Cascading Events in the Aftermath of a Targeted Physical Attack on the Power Grid

Rounak Meyur

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

Master of Science
in
Electrical Engineering

Virgilio A. Centeno, Chair
Vassilis Kekatos
Madhav V. Marathe

February 22, 2019
Blacksburg, Virginia

Keywords: Cascading failures, targeted attack, hidden failures

Cascading Events in the Aftermath of a Targeted Physical Attack on the Power Grid

Rounak Meyur

(ABSTRACT)

This work studies the consequences of a human-initiated targeted attack on the electric power system by simulating the detonation of a bomb at one or more substations in and around Washington DC. An AC power flow based transient analysis on a realistic power grid model of Eastern Interconnection is considered to study the cascading events. A detailed model of control and protection system in the power grid is considered to ensure the accurate representation of cascading outages. Particularly, the problem of identifying a set of k critical nodes, whose failure/attack leads to the maximum adverse impact on the power system has been analyzed in detail. It is observed that a greedy approach yields node sets with higher criticality than a degree-based approach, which has been suggested in many prior works. Furthermore, it is seen that the impact of a targeted attack exhibits a non-monotonic behavior as a function of the target set size k. The consideration of hidden failures in the protective relays has revealed that the outage of certain lines/buses in the course of cascading events can save the power grid from a system collapse. Finally, a comparison with the DC steady state analysis of cascading events shows that a transient stability assessment is necessary to obtain the complete picture of cascading events in the aftermath of a targeted attack on the power grid.

Cascading Events in the Aftermath of a Targeted Physical Attack on the Power Grid

Rounak Meyur

(GENERAL AUDIENCE ABSTRACT)

The modern day power system has been identified as a critical infrastructure providing crucial support to the economy of a country. Prior experience has shown that a small failure of a component in the power grid can lead to widespread cascading events and eventually result in a blackout. Such failures can be triggered by devastating damage due to a natural calamity or because of a targeted adversarial attack on certain points in the power system. Given limited budget to avoid widespread cascading failures in the network, an important problem would be to identify critical components in the power system. In this research an attempt has been made to replicate the actual power system conditions as accurately as possible to study the impact of a targeted adversarial attack on different points in the network. Three heuristics have been proposed to identify critical nodes in the network and their performance has been discussed. The case studies of cascading events have been performed on a synthetic power system network of Washington DC to achieve the actual system conditions of an operating power grid.

Acknowledgments

I would like to express my heartfelt gratitude to my academic advisor and committee chair Dr. Virgilio Centeno, who has been a source of immense support and inspiration throughout my time at Virginia Tech. His encouragement has been instrumental in my decision to further continue my academic journey towards a doctoral degree.

I would also like to thank Dr. Vassilis Kekatos for the guidance I received as a graduate student and the nurturing ambience I have grown to enjoy in the Power Lab. His classes have not only deepened my understanding of power systems but also sharpened my critical analysis skills.

I thank Madhav for having me in the Network Dynamics and Simulation Science Laboratory. I was privileged to work with a group of world-class researchers and experts on network science. I believe not many power system students have the opportunity of being exposed to a large group of people collaborating on modeling complex network dynamics in graduate school. I will wholeheartedly miss everyone at NDSSL.

I cannot thank Dr Anil Vulikanti enough for patiently teaching me how to approach technical problems in my research and encouraging me throughout my time at NDSSL. I would like to thank Dr. Arun Phadke and late Dr. Jim Thorp for discussions related to problems that I studied in this work. I was fortunate to have worked with such esteemed individuals and learnt a lot from their valuable inputs about my work.

I cherish the friendship of my fellow graduate students Manish, Shuchismita, Aditie, Lasya and Akshay. We started our journey together at Blacksburg and have since charted our different paths, but the first semester here continues to be some of my favorite memories.

My life in Blacksburg would have been quite difficult without a bunch of wonderful people around me. I would like to thank Arindam Fadikar for getting me into atheletics. I would always cherish the memories of half marathon experiences in Columbus and Philadelphia, those tiresome rides on Bike Route 76 and the breathtaking experience of hiking the Grand Canyon together.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Critical infrastructures are defined as *those physical and cyber-based systems essential to the minimum operations of the economy and government* [1]. Since they provide crucial support for the delivery of basic services to almost all segments of society, they are regarded as the backbone of the economy of both developed and developing countries throughout the world. As one of the nation's most complex, large-scale networked systems, electric power has become increasingly automated in the past four decades. However, the increased automation has introduced new vulnerabilities to equipment failures, human errors, weather and other natural causes, and physical and cyber-attacks. The ever-increasing system scale and the strong reliance on automatic devices increase the likelihood of turning a local disturbance into a large-scale cascading failure [2, 3, 4]. This kind of wide-area failure may have a catastrophic impact on the whole society.

In the past there are multiple events where a small failure of a component has led to a large blackout. For example, an incorrect relay setting led to the outage of a heavily loaded 230kV transmission line and eventually resulted in a series of cascading events to cause the well known north-east US blackout of 1965 [5]. The blackout of 1977 was initiated by a lightning strike; however, equipment failures and operator errors escalated disturbances in the grid resulting in a widespread blackout [6]. Recently, failures in the protective systems have been

instrumental in causing large blackouts like the Western Electricity Coordinating Council (WECC) blackouts in 1996 and north-east blackout (2003) [7, 8]. In 2012, India experienced the largest power outage in history and it was initiated by a relay misoperation in one of the heavily loaded lines [9].

The US power system comprises of three large networks, namely the Eastern Inter-connection (EI), the Western Inter-connection (WI), and the Texas Inter-connection (TI). The AC-DC-AC ties among these interconnections limit the spread of disturbance between them. The focus of this study is the impact of a localized but severe event occurring in the EI. The EI stretches from Central Canada Eastward to the Atlantic coast (excluding Quebec), South to Florida and West to the foot of the Rockies (excluding most of Texas). All of the electric utilities in the EI are electrically tied together during normal system conditions and operate at a synchronized frequency averaging around 60Hz [10]. Given the geographic spread of the EI, any terrorist attack on particular substations in the EI will likely span large geographical areas [11]. The premise for this study is to explore the preparedness of the power system to a targeted adversarial attack on substations around Washington DC.

1.2 Contribution

The primary interest of this work is to study the impact of a targeted adversarial attack on different substations in the power system network. The targeted terrorist attack is considered to be a detonation of a bomb at one or more substations located near Washington DC. This scenario depicts an attack that is aimed at harming the power grid and thereby *indirectly* affecting the human populace of the city. Since multiple substations can be targeted at the same time, this attack scenario can also be called a coordinated targeted attack.

The proposed methodology uses prior works to synthesize the power network in the Washing-

ton DC region from publicly available data sources such as Google Maps, ISO manuals and archives, etc. The synthesized data overcomes the problems of confidentiality, anonymity and proprietary concerns. Data driven methods are used to infer the synthetic power network. This network representation, along with the detailed agent-based activity and demand models are used to estimate potential impacts on the power system components. The details of the system as well as the pre-blast power system flows occurring in the vicinity of Washington DC are present in prior works [3, 11, 12, 13].

This work studies the *transient stability* of the power system using the *AC power flow analysis* while considering such human-initiated catastrophic event scenarios. Furthermore, the role of protection systems is considered in this work along with the stochastic occurrence of hidden failures. Therefore, the proposed analysis methodology aims to replicate the actual system conditions precisely. Following such analysis, the interesting problem to solve would be the identification of *optimal critical node set*. These nodes are the ones which when targeted results in the maximum impact. The identification of such nodes can help in protecting the substations from being targets of planned adversarial attacks and thereby saving the power grid from total system collapse. Due to the complex nature of the problem, different heuristics are proposed and their performance in identifying the optimal critical set is analyzed.

The following are the main conclusions of our analysis:

1. A well planned targeted attack on a small number of substations is capable of leading the power system to collapse within a few seconds.

2. By taking proper precautionary measures (gas insulated substations (GIS)), the potential damage to the electric power grid can be greatly minimized.

3. A greedy choice of nodes leads to more impact on the power network than the tradi-

tional choice of high degree nodes as the targets for adversarial attack.

4. The addition of target nodes to an existing target set does not necessarily increase the impact on the power grid.

5. Hidden failures in the protective relays may be beneficial in saving the power grid from total system collapse.

6. A time-domain, AC analysis is essential in capturing the full effects of an IND event on the electric power grid.

1.3 Problem Statement

The electric power grid is a spatio-temporal graph whose nodes are the substations and the edges are transmission lines or transformers. A substation can have one or more buses inside it at same or different voltage levels. An example of this is a generating substation that has multiple generating units. Transmission lines connect buses at the same voltage level while transformers connect buses at different voltage levels. In steady state, the power system balances load and generation while keeping the line/transformer flows within their operating limits, voltage magnitudes lying between specified limits, and system frequency averaging around 60 or 50 Hz (60Hz in the Americas, 50Hz in Europe and most of Asia). An *event* is an occurrence that brings the power system out of its steady state and causes it to oscillate. An event can be lightning striking a line, a line touching a tree, human error, etc. In this analysis we study the effects of different no notice/short notice human-initiated catastrophic events on the electric power grid. In this research, we study the effect of a targeted adversarial attack on selected nodes in the power system network. The targeted attack is considered to be the detonation of a bomb at the selected nodes creating a three

phase fault in the connected buses and lines. In this context, we also try to address the problem of identifying the optimal critical target set. The criticality of a node is the impact on the power grid when it is targeted by an adversary. The optimal critical target set is the set of target nodes which has the maximum criticality.

1.4 Outline of Thesis

The thesis is organized as follows. Chapter 2 gives an overview of the state-of-art regarding the different aspects of this work. Chapter 3 discusses the various protection systems employed in transmission lines, transformers and generators in the power system and the associated hidden failures. Chapter 4 details the proposed cascading failure model and formulates a metric to evaluate the impact of a targeted attack. Chapter 5 gives an overview of the simulation setup used to perform the analysis. Chapter 6 lists the different statistical results and some critical observations have been explained. Finally Chapter 7 concludes the thesis and provides a brief summary regarding possible future work.

Chapter 2

Related Works

2.1 Cascading Failure models

The US transmission system has experienced more than 400 blackouts in between 1984 and 1999 as per the NERC reports during this period [14]. The analyses of these blackout data indicate that the probability distribution of blackout sizes obtained have heavy tails with power law dependency [15]. This indicates that a large blackout, though rare, is more likely to occur than they are expected (exponential tails of a Gaussian distribution). Therefore, large blackouts requires more attention not only due to their higher probability of occurrence, but also due to the enormous societal damage caused by such events. These observations led researchers to a series of studies in order to model cascading events in power system aiming to represent large blackouts accurately.

The observation that power system dynamics shows traits of self-organized criticality led [16] to model cascading failures like the Bak-Tang-Wiesenfeld sandpile dynamics model. However, the model involved large time scales and considered load growth and increase in system size. Two failure models have been proposed in [17]. The first model considers loss of load without line outages due to lines operating at their maximum capability, while the second model involves line outages. Two probabilistic cascading failure models have been introduced by Dobson et.al. [18]. The first model considers the redistribution of load on a tripped line to its neighboring lines. The second model involves hidden failures and considers the prob-

abilistic outage of neighboring lines of a tripped line. These models were used to study the effect of system loading on shape of the tails for the probability distribution of size of blackouts. Among these models, the hidden failure model appropriately represents the significant features of power system blackouts above critical loading condition. Two transition points are observed in [19] for cascading failure models: one due to generator capability and the other due to transmission line limits. However, the voltage and rotor angle dynamics were still not considered to assess cascading failures due to instabilities.

[20] shows that sympathetic trips and generator instability play a key role in cascading outages. Transient stability constrained optimal power flow problem is considered in [21, 22] to formulate algorithms for generation redispatch during line or bus outages. However, such redispatch may not be applicable for a large outage in the network following a targeted attack. A simplified Boolean failure model was used to study cascading failures in interdependent power and communication networks in [23]. A stochastic Boolean model of cascading failure is considered by the authors in [24, 25]. In [26], the authors studied the effect of connectivity between layered networks on the cascade probability in the network. The authors used the sandpile dynamics to represent the cascade of loads in the power grids. However it fails to replicate the actual system conditions in a power grid where a node (or bus) trips due to under-voltage or under-frequency and not due to overload.

These papers are useful in that one can often either obtain analytical results or carry out large number of simulations to get a detailed understanding of cascade dynamics. However, the model simplification comes at a cost; the recent blackout reports [7, 8] suggest that cascades need not propagate locally due to complex non-linear nature of the power grid. Furthermore, [27] discusses the various reasons leading to the historic 1996 WSCC outage, the most important being the operation of relays. It is evident from the above discussion that protection systems play a key role in cascading events. Though most of the papers

consider line outages due to overload, the protection system in the power network respond to measured impedance and current.

2.2 Misoperations in power system protection

Based on the NERC data, in more than 70% of the major disturbances, failures in protective relays are found to be a contributing factor [14]. Among these failures, a failed protection system which remains dormant in normal operating condition and becomes exposed during an abnormal condition in the system forms is the most troublesome to tackle[28]. Such failures are termed as hidden failures and these are capable of causing widespread cascading failures in the power system network leading to a major blackout[29].

In the event of a human initiated physical attack on the power grid or a catastrophic weather phenomenon, a major part of the power system network is removed from operation which includes generators, loads, transmission lines and transformers. The power flow through a damaged transmission line or a transformer gets redirected along a different path through unfaulted components. Some of these components might be overloaded which leads to their failure and a possible cascade of overloads[18]. The recent blackouts in the past decade like the large blackout in north-eastern USA and Canada on August 14, 2003 and the 2003 Italy blackout are typical examples of cascading failures in the power network[7, 8]. The 2012 blackout in north and eastern India was primarily initiated due to a false trip issued by a protection relay under critical loading condition of the power grid which resulted in a cascading failure leading to a blackout[9].

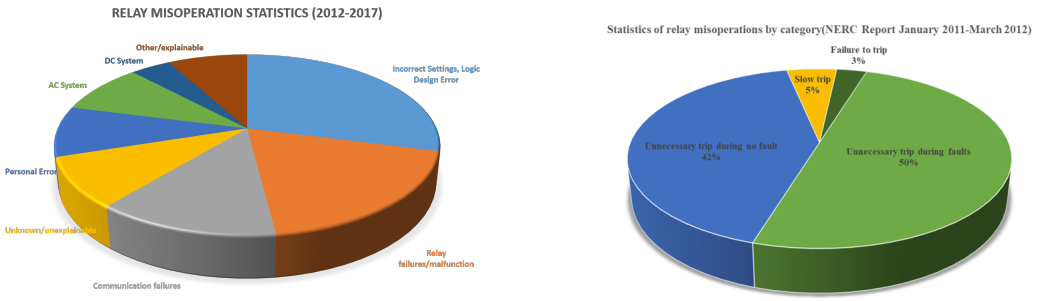
Various complex network theory have been used to analyze different cascading scenarios in order to study the effect of a disturbance in cascading failure propagation, identify the vulnerable areas in a network and to evaluate the hazards of an initial failure in a complex

network system[30, 31]. However, the vastness of the power system network often makes it impossible to analyze all possible failure patterns. Moreover, increased failure in the power grid hampers the operational state of the power system. As more failures occur, the load on other components is increased and thereby the power system slides to a stressed condition. Under such stressed condition, the probability of subsequent failures also increases. Some rare failures such as tree flash-over or hidden failure may cause the failure to propagate over the entire network and causing a large blackout[32]. A power flow entropy based modeling of cascading failures is proposed in [33] which substantiates the heavy tails in the distribution of blackout sizes. A risk assessment model is proposed in [34] to identify the vulnerable components in a power system due to a cascading failure and the severity associated with the failure [35].

