Fricks and K. S. Trivedi, "Importance Analysis with Markov Chains," in *PROCEEDINGS AnnualRELIABILITY AND MAINTAINABILITY Symposium*, 2003.

[3] W. Wang, J. Loman and P. Vasiliou, "Reliability Importance of Components in a Complex System," in *Reliability and Maintainability, 2004 Annual Symposium - RAMS*, 2004.

[4] C. S. Holling, "Resilience and stability of ecological systems," *Annual Review of Ecology and Systematics* , vol. 4, pp. 1-23, 1973.

[5] Y. Y. Haimes, K. Crowther and H. B. M, "Homeland security preparedness:balancing protection with resilience in emergent systems," *Systems Engineering*, vol. 11, no. 4, pp. 287-308, 2010.

[6] D. Henry and J. E. Ramirez-Marquez, "Generic metrics and quantitative approaches for system resilience as a function of time," *Reliability Engineering and System Safety*, pp. 114-122, 2012.

[7] K. Barker, J. E. Ramirez-Marquez and C. M. Rocco, "Resilience-based network component importance measures," *Reliability Engineering and System Safety*, pp. 89-97, 2013.

[8] M. Moghavvemi and O. Faruque, "Real-time contingency evaluation and ranking technique," *Generation, Transmission and Distribution, IEE Proceedings*, vol. 145, no. 5, pp. 517-524, 1998.

[9] C. Paolo, V. Latora and M. Marchiori, "Locating critical lines in high volatge electrical power grids," *Worl Scientific Fluctuations and Noise Letters*, pp. L201-L208, 2005.

[10] R. N. Allan, R. Billinton, I. Sjarief, L. Goel and K. S. So, "A reliability test system for educational purposes basic distribution system data and results," *IEEE Transactions on Power Systems*, vol. 6, no. 2, pp. 813-820, 1991.

[11] A. A. Alkuhayli, "Reliability Evaluation Of Distribution Systems Containing Renewable Distributed Generations," Missouri University of Science and Technology, Rolla, 2012.

[12] L. Husshi, S. Jian and L. Sige, "Reliability evaluation of distribution system containing Microgrids," *China International Conference Electricity Distribution (CICED)*, pp. 1-6, 2010.

[13] I. Bae and K. J, "Reliability evaluation of customers in a microgrid," *IEEE Transactions on Power Systems*, vol. 23, no. 3, pp. 1416-1422, 2008.

[14] S. A. C. Juliano and L. Ferrarini, "Reliability Analysis of Power System based on Generalized Stochastic Petri Nets," in *Proceedings of the 10th International Conference on Probabilistic Methods Applied to Power Systems*, 2008.

[15] M. Dumitrescu, "Stochastic Petri Nets Architectural Modules for Power System Availability," in *The 9th IEEE International Conference on Electronics, Circuits and Systems*, 2002.

[16] S. C. White and S. Sedigh, "Evaluating and Modeling Security with Petri Nets," *In preparation 2013*.

[17] A. Faza, "Reliability Modeling for the Advanced Electric Power Grid," Missouri University of Science and Technology, Rolla, 2007.

[18] A. Lininger, B. McMillin, M. Crow and B. Chowdhury, "Analysis of max-flow values for setting FACTS devices," in *Power Symposium, 2007. NAPS '07. 39th North American*, 2007.

[19] J. Chaloupek, D. R. Tauritz, B. McMillin and C. M, "Evolutionary optimization of flexible ac transmission system device placement for increasing power grid reliability," *Proceedings of the 6th International Workshop on Frontiers in Evolutionary Algorithms (FEA '05),* pp. 516-519, 2005.

[20] "Power World Contingency Analysis Video Tutorial," *http://www.powerworld.com/training/online-training/contingency-analysis/September 2013*.

[21] A. J. Wood and B. F. Wollenberg, POWER GENERATION, OPERATION, AND CONTROL, New York: John Wiley & Sons, Inc., 1996.

[22] K. S. Trivedi, Probability & Statistics With Reliability, Queuing And Computer Science Applications, New York: John Wiley and Sons Inc., 2008.

VITA

Kamlesh Ashok Joshi was born in Aurangabad, Maharashtra India. He received his primary and secondary education in Aurangabad, India graduating from Saraswati Bhuvan Prashala Aurangabad. Kamlesh received his Bachelor's degree in Electrical, Electronics and Power Engineering from Government College of Engineering Aurangabad (GCOE-Aurangabad), an autonomous institute of Government of Maharashtra. He received his Master of Science degree in Electrical Engineering from Missouri University of Science and Technology in May 2014. He is working as an Electrical Engineer-I with Black & Veatch at Overland Park, Kansas.