The vital contribution of the proposed work is the inclusion of a stochastic model to simulate hidden failures in the power system whose effects surface out in the aftermath of a human initiated attack on the network. An important step in modeling cascading failures is to evaluate the probability of tripping of each component in the power system network. The recent NERC statistics of relay misoperations [10, 36, 37, 38] show that nearly 41% of relay misoperations are caused by unnecessary trips during a fault and about 51% contribute to unnecessary trips with no faults. These statistics strongly indicate that misoperations due to unnecessary trips are more probable than slow trips or failure to trip which contribute to the remaining 8%. Furthermore, 20% of misoperations are caused by relay failures/malfunction and 28% are due to incorrect setting or logic design. Such relay failures or faulty settings are often the principal determinant of the occurrence of a hidden failure in the power system.

The statistics of misoperations is shown in Fig. 2.1. These show that relay misoperations, though rare, has resulted in more than 90% unnecessary trips. The statistics of source of relay misoperations show that the major contributor of such events are hidden failures and

relay malfunctions. Therefore, it is necessary to analyze these failures while studying events like cascading outages in the power system. Furthermore, it is to be noted that though the occurrence of a hidden failure in a relay is stochastic as discussed in [39], the unnecessary trip issued is not probabilistic. This work takes into account these facts while modeling relay misoperations due to hidden failures.



(a) Statistics of relay misoperations by source.

(b) Statistics of relay misoperations by category.

Figure 2.1: NERC Statistics of relay misoperations.

2.3 Power flow method

A number of authors [14, 15, 16, 17, 18, 40, 41, 42, 43, 44, 45] have studied cascading failures in power grids using quasi steady state analysis with DC power flow. Informally, in these papers, a transmission line fails when the power flow exceeds the capacity of the line. The power is redistributed either to the neighboring lines as in the case of sandpile like models or is redistributed by recomputing the steady state DC power flow. The usage of DC power flow as the computation engine for the cascading failure model reduces the computational burden at the cost of severe approximation of actual system conditions. The two principal aspects of the DC power flow method are assumption of a flat voltage profile at all buses and neglecting the resistance of the transmission lines. With reactive power component

being ignored and the assumption of a flat voltage profile, the DC power flow analysis may produce good approximations under some circumstances. However, since voltage instability is an important cause for cascading events in the power grid, it is not a suitable tool to simulate such events. In this work, AC power flow model is used to accurately simulate the actual operating point in the power system.

Stability of power system subjected to cascading events is evaluated either from the network structure point of view (evaluating the degree distribution of nodes) [23, 25, 26, 46] or from the convergence of steady state power flow solution [14, 16, 18, 40]. However, such measures do not necessarily cover all possibilities of grid instability. The non-linear mechanisms like the rotor angle stability or voltage collapse are not accurately captured in these methods [47]. In this work, dynamic transient analysis has been used to assess stability of the power system. The simultaneous modeling of power system dynamics and protection functions like over-current, under-voltage, over-voltage trips etc ensures that the actual operation of the power system is exactly replicated for cascading event studies.

Soltan et.al. [48] compares the AC and DC power flow models in their capability to represent cascading events efficiently. It is concluded that both the methods provide consistent results for scenarios involving no failures. However, for large networks, the DC model underestimates the severity of cascading failures and also provides different set of vulnerable lines. Furthermore, the results are observed for small initiating events like a single edge (line) or node (bus) outage. Zussman et.al. [49] proposed an algorithm based on DC power flow method to identify the approximate location of a targeted cyber-physical attack on the power system. A variation of the DC power flow model is used in [50] in order to incorporate generator scheduling and load shedding in the post outage condition of the power system. Transient stability analysis results are used along with the modified DC power flow model to assess the cascading events in the power grid.

In this work the AC power flow model is used to obtain the system conditions at each instant of simulation and transient stability analysis is performed to assess the stability of the grid. The operation of protection systems for generators, transmission lines and transformers is modeled along with the stochastic occurrence of hidden failures in them. The trip signals of these relays are considered as the sole contributors of node and edge outages in the network.

2.4 Initiating Events

Another important aspect of studying cascading events in the power system network is the impact of different initiating events. In [23, 26, 42], the authors simulated cascading failures in power system which have been initiated by the failure of a random node in the network. In [46], four different types of initiating events are simulated in the Chinese transportation network to replicate different types of targeted attack scenarios. Such models replicate a geographically co-related attack scenario or a targeted attack on random nodes.

However, given the complex non-linear nature of the power system, it would be interesting to study the impact of choosing the target nodes in the network to maximize the impact. This leads to the formulation of the *optimal critical set* problem where in the goal is to find the optimal set of k nodes which results in maximum damage in the network. In this work, three heuristics are proposed to achieve the goal. First, the traditional method of selecting high degree nodes is considered. Then, a greedy choice of target nodes is considered where target nodes are added in a greedy fashion much like the one used in [51]. Finally a random heuristic of selection of target nodes to observe the distribution of impact for randomly chosen target node sets.

2.5 Synthetic Power Network

In most of the prior works [14, 17, 18, 19, 47, 52] the cascading failure analysis is performed on standard IEEE networks like the 118 bus system, 39 bus system, WSCC system etc. However, it is necessary to study the same for realistic power grid networks. For this purpose, the synthetic power system of Washington DC and its neighboring region is used in this work.

Since the power grid data is highly sensitive and of proprietary nature, accurate data is not available publicly. The transmission and sub-transmission system of the region around Washington DC is constructed based on scattered information found in: books, Internet, old maps, manual exploration on Google Earth, and open source information from utilities [53, 54, 55, 56]. These are all integrated to estimate the geographical locations of generators, substations and transmission line routes. The parameters of the system are approximately estimated based on the relative distance between the buses and expert knowledge [2].

With the knowledge of the power system network, the load at each bus in the grid needs to be evaluated. For this reason residential energy demand dynamics have been studied in [12] to get an aggregated load at each bus. Several models like Markov chain models [57, 58], probabilistic empirical load models [59, 60], linear regression models [61, 62] have been used to generate demands at different time scales. Various agent based models have been studied in [13, 62] to generate synthetic load demand for urban and rural areas. A similar approach has been undertaken to generate the load demand for different time scales for the population in the region around Washington DC [12]. The electric load at 1:00 pm on May 22, 2011 is considered as the time instant of consideration for the present study.

Chapter 3

Protection Systems

The vast transmission network is exposed to mercy of the nature making it highly susceptible to faults. These might have varied degree of impact on the power system ranging sagging of lines to damage of important assets in the grid. In order to protect the equipment from such severe phenomena, the power system is equipped with protection elements. The purpose of protection system is two fold: (*i*) detect a fault and (*ii*) isolate the faulted section from the healthy part of the power grid. The first task is performed by a relay where a fault is detected based on an algorithm. The second action is carried out by a circuit breaker, which receives a trip signal from the relay as soon as a fault is detected. In this section the operation of different relays employed for protection of transmission lines, transformers and generators has been discussed. The relays widely used for transmission line protection are directional overcurrent relays, mho distance protection relays, and carrier communication based directional comparison blocking relays. The relays employed for transformer protection are percentage differential relays. For generator protection, a large number of relays are involved; in this study, we are interested in the voltage based generator protection only.

3.1 Overview of directional overcurrent protection

The most widely used non-pilot protection system for transmission lines is the directional overcurrent relays (DOCRs) which detects faults in a particular direction.

3.1.1 Directional overcurrent protection scheme

Fig 3.1 shows the schematic of a directional overcurrent protection scheme. Each end of the transmission line is provided with an overcurrent element (L_{AB},L_{BA}) and a directional element (D_{AB},D_{BA}). The overcurrent element operates if magnitude of the current measured at that end exceeds the pickup value. The directional element determines the direction in which the fault is present from the direction of measured current.

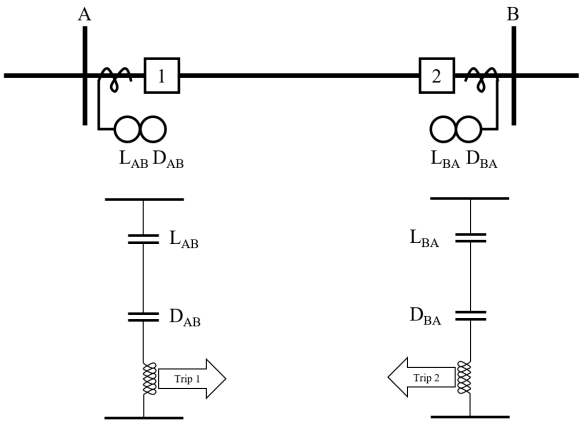
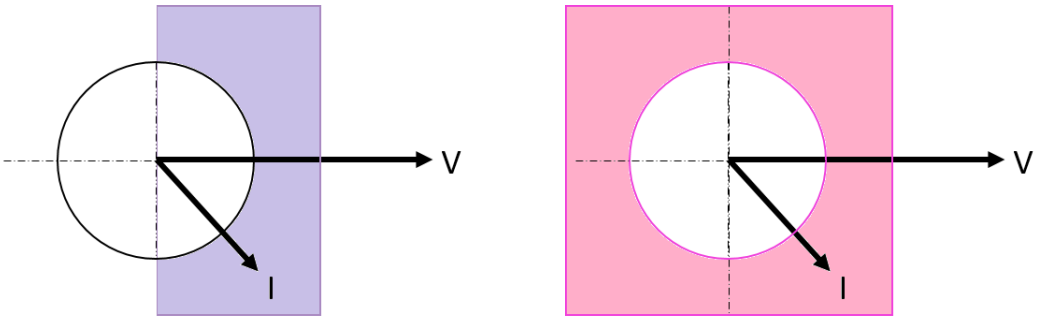


Figure 3.1: Schematic diagram of directional overcurrent protection scheme

3.1.2 Hidden failures in directional overcurrent relays

Consider a mechanical failure in the directional contact where the contacts are permanently closed. This failure remains hidden in normal operating condition since the relay does not issue a trip signal unless the overcurrent element operates. However, in case of a disturbance, if the load pickup is exceeded, the overcurrent element operates and the relay issues a trip signal irrespective of the current direction. Fig. 3.1 shows the operating region of a directional overcurrent relay in the absence an presence of a hidden failure in the directional contact. It is to be noted that the directional element responds to the phase angle between the measured voltage and current.



(a) Normal operating region in absence of hidden failure.

(b) Altered operating region in presence of hidden failure.

Figure 3.2: Operating region of directional overcurrent relay in the absence and presence of hidden failure.

Let the current measured at the ends A and B in Fig 3.1 be I_A and I_B respectively. The voltage and current phase angles at end A are $\phi_{\mathsf{v,A}}$ and $\phi_{\mathsf{i,A}}$ respectively and $\phi_{\mathsf{v,B}}$ and $\phi_{\mathsf{i,B}}$ at end B. Let the load pickup magnitudes for the overcurrent elements at A and B be respectively given by $\mathsf{I}_\mathsf{A}^{\mathsf{pick}}$ and $\mathsf{I}_\mathsf{B}^{\mathsf{pick}}$. The condition for directional relay to generate a trip signal is given by

$$\begin{aligned} \text{Breaker at A trips:} \quad & |\mathsf{I}_\mathsf{A}| > \mathsf{I}_\mathsf{A}^{\mathsf{pick}}, \quad 0 \leq |\phi_{\mathsf{v,A}} - \phi_{\mathsf{i,A}}| \leq \frac{\pi}{2} \\ \text{Breaker at B trips:} \quad & |\mathsf{I}_\mathsf{B}| > \mathsf{I}_\mathsf{B}^{\mathsf{pick}} \quad 0 \leq |\phi_{\mathsf{v,B}} - \phi_{\mathsf{i,B}}| \leq \frac{\pi}{2} \end{aligned} \tag{3.1}$$

This implies that the relay will trip if the current is positive and above the load pickup value. If the directional contact is permanently damaged due to a hidden failure, the relay will trip for positive and negative current, if it exceeds the load pickup value.

$$\begin{aligned} \text{Breaker at A trips:} \quad & |\mathsf{I}_\mathsf{A}| > \mathsf{I}_\mathsf{A}^{\mathsf{pick}} \text{ and failure in } \mathsf{D}_{\mathsf{AB}} \\ \text{Breaker at B trips:} \quad & |\mathsf{I}_\mathsf{B}| > \mathsf{I}_\mathsf{B}^{\mathsf{pick}} \text{ and failure in } \mathsf{D}_{\mathsf{BA}} \end{aligned} \tag{3.2}$$

3.2 Overview of transmission line distance protection

The second type of transmission line relays is the three zone mho distance protection scheme. Protection zones play an important role in this over-reaching distance relay operation [63]. Zone-1 is the primary protection scheme while Zone-2 and Zone-3 are back-up protection schemes. Zone-1 provides high speed protection to approximately 80% of the line which it is designed to protect. It never reaches the bus at the other end of that line. Zone-2 completely covers the protected line and overreaches to a portion of the next line. The primary purpose of Zone-2 is to detect faults in the protected line beyond Zone-1. Zone-2 also provides backup for a failed Zone-1 element, both in the protected line as well as in the next line. Zone-2 is typically set to reach less than the Zone-1 reach of the next line. Zone-3 provides remote back-up protection typically by detecting a fault in the event a remote breaker (which was expected to trip) does not trip. Zone-3 is set to cover 100% or more of the next line beyond the line that is to be protected. Sometimes Zone-3 setting becomes high enough to operate on high load or on power swings. Adequate measures are taken to prevent Zone-3 operation for such situations by using shaped characteristics, load encroachment detection and power swing blocking [64].

3.2.1 Mho distance protection scheme

Coordination in time is essential for successful operation of the three zones especially when the power system is under stress. Zone-1 is designed to be instantaneous whereas Zone-2 and Zone-3 have inherent time delays in their operation. This time delay is called the *fault clearing time*. In case one of the previous zone/s fail to clear the fault, the next zone which detects the fault operates after the fault clearing time is crossed. Thus, in case of an unsuccessful zone operation, the fault persists in the system for a time that is equal to the

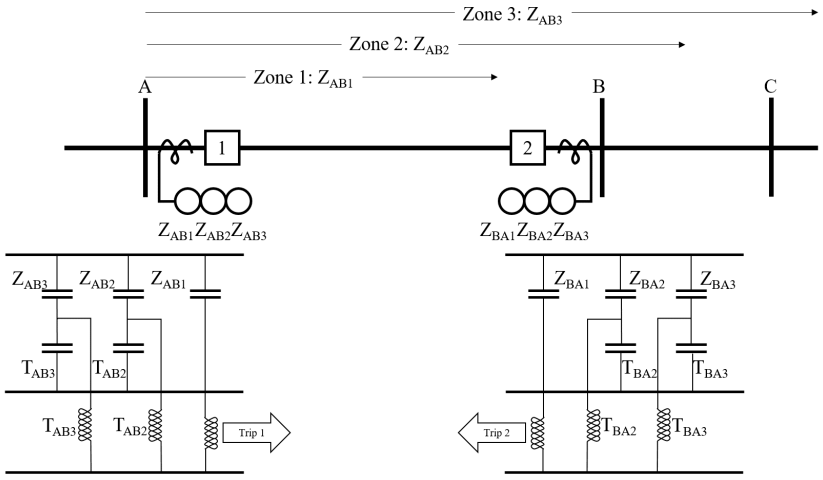


Figure 3.3: Schematic diagram of three zone mho distance protection scheme

fault clearing time of the zone which eventually clears the fault. More details about different protection zones can be found in [64].

For the simulations done here, the fault clearing time for a Zone-2 operation was set at 0.5 seconds, while that for a Zone-3 operation was set at 1 second (industry standard for the EI). The reach of Zone-1 is considered to be 80% of the line it is designed to protect. Zone-2 has a reach of 150% which covers the entire length of the protected line and 50% of the adjacent line. Zone-3 has a reach of 250% which covers the entire length of the protected line and the adjacent line and covers some portion of the next adjacent line. Fig 3.3 represents the schematic for a three zone mho distance relay which is designed to protect the line A-B. The inherent time delays for the operation of Zone-2 and Zone-3 is implemented through the timer contacts ($\mathsf{T_{AB2}}$,$\mathsf{T_{BA2}}$ for Zone-2 and $\mathsf{T_{AB3}}$,$\mathsf{T_{BA3}}$ for Zone-3) and their corresponding timer coils.

Fig 3.4 shows the operating zones of the mho distance relay at A designed to protect the line A-B. Let $\mathsf{M_{AB1}}, \mathsf{M_{AB2}}, \mathsf{M_{AB3}}$ indicate operating zones Zone-1, Zone-2 and Zone-3 for the mho relay at A. If the apparent impedance (the impedance measured by the relay) encroaches a

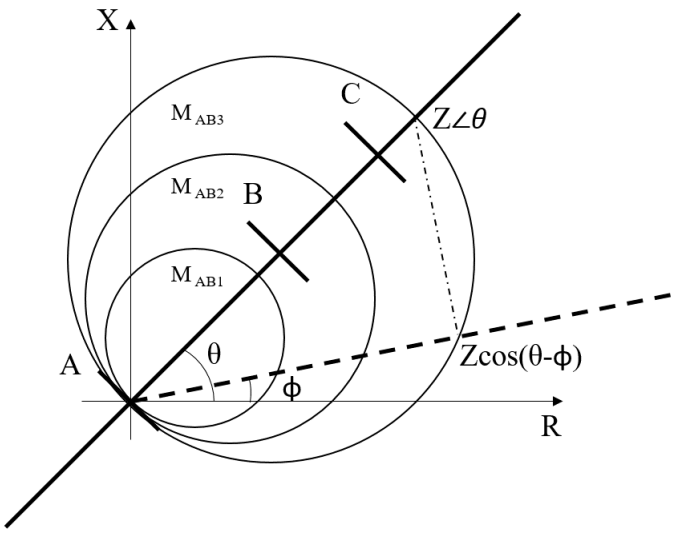


Figure 3.4: Operating zones of a mho distance protection relay

particular zone, the zone element contact ($\mathsf{Z_{AB1}}, \mathsf{Z_{AB2}}, \mathsf{Z_{AB3}}$) closes instantaneously. However for Zone-2 or Zone-3, the trip coil is not energized since the timer contact ($\mathsf{T_{AB2}}, \mathsf{T_{AB3}}$) remains open. The timer contact closes only after the inherent time delay.

From Fig. 3.4, it is evident that the diameter of an operating zone lies on the impedance line A-B-C. Let the complex impedance at the point on an operating zone be $\mathsf{Z}\angle\theta$ where θ is the impedance angle of the line. It is to be noted that this point lies along the impedance line A-B-C. Therefore, the zone is designed to issue trip signal if the apparent impedance ($\mathsf{Z^{app}}$) is less than $\mathsf{Z}\angle\theta$. However, under normal operating condition, a power system operates at high power factor. Hence the apparent impedance of a line lies at a considerably smaller impedance angle, such as along the dotted line with an angle of ϕ. Therefore, the apparent impedance encroaches the operating zone of the mho distance element at an impedance given by $\mathsf{Z}\cos(\theta - \phi)$.

With variation in the operating power factor of the line ($\cos\phi$), the zone encroachment impedance also varies. Fig. 3.5 depicts the variation of zone encroachment impedance for a

zone setting of $1\angle 80^o$ with line power factor varying from 0.1 to 1.0.

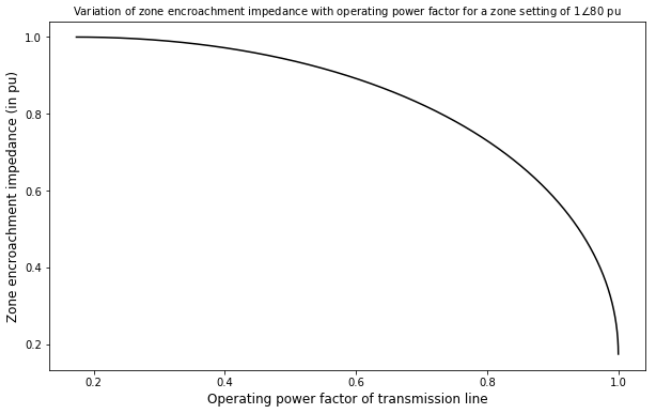
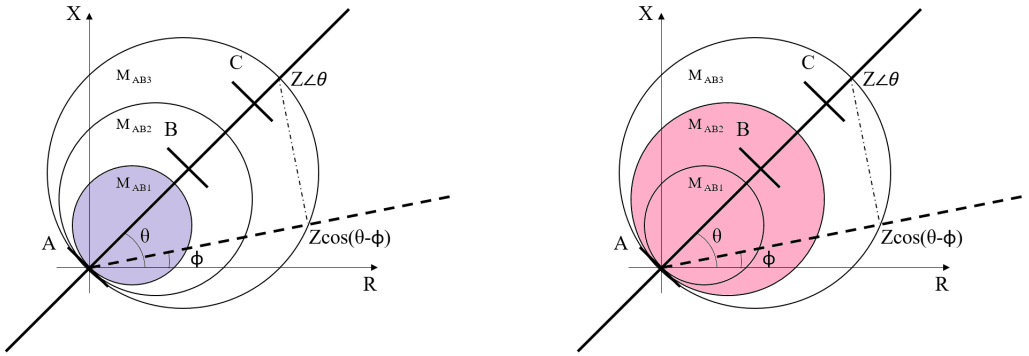


Figure 3.5: Variation in zone encroachment impedance with operating line power factor

3.2.2 Hidden failures in mho distance protection relays

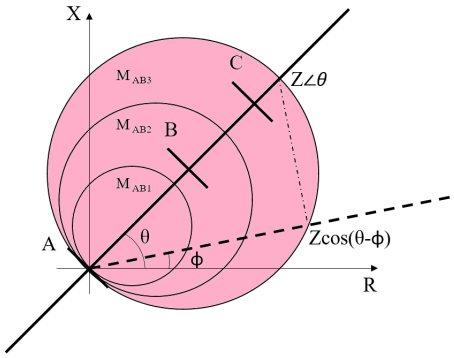
Consider the case of a hidden failure (contacts get permanently closed) in the timer contacts of Zone-2 or Zone-3. The trip coil is not energized until the apparent impedance encroaches any of these zones (since contacts $\mathsf{Z_{AB2}}$, $\mathsf{Z_{AB3}}$ are open). Therefore, the failure in timer contacts remain hidden until the instant when apparent impedance encroaches the zone which has a failed timer contact. This leads to an instantaneous trip in these backup zones which is unnecessary (since they are supposed to issue a trip signal with a particular delay). It is to be noted that the Zone 1 does not have any timer contact and hence there is no possibility of the occurrence of a hidden failure. Fig. 3.6 compares the operating region of mho distance protection element in the presence and absence of hidden failures in its timer contacts.

Let $\mathsf{Z_A}$ and $\mathsf{Z_B}$ be the apparent impedances measured at ends A and B respectively. Let $\mathsf{M_{AB1}}, \mathsf{M_{AB2}}, \mathsf{M_{AB3}}$ indicate operating zones Zone-1, Zone-2 and Zone-3 for mho relay at A and $\mathsf{M_{BA1}}, \mathsf{M_{BA2}}, \mathsf{M_{BA3}}$ be the same for mho relay at B. The condition of mho distance relay



(a) Normal operating region in absence of hidden failure.

(b) Altered operating region in presence of hidden failure in Zone 2 timer contact.



(c) Altered operating region in presence of hidden failure in Zone 3 timer contact.

Figure 3.6: Operating region of mho distance protection relay in the absence and presence of hidden failures in the timer contacts.

to issue an instantaneous trip signal for line A-B is given by

$$\begin{aligned} &\text{Breaker at A trips:} \quad \mathsf{Z_A} \in \mathsf{M_{AB1}} \\ &\text{Breaker at B trips:} \quad \mathsf{Z_B} \in \mathsf{M_{BA1}} \end{aligned} \tag{3.3}$$

For hidden failure in timer contacts, the condition for which instantaneous trip signal is

issued for the line A-B is given by

$$\begin{aligned}
&\text{Breaker at A trips:} \quad Z_A \in M_{AB2} \text{ and failure in } T_{AB2} \\
&\text{Breaker at A trips:} \quad Z_A \in M_{AB3} \text{ and failure in } T_{AB3} \\
&\text{Breaker at B trips:} \quad Z_B \in M_{BA2} \text{ and failure in } T_{BA2} \\
&\text{Breaker at B trips:} \quad Z_B \in M_{BA3} \text{ and failure in } T_{BA3}
\end{aligned} \tag{3.4}$$

3.3 Overview of directional comparison blocking scheme

The third widely used protection scheme for transmission lines is the power line carrier (PLC) communication based directional comparison blocking scheme [63]. In this type of protection system, the direction of a fault on the transmission line is identified (within the protected line or external to it) and the information is sent to the remote end to allow/block the relay operation.

3.3.1 PLC based directional comparison block scheme

Fig. 3.7 shows a schematic of the directional comparison blocking scheme. Each end of the transmission line has a directional mho distance element (D_{AB},D_{BA}) and a reversed mho carrier start relay (C_{AB},C_{BA}) as shown in Fig. 3.8. The directional mho element is set to detect faults in the direction of the remote end. The reverse mho element detects a fault in the opposite direction and sends a carrier *block* signal to the receiver relay at the remote end. Transmission of this signal is stopped if the directional element detects a fault in its zone of operation. The receiver relay at the remote end opens the normally closed receiver contact if it receives a carrier *block* signal. Therefore, a trip signal is issued to the circuit breaker if the directional element has operated at an end and no blocking signal is received

from the remote end.

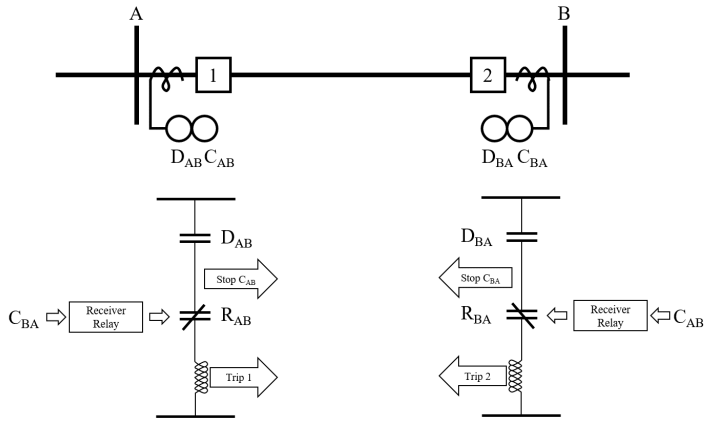


Figure 3.7: Schematic diagram of PLC based directional comparison blocking scheme

If a fault occurs on the transmission line A-B in Fig 3.7, the directional elements (D_{AB},D_{BA}) detects the fault and stops the carrier start relays (C_{AB},C_{BA}) from transmitting the carrier block signal. Therefore, the directional contact operates and the receiver contacts remain closed, thereby tripping the circuit breakers at A and B. If the fault is external to the line and beyond B, the directional element at A (D_{AB}) detects it and operates. It also stops transmitting the carrier block signal (C_{AB}) to the other end (B). The directional element at B (D_{BA}) does not operate since the fault is not in its operating region and hence breaker (2) at B does not trip. However, the fault is detected by the reversed mho carrier start relay at B (C_{BA}) which transmits carrier blocking signal to end A. This signal is received by the receiver element at A and opens the receiver contact (R_{AB}). Therefore, breaker (1) at A is inhibited from operation.

3.3.2 Hidden failures in PLC based directional comparison blocking relays

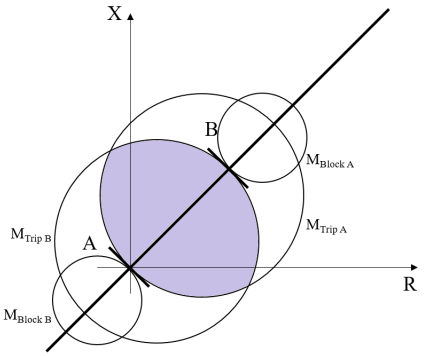
Similar to the previous two types of relays, the carrier based directional overcurrent protection relays are equally susceptible to hidden failures. Consider a mechanical failure in the receiver contact at any end where the contacts are permanently closed. In such a case, the relay issues a trip signal if the fault is detected in the zone of operation of the directional element at that end. A carrier blocking signal from the other end has no effect on the trip logic. Furthermore, such a failure remains hidden as the relay does not issue trip signal until the directional element detects a fault. We consider the mho relay characteristics as shown in Fig. 3.8 which compare the operating regions in the absence and presence of the hidden failures in the receiver contacts.

Let $\mathsf{M}_{\mathsf{Trip\ A}}$ and $\mathsf{M}_{\mathsf{Trip\ B}}$ be the operating characteristics of the directional mho elements at ends A and B respectively. Similarly, let $\mathsf{M}_{\mathsf{Block\ A}}$ and $\mathsf{M}_{\mathsf{Block\ B}}$ be the operating characteristics of the reversed mho carrier start relays responsible for transmitting blocking signals to ends A and B respectively. The condition for the PLC based directional comparison blocking relay to generate a trip signal based on the complex impedances Z_A and Z_B measured at A and B respectively is given by

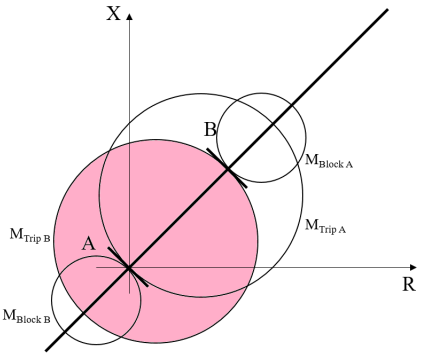
$$\text{Breakers at A,B trip:} \quad \mathsf{Z}_\mathsf{A} \in \mathsf{M}_{\mathsf{Trip\ A}} \text{ and } \mathsf{Z}_\mathsf{B} \in \mathsf{M}_{\mathsf{Trip\ B}} \tag{3.5}$$

If the receiver contact of the relay at an end is permanently damaged due to a hidden failure, the relay issues a trip signal based on the directional element at the same end.

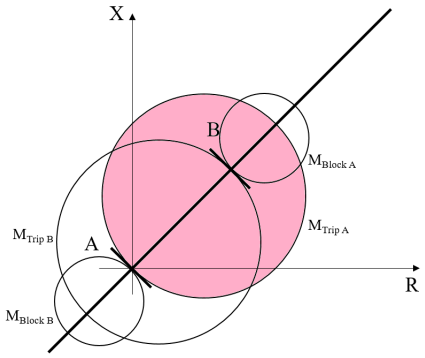
$$\begin{aligned} &\text{Breaker at A trips:} \quad \mathsf{Z}_\mathsf{A} \in \mathsf{M}_{\mathsf{Trip\ A}} \text{ and failure in } \mathsf{R}_{\mathsf{AB}} \\ &\text{Breaker at B trips:} \quad \mathsf{Z}_\mathsf{B} \in \mathsf{M}_{\mathsf{Trip\ B}} \text{ and failure in } \mathsf{R}_{\mathsf{BA}} \end{aligned} \tag{3.6}$$



(a) Normal operating region in absence of hidden failure.



(b) Altered operating region in presence of hidden failure in receiver contact of end A.



(c) Altered operating region in presence of hidden failure in receiver contact of end B.

Figure 3.8: Operating region of PLC based directional comparison blocking relay in the absence and presence of hidden failure.

3.4 Overview of percentage differential relay

The protection system used to detect internal faults in a transformer is the percentage differential protection scheme. This relay is a variation of the differential protection, where the currents at the two ends of the transformer are compared to identify internal faults. However, the traditional differential protection is sensitive to inrush currents which are treated as internal faults. Therefore, the percentage differential protection scheme is employed to restrain the relay from tripping during such events.

3.4.1 Percentage differential protection scheme

Fig. 3.9 shows the schematic of a percentage differential relay for a transformer. The relay has two coils namely the operating coil and restraining coil. The operating coil responds to the difference in measured currents ($\mathsf{I}_{\mathsf{As}} - \mathsf{I}_{\mathsf{Bs}}$) at the two ends of the transformer A-B. The restraining coil responds to the average of the measured currents $\left(\frac{\mathsf{I}_{\mathsf{As}} + \mathsf{I}_{\mathsf{Bs}}}{2}\right)$. The restraining coil is present to avoid false trips due to heavy inrush currents.

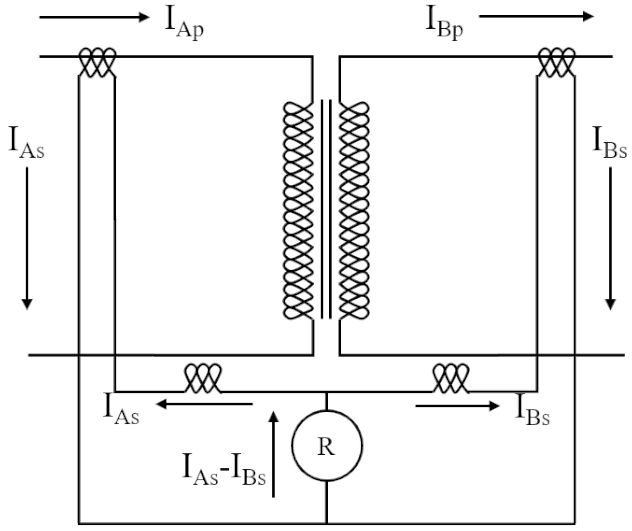


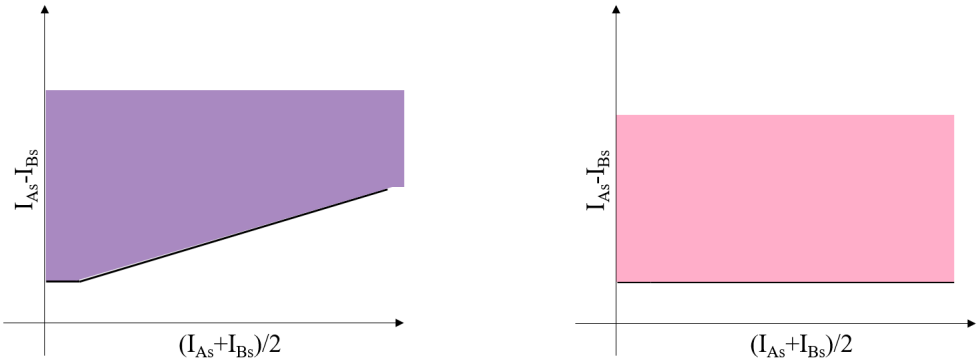
Figure 3.9: Schematic diagram of percentage differential protection of transformer

Under normal operating condition, the differential current is caused due to the magnetizing component of the transformer equivalent circuit which accounts for $1-4\%$ of the rating [65]. The trip signal is sent to the transformer circuit breakers if

$$\left(\mathsf{I}_{\mathsf{As}} - \mathsf{I}_{\mathsf{Bs}}\right) - K\left(\frac{\mathsf{I}_{\mathsf{As}} + \mathsf{I}_{\mathsf{Bs}}}{2}\right) \geq \mathsf{I}_{\mathsf{min}}^{\mathsf{pick}} \tag{3.7}$$

where K denotes the sensitivity of the percentage differential relay and is expressed as a percentage. $\mathsf{I}_{\mathsf{min}}^{\mathsf{pick}}$ is the minimum pickup value of the differential current.

3.4.2 Hidden failure in percentage differential relays



(a) Normal operating region in absence of hidden failure.

(b) Altered operating region in presence of hidden failure.

Figure 3.10: Operating region of percentage differential relay in the absence and presence of hidden failure.

Fig. 3.10 shows the operating region (shaded region) of a percentage differential relay. Similar to transmission line relays, hidden failures in the percentage differential relays can affect the tripping logic. If the restraining coil is shorted internally, the trip signal is generated if difference in the measured currents exceeds the minimum pickup value. Such false trip signals are generated for high currents flowing through the transformer. This failure remains hidden since the relay does not issue a trip signal until the difference in measured currents at the two ends of the transformer is considerable. Therefore, tripping condition of a percentage differential relay with hidden failure in the restraining coil is given by

$$\mathsf{I}_{\mathsf{As}} - \mathsf{I}_{\mathsf{Bs}} \geq \mathsf{I}_{\mathsf{min}}^{\mathsf{pick}} \tag{3.8}$$

3.5 Generator Protection

Generators are the most vital equipment in a power grid and is responsible for maintaining the stability of the system. Therefore, they are provided with a wide range of protection systems. In this work, we are considering the overvoltage and undervoltage generator relays. If a generator bus violates the allowable voltage limits for a definite duration of time, the over/undervoltage relays issue corresponding trip signal.

In practical cases, when multiple HV transmission lines are tripped during a disturbance, the reactive support drops. This causes the generators to provide reactive power through excitation of the field (rotor) circuit. If it exceeds the generator capability, the overexcitation protection issues a trip signal. However, if it does not trip and the generator is made to operate above reactive power limits, the generator bus voltage drops and the undervoltage relay issues a trip signal. In this study, we consider the trip signal of the undervoltage relays to be responsible for generator outages.

Since the generators are important from the stability aspect of the power system, the overvoltage and undervoltage relays are provided with fault clearance time (or delay). A separate timer is activated for each voltage limit violation. The generator trips if any of the timers reaches their respective fault clearance time. Generally, two overvoltage and two undervoltage limits are provided for every generator: one for moderate limit violation with longer clearance time and the other for severe limit violation with shorter clearance time.

In previous works, probability of occurrence of hidden failure for generator protection relays have been proposed in [40] as a function of the generator voltages. However, keeping in consideration, the strict maintenance guidelines provided by the Federal Regulatory Commission [66], the occurrence of failures in the generator protection elements is considered less probable. Therefore, hidden failures in generator relays is not studied in the present work.

Chapter 4

Cascading Failure Model

4.1 Initializing the model

Let $\mathsf{G} = (\mathsf{V}, \mathsf{E})$ denote the entire power system network with n nodes and m edges. V denotes the nodes of the graph which are the buses in the power grid and E denotes the edges of the graph which are the transmission lines and transformers in the power system. Let $\mathsf{E_L}$ denote the set of transmission lines and $\mathsf{E_T}$ be the set of transformers with $\mathsf{E} = \mathsf{E_L} \cup \mathsf{E_T}$.

4.2 Identifying edges susceptible to hidden failures

A subset of the edges, $\mathsf{F} \subset \mathsf{E}$ is selected which are the critical edges in the network. This implies that a hidden failure in these edges $e \in \mathsf{F}$ is more likely to cause a line trip than a hidden failure in the other edges. The set F comprises of a set of transmission lines $\mathsf{F_L}$ and a set of transformers $\mathsf{F_T}$ with $\mathsf{F} = \mathsf{F_L} \cup \mathsf{F_T}$. These sets are chosen by the following criteria.

1. Let $\mathsf{Z}_{e,\text{pre}}$ and $\mathsf{Z}_{e,\text{post}}$ denote the apparent impedances for a transmission line e before and after the initiating event respectively. A set of edges for which the difference between these impedances is more than a threshold value $\mathsf{Z}_{\text{thresh}}$ is identified and included in the set $\mathsf{F_L}$.

$$|\mathsf{Z}_{e,\text{pre}} - \mathsf{Z}_{e,\text{post}}| \geq \mathsf{Z}_{\text{thresh}} \Rightarrow e \in \mathsf{F_L} \tag{4.1}$$

2. Let $\mathsf{I}_{e,\text{pre}}$ and $\mathsf{I}_{e,\text{post}}$ denote the measured currents for a transmission line e before and after the initiating event respectively. A set of edges for which the difference between these currents is more than a threshold value $\mathsf{I}_{\text{thresh}}$ is identified and included in the set $\mathsf{F_L}$.

$$|\mathsf{I}_{e,\text{pre}} - \mathsf{I}_{e,\text{post}}| \geq \mathsf{I}_{\text{thresh}} \Rightarrow e \in \mathsf{F_L} \tag{4.2}$$

3. Let $\Delta\mathsf{I}_{e,\text{pre}}$ and $\Delta\mathsf{I}_{e,\text{post}}$ denote the difference between measured currents at ends of a transformer e before and after the initiating event respectively. A set of transformer edges for which the difference between these terms is more than a threshold value $\Delta\mathsf{I}_{\text{thresh}}$ is identified and included in the set $\mathsf{F_T}$.

$$|\Delta\mathsf{I}_{e,\text{pre}} - \Delta\mathsf{I}_{e,\text{post}}| \geq \Delta\mathsf{I}_{\text{thresh}} \Rightarrow e \in \mathsf{F_T} \tag{4.3}$$

4.3 Identifying relays with hidden failures

It is assumed that each end of a transmission line (edge) has three relays: a mho relay, a directional overcurrent relay and a PLC based directional comparison blocking relay at each end. Similarly, each transformer has a percentage differential relay. For each simulation, the relays with hidden failure are identified by performing a Bernoulli trial for each relay in the network with a definite probability of success. In this study, the success probability of the Bernoulli trials is considered to be 0.2% for each type of relay.

Let $\mathsf{H_{DA}}, \mathsf{H_{DB}} \subset \mathsf{F_L}$ be the set of edges with hidden failure in the directional contact of directional overcurrent relays at the first second ends respectively. These are the edges for which the outcome of Bernoulli trial was a success. Similarly, let $\mathsf{H_{TA2}}, \mathsf{H_{TB2}} \subset \mathsf{F_L}$ denote the set of edges with hidden failure in the timer contact of Zone-2 in mho relays at the first and second ends respectively. Likewise, let $\mathsf{H_{TA3}}, \mathsf{H_{TB3}} \subset \mathsf{F_L}$ be the edges with hidden failures in

the Zone-3 timer contact of mho relays and $\mathsf{H_{RA}}, \mathsf{H_{RB}} \subset \mathsf{F_L}$ are the set of edges with hidden failure in the receiver contact of PLC based directional comparison blocking relays. Let $\mathsf{H_T} \subset \mathsf{F_T}$ be the set of transformers (edges) with hidden failure in the restraining coil of the percentage differential relays.

4.4 Power Flow Model

The state of each node i is represented by its voltage $U_i = |U_i|e^{j\theta_i}$ where $|U_i|$ denotes the magnitude of the bus voltage and the phase angle of the voltage is given by θ_i. In the present work, at every time step the AC power flow problem is solved. Therefore, the voltage magnitude and phase angle at each bus in the power grid is solved from the known active and reactive power injections at every bus [7, 67]. The injected apparent power at node i is given by

$$S_i = \sum_{k=1,k\neq i}^{n} S_{ik} = \sum_{k=1,k\neq i}^{n} U_i y_{ik}^{\star}(U_i^{\star} - U_k^{\star}) = U_i(\mathbf{Yu})_i^{\star} \tag{4.4}$$

where $\star$ denotes the complex conjugate, $\mathbf{u} = [U_1 U_2 \cdots U_n]^T$ denotes the vector of node voltages and y_{ik} is the corresponding element of the admittance matrix $\mathbf{Y}$ denoting the equivalent impedance of the edge between nodes i and k. The admittance matrix depends on the topology of the power system network and is given by

$$Y_{ik} = \begin{cases} \sum_{i\neq k} y_{ik}, & \text{if } k = i \\ -y_{ik}, & \text{if } k \in \mathsf{N}(i) \\ 0, & \text{if } k \notin \mathsf{N}(i) \end{cases} \tag{4.5}$$

Considering the complex admittance matrix $\mathbf{Y}$ as the sum of two real matrices $\mathbf{G}$ and $\mathbf{B}$ given by $\mathbf{Y} = \mathbf{G} + j\mathbf{B}$ and using the expression for apparent power $S_{ik} = P_{ik} + jQ_{ik}$, the following expressions are obtained for real (P_i) and reactive (Q_i) power injections at the node i.

$$\begin{aligned} P_i &= \sum_{k=1}^{n} |U_i||U_k|(G_{ik}\cos\theta_{ik} + B_{ik}\sin\theta_{ik}) \\ Q_i &= \sum_{k=1}^{n} |U_i||U_k|(G_{ik}\sin\theta_{ik} - B_{ik}\cos\theta_{ik}) \end{aligned} \tag{4.6}$$

where $\theta_{ik} = \theta_i - \theta_k$.

4.5 Transient Stability Analysis

The ability of power system to maintain synchronism when subjected to a large disturbance is termed as transient stability [7, 67]. In response to a rapid loss of load (or generation), the power system frequency will increase (or decrease). However, the generator controls respond to this change by changing the power output to meet the electric load demand based on Equation 4.7.

$$P_{m,g} - P_{e,g}(\delta_g) = M_g\ddot{\delta}_g + D_g\dot{\delta}_g \tag{4.7}$$

P_m is the mechanical power input, $P_e(\delta)$ is the electrical power output as a function of the electrical angle (δ), M is a function of the machine's inertia, and D corresponds to the damping coefficient. Equation 4.7 is the governing equation for a generic transient stability analysis [67, 68]. In the present study we have followed a numerical integration method to solve the differential equations.

4.6 Failure of edges

The generator, transmission line and transformer relays are set based on their position in the power grid and keeping in mind the region of protection for each of them. A detailed account of relay settings for each element in the power system is given in Appendix A. The failure of lines, transformers and generators is dependent on the operation of these protection relays.

4.6.1 Failure of transmission lines

For every time step in the simulation, apparent impedances at two ends of a transmission line (edge) e are denoted by $\mathsf{Z}_{\mathsf{e,A}}$ and $\mathsf{Z}_{\mathsf{e,B}}$. The impedances are complex quantities which can be represented on a two dimensional complex plane as $\mathsf{Z}_{\mathsf{e,A}} = \mathsf{R}_{\mathsf{e,A}} + j\mathsf{X}_{\mathsf{e,A}}$ and $\mathsf{Z}_{\mathsf{e,B}} = \mathsf{R}_{\mathsf{e,B}} + j\mathsf{X}_{\mathsf{e,B}}$. The magnitude of measured currents at the two ends are $\mathsf{I}_{\mathsf{e,A}}$ and $\mathsf{I}_{\mathsf{e,B}}$ and the phase angle difference between measured currents and voltages at ends A and B are ϕ_{A} and ϕ_{B} respectively. The transmission line are tripped based on the relay settings for the line. We consider this tripping or removal of edge as a failure.

Directional overcurrent relays. The following conditions are considered for line trips caused by directional overcurrent relays. For the correct operation of relays, the following must hold.

$$\begin{aligned} &\text{Trip at end A:} \quad (\mathsf{I}_{\mathsf{e,A}}, \phi_{\mathsf{A}}) \in \mathsf{M}_{\mathsf{e,A}}, \quad \text{for } \mathsf{e} \in \mathsf{E}_{\mathsf{L}} \\ &\text{Trip at end B:} \quad (\mathsf{I}_{\mathsf{e,B}}, \phi_{\mathsf{B}}) \in \mathsf{M}_{\mathsf{e,B}}, \quad \text{for } \mathsf{e} \in \mathsf{E}_{\mathsf{L}} \end{aligned} \tag{4.8}$$

For hidden failures in the directional contact of DOCRs, the conditions are

$$\begin{aligned} &\text{Trip at end A:} \quad (\mathsf{I}_{\mathsf{e,A}}, \phi_{\mathsf{A}}) \in \mathsf{M}_{\mathsf{e,HFA}}, \quad \text{for } \mathsf{e} \in \mathsf{H}_{\mathsf{DA}} \\ &\text{Trip at end B:} \quad (\mathsf{I}_{\mathsf{e,B}}, \phi_{\mathsf{B}}) \in \mathsf{M}_{\mathsf{e,HFB}}, \quad \text{for } \mathsf{e} \in \mathsf{H}_{\mathsf{DB}} \end{aligned} \tag{4.9}$$

Mho distance relays. The following conditions are considered for line trips caused by mho distance relays. The Zone-1 trip is instantaneous for all edges in the graph G.

$$\begin{aligned} &\text{Zone-1 trip at end A:} \quad (\mathsf{R_{e,A}}, \mathsf{X_{e,A}}) \in \mathsf{M_{e,A1}}, \quad \text{for } e \in \mathsf{E_L} \\ &\text{Zone-1 trip at end B:} \quad (\mathsf{R_{e,B}}, \mathsf{X_{e,B}}) \in \mathsf{M_{e,B1}}, \quad \text{for } e \in \mathsf{E_L} \end{aligned} \tag{4.10}$$

The Zone-2 and Zone-3 trips are instantaneous for the edges in which the relays are affected by hidden failures.

$$\begin{aligned} &\text{Zone-2 trip at end A:} \quad (\mathsf{R_{e,A}}, \mathsf{X_{e,A}}) \in \mathsf{M_{e,A2}}, \quad \text{for } e \in \mathsf{H_{TA2}} \\ &\text{Zone-2 trip at end B:} \quad (\mathsf{R_{e,B}}, \mathsf{X_{e,B}}) \in \mathsf{M_{e,B2}}, \quad \text{for } e \in \mathsf{H_{TB2}} \\ &\text{Zone-3 trip at end A:} \quad (\mathsf{R_{e,A}}, \mathsf{X_{e,A}}) \in \mathsf{M_{e,A3}}, \quad \text{for } e \in \mathsf{H_{TA3}} \\ &\text{Zone-3 trip at end B:} \quad (\mathsf{R_{e,B}}, \mathsf{X_{e,B}}) \in \mathsf{M_{e,B3}}, \quad \text{for } e \in \mathsf{H_{TB3}} \end{aligned} \tag{4.11}$$

PLC based directional comparison block relays. The following conditions are considered for line trips caused by PLC based directional comparison block relays. For the correct operation of the relays, the condition of trip is given by

$$(\mathsf{R_{e,A}}, \mathsf{X_{e,A}}) \in \mathsf{M_{e,Trip\ A}} \bigcap \mathsf{M_{e,Trip\ B}}, \quad \text{for } e \in \mathsf{E_L} \tag{4.12}$$

For a hidden failure in the receiver contact at any end, the trip condition is given by

$$\begin{aligned} &\text{Trip at end A:} \quad (\mathsf{R_{e,A}}, \mathsf{X_{e,A}}) \in \mathsf{M_{e,Trip\ A}}, \quad \text{for } e \in \mathsf{H_{RA}} \\ &\text{Trip at end B:} \quad (\mathsf{R_{e,B}}, \mathsf{X_{e,B}}) \in \mathsf{M_{e,Trip\ B}}, \quad \text{for } e \in \mathsf{H_{RB}} \end{aligned} \tag{4.13}$$

4.6.2 Failure of transformers

For every simulation time step, the magnitude of rms currents at the two ends of a transformer e are measured as $\mathsf{I}_{\mathsf{e,A}}$ and $\mathsf{I}_{\mathsf{e,B}}$. The condition for normal operation of percentage differential relay for the transformer e is given by

$$\text{Transformer trip:} \quad (\mathsf{I}_{\mathsf{e,A}}, \mathsf{I}_{\mathsf{e,B}}) \in \mathsf{M}_{\mathsf{e,op}}, \quad \text{for } e \in \mathsf{E}_{\mathsf{T}} \tag{4.14}$$

For hidden failure affected transformer percentage differential relays, the trip condition is given by

$$\text{Transformer trip:} \quad (\mathsf{I}_{\mathsf{e,A}}, \mathsf{I}_{\mathsf{e,B}}) \in \mathsf{M}_{\mathsf{e,min}}, \quad \text{for } e \in \mathsf{H}_{\mathsf{T}} \tag{4.15}$$

4.7 Failure of nodes

4.7.1 Failure of generators

At every time step of simulation, the voltage magnitude at the generator buses are measured and the timers $\mathsf{T}_{\mathsf{g,1}}$, $\mathsf{T}_{\mathsf{g,2}}$ and $\mathsf{T}_{\mathsf{g,3}}$ are updated based on the settings in Eq. A.10, A.11 and A.12. The generators for which $\mathsf{M}_{\mathsf{g,Trip}}$ is True are tripped.

$$\text{Generator trip:} \quad \mathsf{M}_{\mathsf{g,Trip}} = \mathsf{True}, \quad \text{for } g \in \mathsf{V}_{\mathsf{G}} \tag{4.16}$$

4.7.2 Failure of non-generator buses

After every time step of simulation, when multiple edge failure occurs, the graph G is checked for isolated nodes. These nodes are removed from the graph and counted towards the number

of nodes failed. The next simulation step is initiated on the modified graph with the removed nodes. Let V' denote the set of nodes which have zero degree and E' be the set of edges which have failed in the current time step.

$$\mathsf{V}' = \{v | \mathsf{deg}(v) = 0, \quad \text{for } v \in \mathsf{V}\} \tag{4.17}$$

The modified graph for the next time step of simulation is given by

$$\mathsf{G}(t + \Delta t) = (\mathsf{V} \setminus \mathsf{V}', \mathsf{E} \setminus \mathsf{E}') \tag{4.18}$$

4.8 Schematic of power flow simulation

In this work, a power flow simulation is run for every 8 ms. Fig. 4.1 summarizes the actions performed at each time step of simulation. The power flow problem is solved to obtain the states of the power system at every instant. This solution is used as initial values for the differential equations required to solve the transient stability problem. The operation of protection systems and system constraints are thereafter considered before proceeding to the next instant of simulation.

4.9 Power System Collapse

A power system collapse can occur due to different reasons which can be attributed to the transient rotor angle stability and voltage stability of the grid. In the present study, the transient stability is used to identify a system collapse. The ability to maintain synchronism when subjected to large disturbances is known as transient stability [68]. If a set of generator

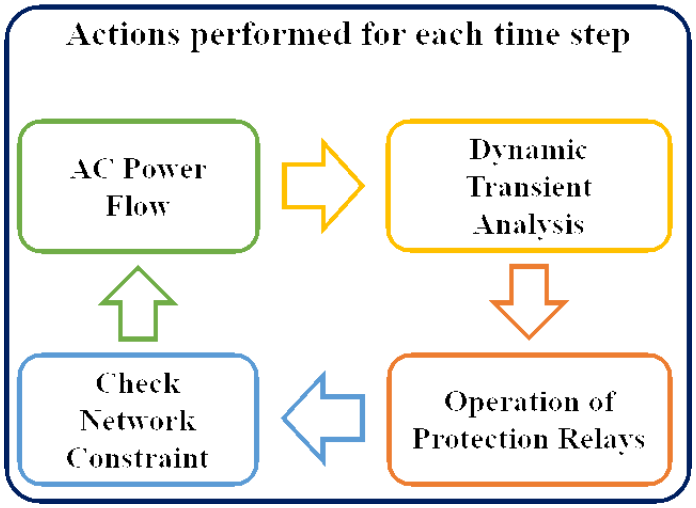


Figure 4.1: Actions undertaken for each time step of simulation

rotor angles differ from the rotor angles of another set by more than 180 degrees, the two sets of generators are said to be operating out of step [63]. In such a scenario, the generators trip due to the operation of out-of-step relays and the results in a load-generation imbalance in the power grid. This causes frequency at the load buses to drop below the allowable range and thereby triggers automatic under-frequency load shedding at these buses. Since this load-shedding is automatic and hence uncontrolled, it results further load-generation imbalance. The over-frequency at the less loaded generator buses causes them to trip and this process continues resulting in a widespread blackout.

4.10 Evaluating impact of an attack

In order to consider the probabilistic occurrence of hidden failures in the protection relays, each simulation is run multiple number of times. In this case, we have chosen this number to be 20. The impact of an attack is therefore calculated as follows.

1. The mean number of nodes lost or buses tripped in the course of simulation. This is

denoted by n_i for attack on the target set $\mathsf{A_i}$.

$$n_i = \frac{1}{20}\sum_{j=1}^{20} n_{ij} \tag{4.19}$$

where n_{ij} is the number of nodes lost or buses tripped for the j^{th} simulation.

2. The empirical probability of blackout which denotes the fractional number of simulations for which the system collapses due to instability. This is denoted by b_i for attack on the target set $\mathsf{A_i}$.

$$b_i = \frac{1}{20}\sum_{j=1}^{20} b_{ij} \tag{4.20}$$

where b_{ij} denotes the system condition for the j^{th} simulation

$$b_{ij} = \begin{cases} 1, & \text{system collpases.} \\ 0, & \text{system does not collapse.} \end{cases} \tag{4.21}$$

We define a map $\mathsf{Imp} : \mathsf{A} \to \mathbb{R}^+$ which assigns to each attack set $\mathsf{A_i} \in \mathsf{A}$ the impact on power system due to the attack. We have

$$\mathsf{Imp}(\mathsf{A_e}) = \beta_n \cdot n_i + \beta_b \cdot b_i \tag{4.22}$$

where n_i and b_i respectively indicate the number of nodes lost and the empirical probability of a blackout when the target set $\mathsf{A_i}$ is attacked. The factors β_b and β_n are suitable weights assigned to each impact measure. In this case, $\beta_n = 1$ and $\beta_b = 100$ are considered as suitable choices.

Chapter 5

Targeted Attack Setup

This scenario considers the case where an adversary strategically selects a set of substation buses and performs a physical attack at these locations. This study considers the case where the adversary aims to cause the maximum impact on the power system by attacking an optimal set of target nodes. When a particular substation bus is physically attacked, it creates a three phase fault on transmission lines and the transformers connected to it. This causes the protection systems in the power grid to respond and isolate the faulted section from the remaining system. The NERC TPL-001-1 standard requires the power grid to be operated in normal operating condition for the loss of a single system component ($N-1$ contingency) [69]. However, if the number of components lost exceeds 2, the occurrence of a widespread blackout in the grid is likely [70].

A cataclysmic event like the detonation of a bomb occurring in the power system can have the following outcomes: (a) minor redistribution in power flow with no subsequent tripping, (b) major redistribution in power flow with little or no subsequent tripping, and (c) cascade scenario leading to widespread tripping and instability. In the first two outcomes, the power system reaches a new equilibrium point whereas the system collapses almost immediately in the third outcome. The final equilibrium point is stable for outcome (a) while it may or may not be stable for outcome (b). When it comes to understanding the effects of an event, outcomes (a) and (c) are fairly easy to generalize. An outcome like (a) will cause minor oscillations in the responses of the generating machines that are located in the vicinity of

the event and will typically subside within a few seconds. An outcome like (c) will cause voltage/frequency imbalance and will cause large number of lines/generators to trip in a very short time-frame (few seconds). However, an outcome like (b) is difficult to generalize. The reason for this is that although the system does reach an equilibrium point, there is no guarantee that it will continue to be stable especially if any subsequent minor change occurs in the system. Thus, it needs to be examined on an event-specific basis. In this work, we analyze these three outcomes for several targeted attack scenarios.

5.1 Simulation setup:

For the purpose of simulating the actual sequence of events, three states of the power system are considered:

(i) Pre-attack state: this state represents the stable equilibrium point of the power system where it operates before the attack occurs;

(ii) The attack state: this state represents the targeted attack on the group of nodes. A sudden three phase fault occurs at the targeted buses along with three phase faults in the lines and transformers connected to them. The system stays in this state momentarily before the protective devices comes into operation;

(iii) Post-attack state: this state represents the operating point of the power system where it may return to a stable equilibrium point or might collapse altogether.

In this study, every simulation is performed for a time duration of 6.5s using PSS/E [71, 72]. The simulation is initiated for the power system condition in the synthetic network of Washington DC on May 22, 2010 at 1:00pm. The initiating event occurs at 0.5s and its effect on the power grid is studied for an additional 6s. At the end of each simulation, the impact

of the initiating event is evaluated as discussed in the next section. If a system collapse occurs prior to 6.5 seconds, the simulation is terminated at that instant and the impact is calculated. At the end of the simulation, the impact of targeted attack is evaluated based on two attributes: (*i*) the number of nodes lost or buses tripped: the higher the number, the more is the impact of the attack, since a bus trip results in the loss of load connected to it. and (*ii*) the occurrence of a system collapse. Fig. 5.1 shows the summary of steps involved in each simulation.

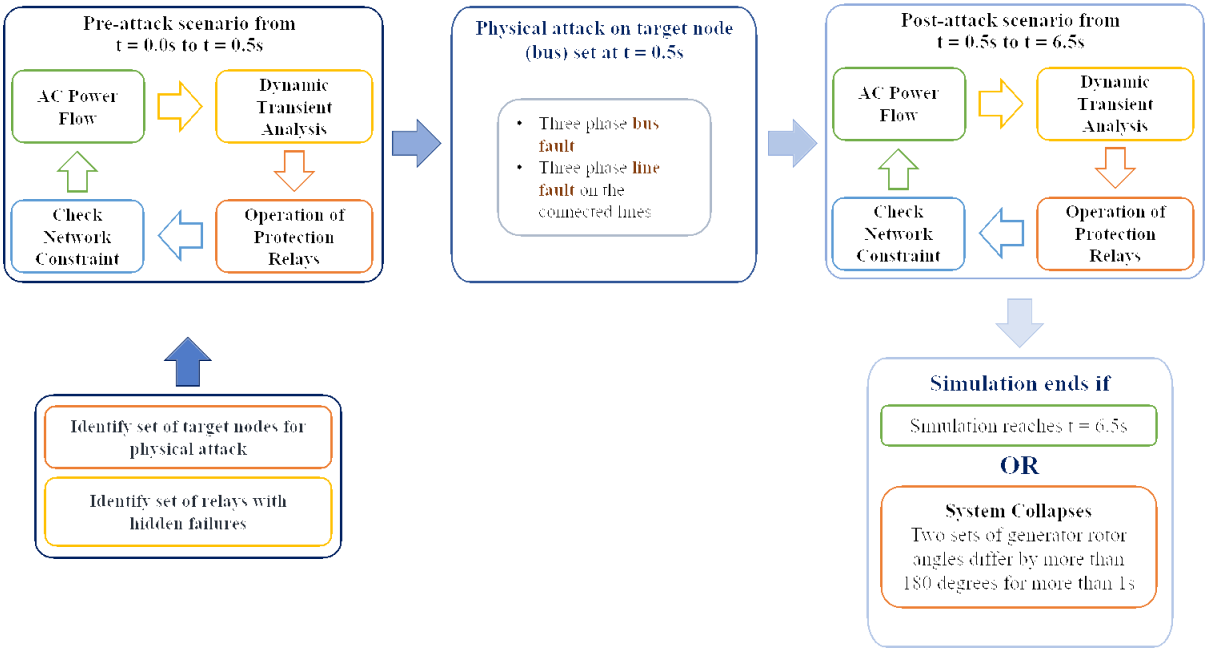


Figure 5.1: Flowchart showing steps in each simulation.

5.2 Optimal critical node problem

A fundamental problem that arises in this context is to identify *critical nodes* of the power network. We define the criticality of a set of target nodes S as the "impact" on power system, when they are attacked together. The impact can be measured in terms of many

metrics, e.g., the number of nodes lost, amount of load lost, the empirical probability of the occurrence of an unstable power swing, the voltage and frequency deviation etc. In this research two measures, viz. number of nodes lost and empirical probability of system collapse are used. The empirical probability is the ratio of number of simulations which resulted in unstable power swing to the total number of simulations. The set of nodes with the maximum criticality (over all subsets of the same size) is referred to as an optimum critical set.

Given a parameter k, the optimal critical node problem is to find a set of k nodes, whose failure will have the largest possible impact on the power grid. Since finding an optimal critical set is a challenging non-linear optimization problem, we study various heuristics to find sets with high criticality. We will use the terms "targeted" or "attacked" synonymously from now on.

In the following few sections, three heuristics would be proposed to identify the optimal critical set for a targeted attack. Each heuristic would be followed by example simulations depicting the selection strategy for target set size of $k = 3$. The nodes are selected from the substation buses in and around Washington DC. Though the transient stability analysis is performed on the entire EI, the statistical results is observed for only the region around Washington DC. This includes the control areas under Pennsylvania-New Jersey-Maryland (PJM) Interconnection, American Electric Power (AEP), Baltimore Gas and Energy (BG&E), Potomac Electric Company (PEPCO) and Dominion Virginia Power (DVP) [53, 54, 55, 56]. This area consists of 3571 nodes with 330 generator nodes. There are 4622 edges which consists of 3520 transmission lines and 1102 transformers.

5.3 High degree heuristic

This heuristic aims to select a subset T of k nodes from the original set S of N possible target nodes such that the sum of node degrees of the selected subset is maximum. Mathematically, we can express this problem as

$$\mathsf{T} = \arg \max_{\substack{\mathsf{T} \in \mathcal{P}(\mathsf{S}) \\ |\mathsf{T}|=k}} \sum_{s \in \mathsf{T}} \deg(s) \tag{5.1}$$

where $\mathcal{P}(\mathsf{S})$ denotes the power set of S and $\deg(\mathsf{s})$ denotes the degree of node s. Let D be the set of degrees of the nodes in S.

Remark 1. If the elements of D are unique, the solution to Eq. 5.1 is unique.

Proof. Let $\mathsf{S}^{\dagger} = \{s_1, s_2, \cdots, s_N\}$ denote the set of nodes $s \in \mathsf{S}$ sorted in descending order of their degrees. The solution of Eq. 5.1 is obtained by selecting the first k nodes of $\mathsf{S}^{\dagger}$. That is, $\mathsf{T} = \{s_1, s_2, \cdots, s_k\}$.

Remark 2. If the elements of D are not unique, the solution to Eq. 5.1 may not be unique.

Proof. Let $\mathsf{S}^{\dagger} = \{s_1, s_2, \cdots, s_N\}$ denote the set of nodes $s \in \mathsf{S}$ sorted in descending order of their degrees such that $\deg(s_1) > \deg(s_2) > \cdots > \deg(s_m) > \deg(s_{m+1}) = \cdots = \deg(s_{m+l}) > \cdots \deg(s_N)$. If $k \leq m$ or $k \geq m + l$, the choice is unique and is given by $\mathsf{T} = \{s_1, s_2, \cdots, s_k\}$. However, if $k \in [m + 1, m + l]$, then the choice of target nodes is given by $\mathsf{T} = \{s_1, s_2, \cdots, s_k\} \bigcup \mathsf{W}$, where W is a set of any $k - m$ nodes among l nodes in $\{s_{m+1}, s_{m+2}, \cdots, s_{m+l}\}$. Therefore, there are $\binom{l}{k-m}$ choices of target sets.

We pick the top k nodes with the highest degree (also referred to as having maximal connectivity). This has been suggested as the best choice in many prior works, e.g., as discussed in [47]. The highest degree nodes are those buses which have the highest number of transformers and transmission lines connected to it. Such a choice is motivated by the idea to

Algorithm 1 High degree heuristic to select target sets for adversarial attack

Require: k,S
1: Sort the nodes in set S in descending order of their degrees.
2: Solve Eq. 5.1 for the target set T
3: **if** The solution for T is unique **then**
4: Choose the target set T as the targets of adversary attack.
5: **else**
6: Evaluate impact of targeted attacks on all possible target sets.
7: Choose the target set which has the maximum impact.
8: **end if**

maximize the initial impact. If a substation bus with high degree is targeted, it experiences a three phase fault due to the blast along with all the edges connected to it. Therefore, a large number of branches are tripped resulting in a severe change in power flows in the system. Algorithm 1 shows the pseudo-code for this heuristic. A targeted attack on these nodes would lead to the highest number of line outages resulting in higher chance of an unstable power swing. We now consider two sets of simulations as examples for this heuristic. In the first set, the target nodes are chosen from all nodes in the power system under consideration. For the second set of simulations, the target nodes are selected only from the set of 500kV nodes.

5.3.1 Targets selected from entire power grid

Let $\mathsf{G} = (\mathsf{V}, \mathsf{E})$ denote the entire power system network. In this case, we consider the possible target set $\mathsf{S} = \mathsf{V}$. Using Algorithm 1, the nodes are sorted in descending order of their degrees. Among the set of all nodes in the power system under consideration, there are five high degree nodes denoted by Target ID A,B,C,D and E. The voltage ratings of these five high degree nodes are listed in Table 5.1. Each of these nodes have a degree of 16. This implies that each node has 16 edges connected to it. Therefore, a fault in the target node results in a three phase fault in the connected edges and hence leads to multiple outages.

Table 5.1: Voltage of high degree nodes in the power system

Target ID	A	B	C	D	E
Voltage (kV)	345	230	230	138	138

For target set size $k = 1$, we have $\binom{5}{1}$ or 5 possible target sets. Similarly, we have $\binom{5}{2}$ or 10 choices for target sets of size $k = 2$ and $\binom{5}{3}$ or 10 possible target sets of size $k = 3$. Fig. 5.2 shows the comparison of impact when the 25 possible target sets are attacked individually. Fig. 5.2a shows comparison of the number of nodes lost in the course of the simulation and Fig. 5.2b shows the fractional number of simulations resulting in unstable power swing. Fig. 5.2c shows comparison of the overall impact of the attack on the 25 possible target sets.

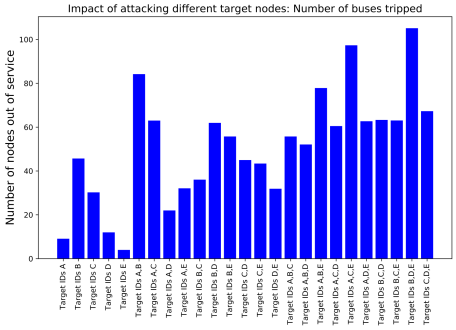
5.3.2 Targets selected from 500kV nodes

In this set of simulations the high degree nodes are chosen only from the 500kV nodes. Let $\mathsf{V}^{\dagger} \subset \mathsf{V}$ denote the 500kV nodes in the power system. In the power grid around Washington DC there are 31 nodes with voltage level at 500kV and hence $|\mathsf{V}^{\dagger}| = 31$. These nodes are named as Target ID $1, 2, \cdots, 31$. The degree of these 31 nodes are shown in Fig. 5.3. The high degree nodes are identified to be Target IDs $18, 21, 22$ and 23 and their corresponding degrees are shown in Table 5.2.

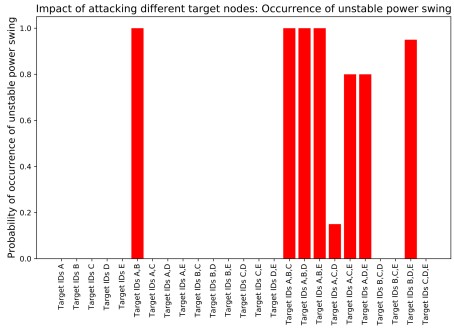
Table 5.2: Degree of highly connected 500kV target nodes

Target ID	18	21	22	23
Degree	7	7	13	7

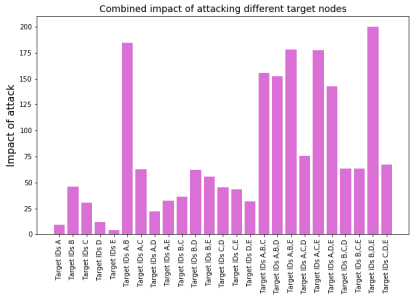
When the nodes are arranged in descending order of degree, the first four nodes are Target IDs 22,18,21 and 23. For target set size of $k = 1$, the choice according to Algorithm 1 would be only Target ID 22. Similarly, for target set size of $k = 2$, the choices would be



(a) Mean number of node outages.



(b) Empirical probability of system collapse.



(c) Overall impact of targeted attacks.

Figure 5.2: We compare impact of targeted attack on high degree nodes with target set sizes $k = 1, 2, 3$. For target set size of $k = 1$, attacking Target ID B results in the maximum impact. The target set comprising Target IDs A,B leads to maximum impact for target set size $k = 2$. For target set size $k = 3$, the maximum impact is caused by the set consisting of Target IDs B,D,E.

three; combining Target ID 22 with any one of Target IDs 18,21 and 23. For $k = 3$, there are three choices. However, in order to assess the efficacy of the heuristic, we consider all possible selections of $k = 1, 2, 3$ nodes from the four high degree target nodes (Target IDs 22,18,21 and 23). This gives us 14 possible combinations of the four nodes. Fig. 5.4 shows the comparison of impact when the 14 possible target sets are attacked. Fig. 5.4a shows comparison of the number of nodes lost in the course of the simulation and Fig. 5.4b shows the fractional number of simulations resulting in system collapse. Fig. 5.4c shows comparison of the overall impact of the attack on the 14 possible target sets.

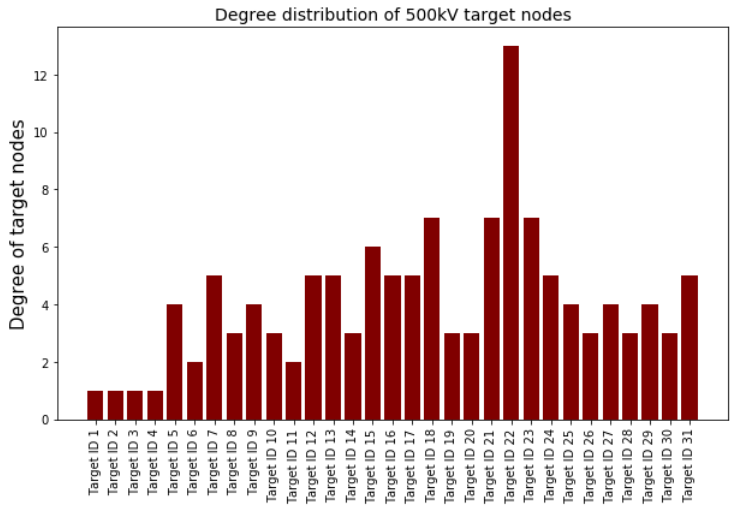


Figure 5.3: Comparison of degree of 500kV nodes in the power grid.

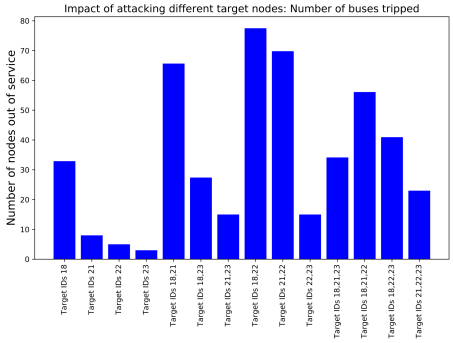
Algorithm 2 Greedy heuristic to select target sets for adversarial attack

Require: k,S
1: Initialize target set $\mathsf{T} = \emptyset$.
2: **while** length of the target set is less than k $|\mathsf{T}| < k$ **do**
3: **for** each node $s \in \mathsf{S}$ **do**
4: Choose target set by add node s to the set T as $\mathsf{A} = \mathsf{T} \bigcup \{s\}$
5: Evaluate impact of targeted attack on the target set A.
6: **end for**
7: Choose the target set $\mathsf{A}^\star$ which resulted in the maximum impact.
8: Remove the newly added node from the input set $\mathsf{S} = \mathsf{S} \setminus \mathsf{A}^\star$ and update the new target set $\mathsf{T} = \mathsf{A}^\star$.
9: **end while**

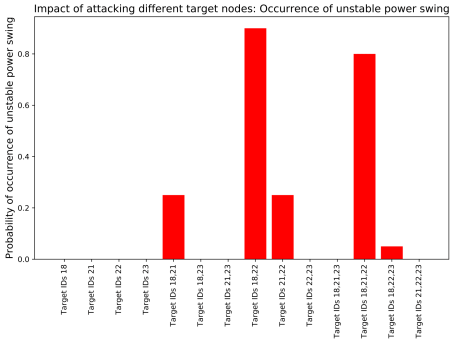
5.4 Greedy heuristic

In this heuristic, we pick k nodes in successive iterations from the power grid. In each iteration, the node which leads to the maximum additional impact is added to the target set. Algorithm 2 shows the pseudo-code for selecting target nodes using this heuristic. This strategy is motivated by greedy algorithms, which has been shown to be very effective in some problems (see [51]). The details of this heuristic is discussed below.

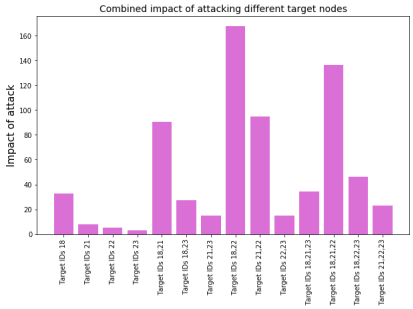
The optimal critical node set of size k is built through k iterations by adding one node in



(a) Mean number of node outages.



(b) Empirical probability of system collapse.



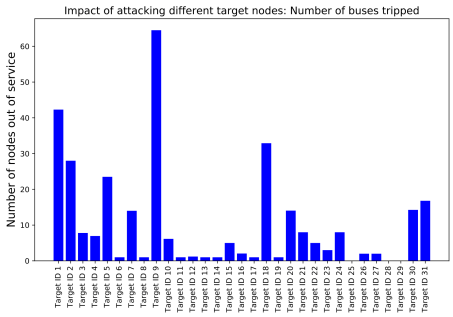
(c) Overall impact of targeted attacks.

Figure 5.4: We compare impact of targeted attack on high degree 500kV nodes with target set sizes $k = 1, 2, 3$. For target set size of $k = 1$, attacking Target ID 18 results in the maximum impact. It is interesting to note that this is not the highest degree node. The target set comprising Target IDs 18,22 leads to maximum impact for target set size $k = 2$. For target set size $k = 3$, the maximum impact is caused by the set consisting of Target IDs 18,21,22.

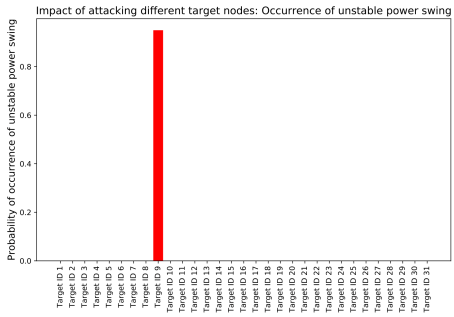
each iteration. Due to large number nodes (4277) in the power grid under consideration, the choice of target nodes has been limited to only 500kV buses. As discussed before, there are 31 of them and they are named as Target ID $1, 2, \cdots, 31$. The greedy heuristic is used to build the target node set of size $k = 3$ through 3 iterations. These three iterations are detailed below.

5.4.1 Iteration 1

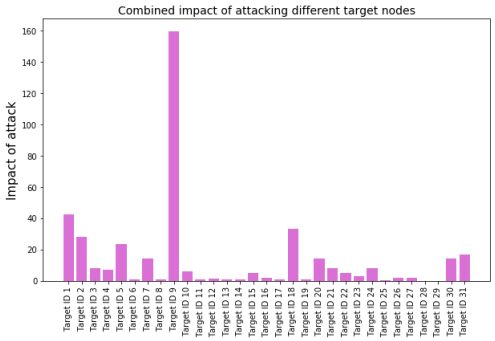
Fig. 5.5 shows the comparison of impact when the 31 possible 500kV target nodes are attacked individually. The target node which results in the maximum impact would be added as the first element in the optimal critical target set. Fig. 5.5a shows comparison of the number of nodes lost and Fig. 5.5b shows the fractional number of simulations resulting in system collapse. Fig. 5.5c shows comparison of the overall impact of the attack on 31 target nodes. It is observed that Target ID 9 results in the maximum impact.



(a) Mean number of node outages.



(b) Empirical probability of system collapse.

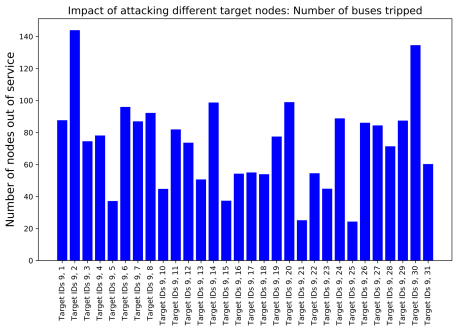


(c) Overall impact of targeted attack.

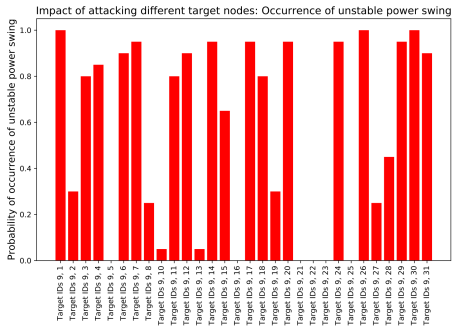
Figure 5.5: Iteration 1: We compare impact of targeted attacks of 500kV nodes sets of size $k = 1$. We see that Target ID 9 causes the maximum impact. We would include this node in all the target sets for the successive iterations.

5.4.2 Iteration 2

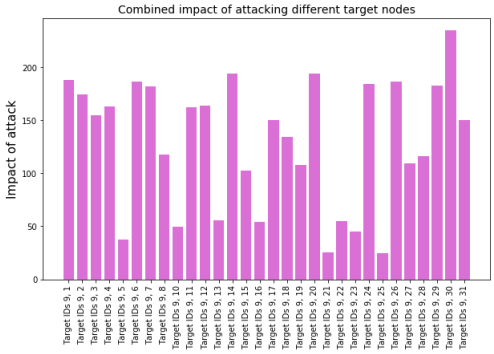
In the preceding iteration, Target ID 9 has been identified as the target node resulting in maximum impact. Fig. 5.6 shows the comparison of impact when the target set includes Target ID 9 and each of remaining 30 nodes. The set which results in the maximum impact would be considered for the following iteration. Fig. 5.6a shows comparison of the number of nodes lost and Fig. 5.6b shows the fractional number of simulations resulting in system collapse. Fig. 5.6c shows comparison of the overall impact of the attack on 30 target sets. It is observed that target set with nodes 9 and 30 results in the maximum impact.



(a) Mean number of node outages.



(b) Empirical probability of system collapse.

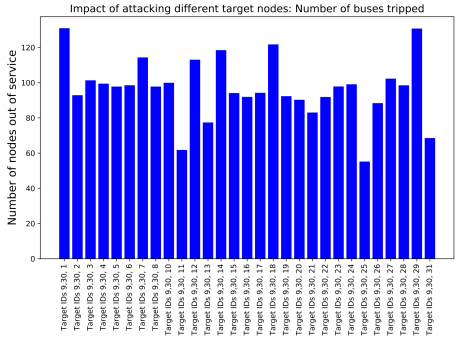


(c) Overall impact of targeted attack.

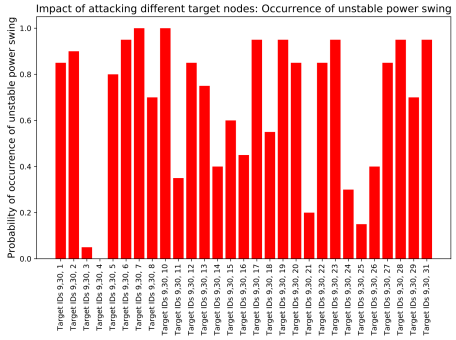
Figure 5.6: Iteration 2: We compare impact of targeted attacks of 500kV nodes sets of size $k = 2$. We see that target set comprising of Target IDs 9 and 30 causes the maximum impact. We would include these pair of nodes in all the target sets for the successive iterations.

5.4.3 Iteration 3

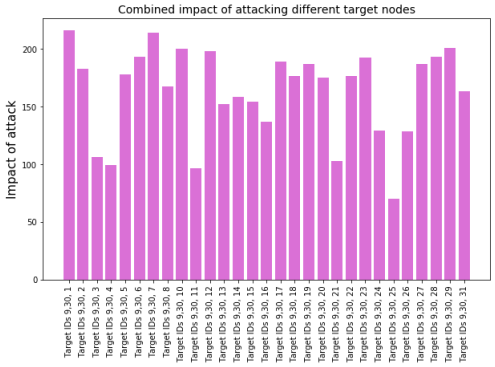
In the previous iteration, Target ID 9,30 has been identified as the target set of size $k = 2$ resulting in maximum impact. Fig. 5.7 shows the comparison of impact when the target set includes Target IDs 9,30 and each of remaining 29 nodes. Fig. 5.7a shows comparison of the number of nodes lost and Fig. 5.7b shows the fractional number of simulations resulting in system collapse. Fig. 5.7c shows comparison of the overall impact of the attack on 29 target sets. It is observed that target set with nodes 9,30 and 1 results in the maximum impact.



(a) Mean number of node outages.



(b) Empirical probability of system collapse.



(c) Overall impact of targeted attack.

Figure 5.7: Iteration 3: We compare impact of targeted attacks of 500kV nodes sets of size $k = 3$. We see that target set comprising of Target IDs 9, 30 and 1 causes the maximum impact. We would include these three nodes in all the target sets for the successive iterations.

Algorithm 3 Greedy heuristic to select target sets for adversarial attack

Require: k,S
1: **for** each node $s \in \mathsf{S}$ **do**
2: Compute the impact of targeted attack on target set $\mathsf{A} = \{s\}$ using Eq. 5.2.
3: Compute the probability of selection of node s in the target set using Eq. 5.3
4: **end for**
5: Draw k random sample nodes without replacement from S to build set T.

5.5 Random heuristic

Another option to evaluate the optimal set of k critical nodes would be to calculate the impact of attacking sets of k nodes from a possible set of N target nodes. This results in the number of choices to be $\binom{N}{k}$, which can be compared to obtain set resulting maximum impact. However, evaluating all the possible choices can increase the computational burden. This can be avoided by employing the following heuristic.

Let S denote the set of N possible target nodes given by $\mathsf{S} = \{s_1, s_2, \cdots, s_N\}$. We define a mapping $g : \mathsf{S} \to \mathbb{R}^+$ which assigns to each target node $s_i \in \mathsf{T}$ the impact on the power system due to the attack on only that target node. We have

$$g(s_i) = \mathsf{Imp}(\{s_i\}) \tag{5.2}$$

where $\mathsf{Imp}(\cdot)$ indicates the impact of an attack on target set $\cdot$ computed using Eq. 4.22.

The probability of selecting the node s_i in the optimal target set is given by

$$\mathbb{P}[s_i] = \frac{g(s_i)}{\sum_{i=1}^{N} g(s_i)} \tag{5.3}$$

The optimal set of k target nodes is selected by random sampling from set S without replacement. The sampling is performed based on the probabilities of selection as computed in Eq. 5.3. Algorithm 3 shows the pseudo-code for the proposed random heuristic.

For this heuristic, the target set is chosen randomly depending on the impact of targeted attacks when the nodes are attacked individually. For this purpose, 500 simulations are run to have different choices of target sets of size $k = 3$. The impact of each attack is evaluated using the relation in Eq. 4.22. Choosing target nodes randomly provides an overall picture of the impact of a targeted attack on the power grid.

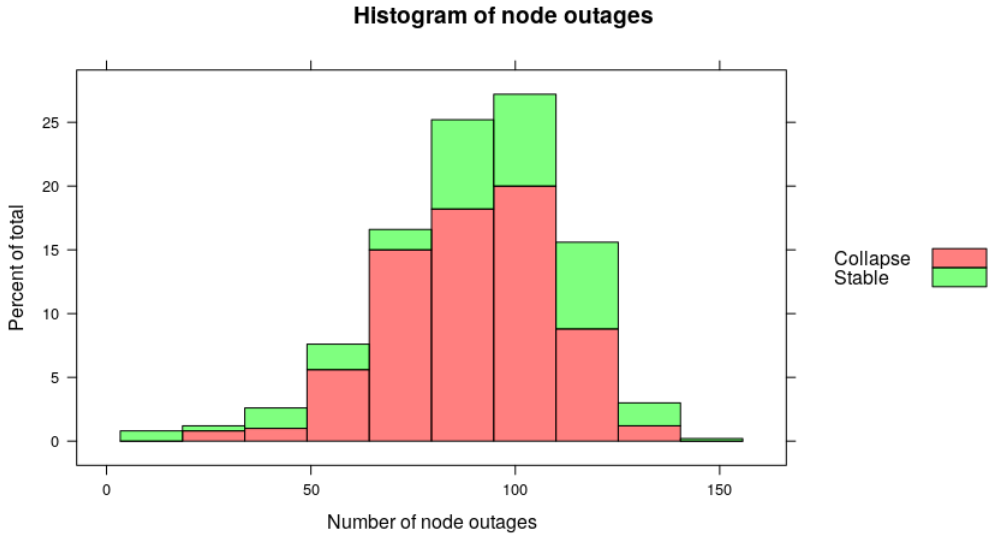


Figure 5.8: Histogram of node outages for stable and unstable outcome of cascading events. This shows the relative distribution of stable and unstable systems as a result of a targeted attack on target sets of size $k = 3$. It is noted that a power system collapse is more likely when target set size of $k = 3$ is considered.

Fig. 5.8 shows the histogram of node outages. The colors represent relative frequencies of the outcome of cascading events in terms of the power grid stability. The histogram of impact is shown in Fig. 5.9. One of the important observations from this histogram is the fact that it is not a bell shaped histogram. On the contrary, a targeted attack with large impact is more frequent than low impact cascading events.

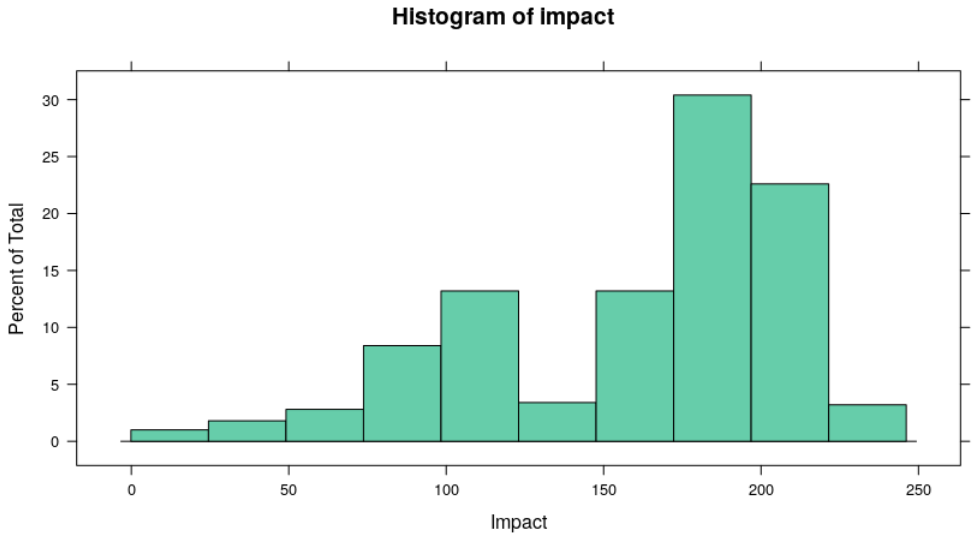


Figure 5.9: We consider the histogram of impact of targeted attack. It is noted that using this heuristic, the targeted attack is more likely to result in a large impact. Therefore, this heuristic is effective in identifying a sub-optimal critical target set.

Chapter 6

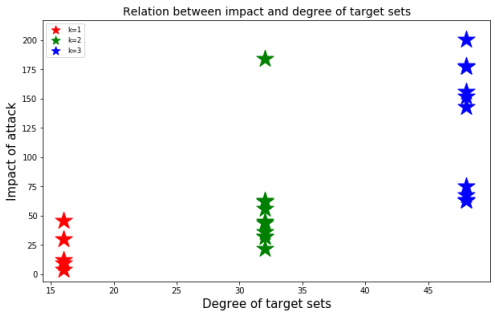
Results and Discussion

A number of simulations have been performed on the simulation setup discussed in the previous chapter. This chapter deals with some important observations made for the different cascading failure scenarios. Particularly, the three heuristics to identify the optimal critical node set are extensively analyzed and most results are observed from this analysis. Due to large computational necessity, the optimal critical set problem is considered for set sizes of $k = 1, 2, 3$ only.

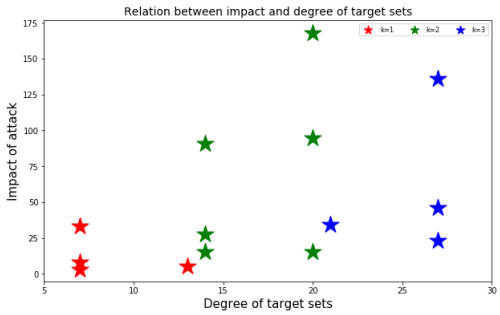
6.1 Relation of impact and degree of target set

One of the most interesting observation made for the different heuristics was the relation between the impact of targeted attack and the degree of target set. The degree of a target set is the sum of the degrees of the constituent nodes. Many prior works [23, 25, 26, 46] have assumed highly connected nodes in the network to be the most critical nodes and have studied cascading events as a result of a targeted attack on these nodes. However, such assumption is true when cascading failure models are developed based on simplified dynamics like sandpile model. However, when we consider the actual power system dynamics along with the role of protection and control systems associated with it, the above assumption may not hold true.

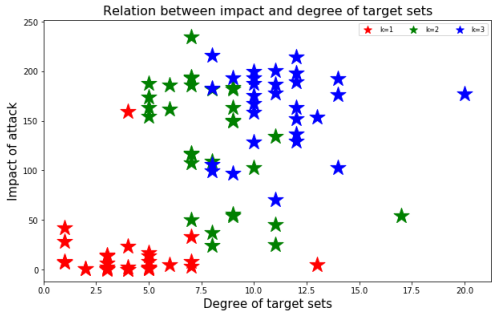
Fig. 6.1a shows the relation between impact of targeted attack and the degree of target sets.



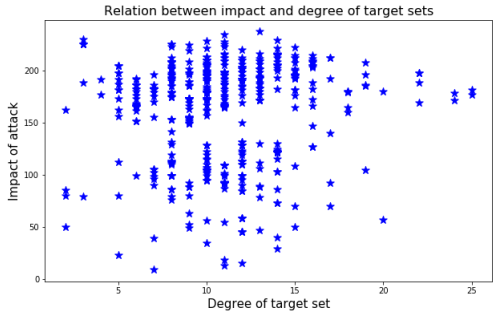
(a) Targeted nodes selected using high degree heuristic on all nodes.



(b) Targeted nodes selected using high degree heuristic on 500kV nodes.



(c) Targeted nodes selected using greedy heuristic on 500kV nodes.



(d) Targeted nodes selected using random heuristic on 500kV nodes.

Figure 6.1: We compare the variation of impact of targeted attack with degree of target sets. The targeted node sets are chosen using different heuristics. The assumption in prior works that targeting high degree node sets leads to maximum impact does not hold true for all cases.

The nodes for targeted attack is chosen using the high degree heuristic on the entire power system under consideration as discussed in Section 5.3.1 in Chapter 5. The degree of a target set indicates the number of lines or transformers which are affected by a targeted attack. These are the edges in the network which experience a three phase fault at the instant of attack and are tripped. It is observed that an attack on a larger target set results in an increased impact. The red markers correspond to high degree target sets of size $k = 1$ (each of the node has a degree of 16). Similarly, the green and blue markers respectively represent the target sets of sizes $k = 2$ (having a total degree of 32) and $k = 3$ (having a total degree of 48). Though such monotonic relation between impact and target set size is observed, the

monotonic nature is not necessarily obvious.

Fig. 6.1b shows the relation between impact and degree of target sets. In this case, the targets chosen using high degree heuristic on 500kV nodes as discussed in Section 5.3.2 in Chapter 5. The red, green and blue markers respectively represent the impact of targeted attacks on node sets of sizes $k = 1, 2$ and 3. It is observed that the monotonic nature of the relation is not true for this case. Fig. 6.1c shows the relation between impact and degree of target sets considered in greedy heuristic which is discussed in Section 5.4 in Chapter 5. The red, green and blue markers respectively represent the impact of targeted attacks on node sets of sizes $k = 1, 2$ and 3. The non-monotonic nature of the relation is further observed in this case.

6.2 Non-monotonicity of criticality

One of the notable observations made from the targeted attack simulations is the non-monotonic behavior of the impact with the target set size. In this context, criticality of a target set is the impact when nodes in the set are attacked simultaneously. A non-monotonic behavior means that adding nodes to the target set does not necessarily imply an increased impact. In this section, an attempt to explain such phenomena is made. Three examples are considered in order to do so:

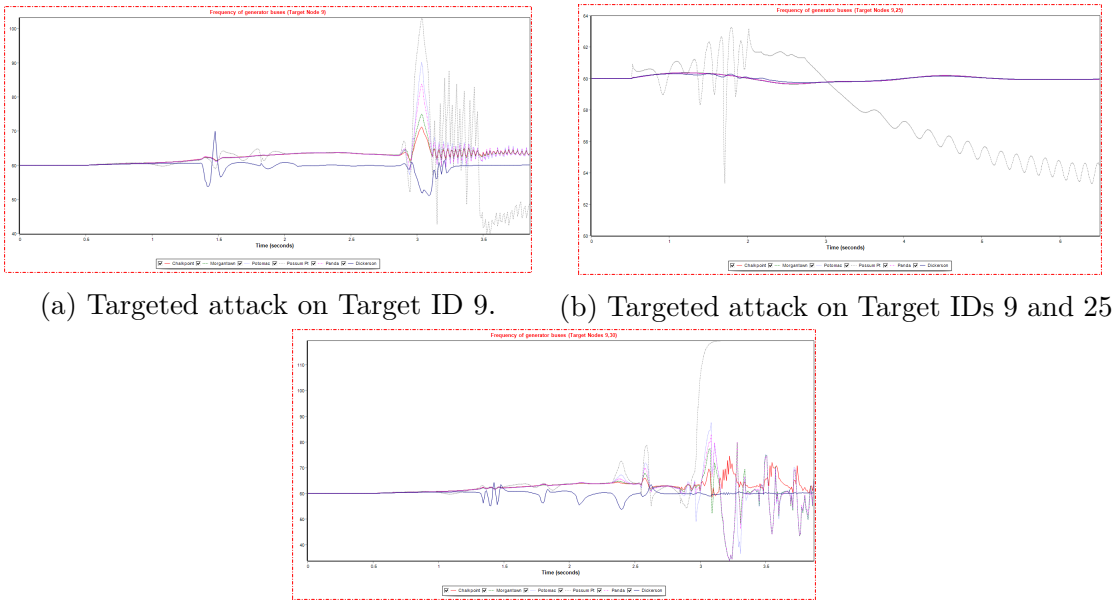
1. The target set consists of a single node Target ID 9. From Fig. 5.5 it is known to produce maximum impact resulting in the occurrence of a system collapse.

2. The target set consists of two nodes Target IDs 9,25. From Fig. 5.6 it is known to result in the minimum impact when Target ID 9 is combined with other 500kV nodes. Though general intuition indicates that target set consisting of Target ID 9 along with

other nodes would result in an increased impact, this example shows an opposite result where the system becomes stable.

3. The target set consists of two nodes Target IDs 9,30. From Fig. 5.6, this is known to produce the maximum impact when Target ID 9 is combined with other 500kV nodes.

6.2.1 Response of generators



(a) Targeted attack on Target ID 9.

(b) Targeted attack on Target IDs 9 and 25.

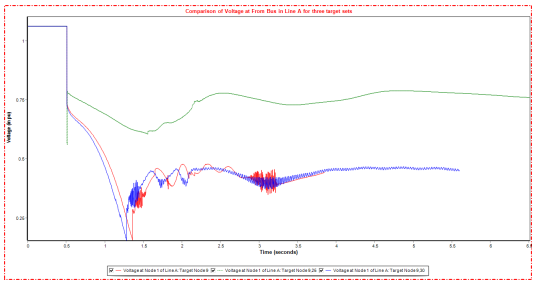
(c) Targeted attack on Target IDs 9 and 30.

Figure 6.2: Frequency at major generating stations for different targeted attacks. For the first and third attack, we observe the frequency at all the generating stations to oscillate considerably which is an indication of an unstable system. For the second attack, the frequency at most of the generating stations is steady indicating a stable system in the aftermath of the attack.

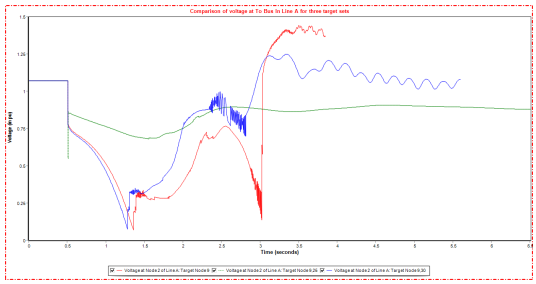
The frequency at the major generating stations in and around Washington DC for the three targeted attacks are shown in Fig. 6.2. For a targeted attack on Target ID 9, all the generating stations are affected which is evident from the oscillations in the frequency curves in Fig. 6.2a. This also agrees with the observation that such an attack results in system collapse. Fig. 6.2b

shows the variation of generator bus frequencies when Target IDs 9 and 25 are attacked. It is observed that except the Possum generating station, the frequencies at other stations are at 60Hz which agrees with our original observation that the system is stable. When Target IDs 9 and 30 are attacked together, all the generating stations are affected and system collapse occurs.

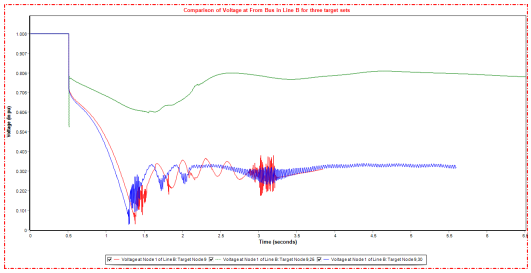
6.2.2 Variation of voltage at different 500kV buses



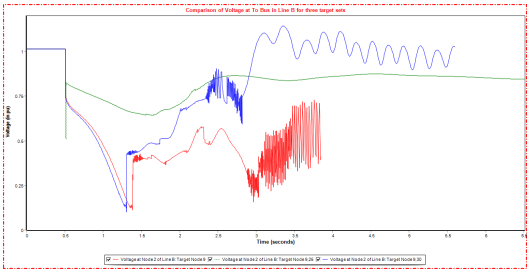
(a) Bus voltage at from bus of Line A.



(b) Bus voltage at to bus of Line A.



(c) Bus voltage at from bus of Line B.



(d) Bus voltage at to bus of Line B.

Figure 6.3: We compare the bus voltages at two ends of Lines A and B for three targeted attacks. We observe that for the first (red) and third (blue) attack, the bus voltages drop considerably as compared to the second (green) attack.

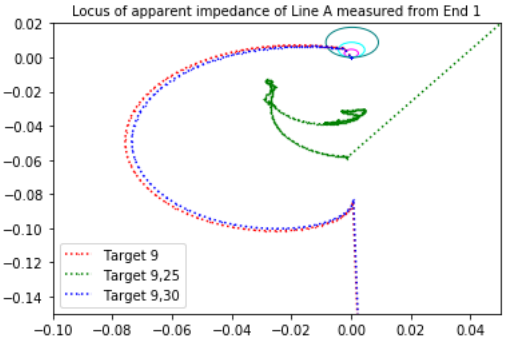
In order to explain this non-monotonic behavior, two representative 500kV transmission lines are considered namely Line A and Line B. It is to be noted that these lines are not affected directly by either of the three targeted attacks. That is, none of these lines trip at the instant of the three targeted attacks. However, bus voltages at the ends of these lines are affected in different ways for the three targeted attacks as shown in Fig. 6.3. It can be observed that

the bus voltages at the ends of these lines decrease significantly when Target ID 9 is attacked individually (red curves) and Target IDs 9 and 30 attacked together (blue curves). When Target IDs 9 and 25 are attacked together, the voltage drop is not significant.

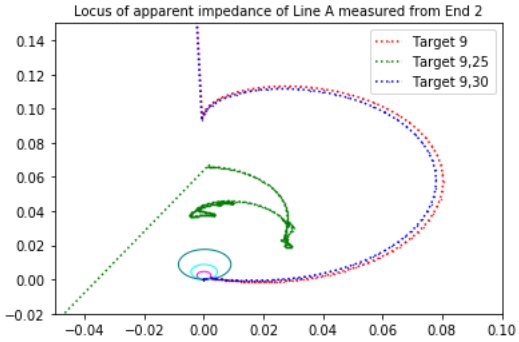
6.2.3 Trajectories of apparent impedance

Next, it is important to note that when several 500kV lines are lost due to the targeted attack, the current in the neighboring transmission lines increase in order to maintain the same power flow in the grid. Therefore, the rise in current flow through the 500kV lines are a common occurrence for all the lines; but only a few of them are affected by significant voltage collapse at the ends. This, in turn, causes the apparent impedance measured in certain lines to decrease significantly as compared to other lines. Fig. 6.4 shows the trajectories of apparent impedance for the three targeted attacks. The circular characteristics are the zones of protection for the lines (magenta: zone 1, cyan: zone 2 and teal: zone 3). The apparent impedance trajectories for the three targeted attacks are denoted by red, green and blue dotted lines respectively.

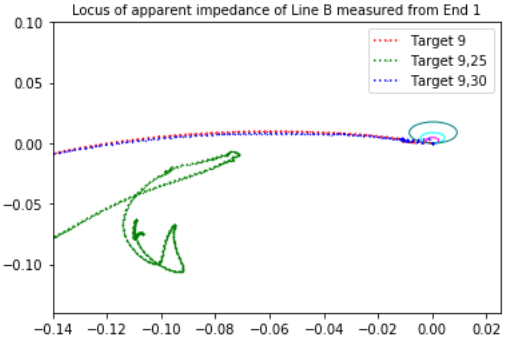
One of the important contribution of this work is the actual representation of edge/node failures in the power system network. Unlike popular failure models like sandpile dynamics, thermal loading level based failure models etc., this work considers the role of protection systems. The operation of these protective relays are considered as the sole condition for node/edge failures. From Fig. 6.4, it is seen that the apparent impedance trajectory encroaches the zones of protection for the target sets $\{9\}$ and $\{9, 30\}$. However, the apparent impedance does not enter the zones of protection for a targeted attack on the set $\{9, 25\}$. Therefore, for the first and third targeted attack, the initial line and bus outages are followed by more 500kV line outages due to operation of mho relays on the lines. The outage of a



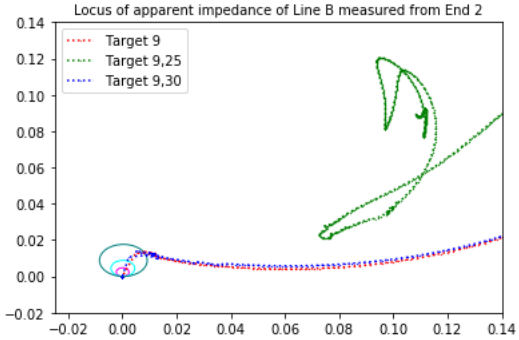
(a) Apparent impedance measured at from bus of Line A.



(b) Apparent impedance measured at to bus of Line A.



(c) Apparent impedance measured at from bus of Line B.



(d) Apparent impedance measured at to bus of Line B.

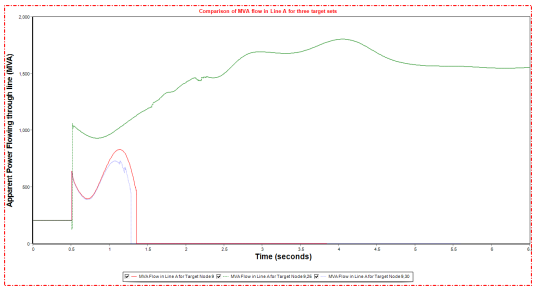
Figure 6.4: We compare the trajectories of apparent impedance at two ends of Lines A and B for three targeted attacks. We observe that for the first (red) and third (blue) attack, the trajectories enter the zone characteristics of the mho relays, and hence results in line trips. For the second (green) attack the trajectory does not enter the characteristics and hence the lines do not trip.

large number of 500kV lines causes a reduced reactive power support in the power system. This results in further voltage collapse due to lack of reactive power causing more lines to trip and leading to instability and system collapse.

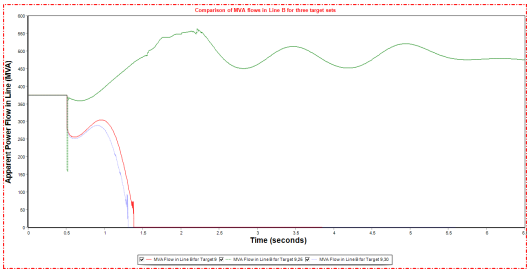
6.2.4 Variation of MVA flows in 500kV lines

Fig. 6.5 shows the MVA flow through the lines A and B for the three targeted attacks. The red and blue curves indicate the MVA flow through the lines for targeted attacks on sets

$\{9\}$ and $\{9, 30\}$ respectively. As explained in the previous discussion, these attacks cause the 500kV lines to trip as opposed to the attack on the target set $\{9, 25\}$. The difference in MVA flow between these three attacks is evident from Fig. 6.5.



(a) MVA flow through Line A for three targeted attacks.



(b) MVA flow through Line B for three targeted attacks.

Figure 6.5: We compare the MVA flowing through Lines A and B for three targeted attacks. We observe that for the first (red) and third (blue) attack, the lines trip and hence MVA flow drops to zero. This reduces the reactive power support leading to voltage drops and further line trips. For the second (green) attack the lines do not trip and hence the MVA flow is maintained leading to a stable condition.

6.2.5 Summary of discussion

We now consider a temporal representation of the three cascading scenarios in the synthetic power grid of Washington DC in Figure 6.6 to summarize the above discussion. The geographical location of the buses in the power system are not precisely represented in the figure due to sensitivity of the information. The black nodes in the networks denote the targeted nodes which fail at the first instant. The different colors of nodes/edges denote their mean time of failure over the 20 stochastic simulations performed for the same targeted attack.

In the first case, when a Target ID 9 is attacked, it results in a number of trips on the neighboring lines as explained in the previous discussion. Particularly, the outage of lines in the yellow ellipse creates a large deficit of reactive power which leads to a number of

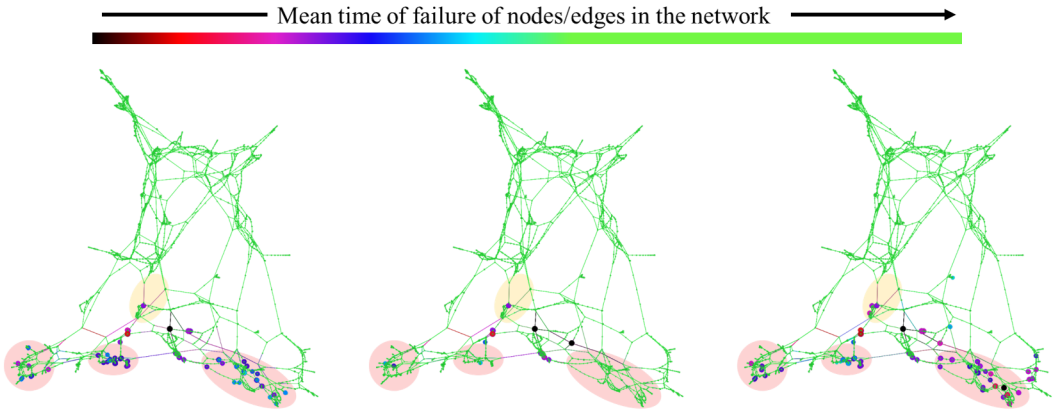


Figure 6.6: We compare the effect of three different targeted attacks on the power system. In the first attack (Target ID 9) and third attack (Target ID 9,30) the lines inside the yellow ellipse trips and this leads to generator trips in the red ellipses. In the second attack (Target ID 9,25) the lines in the yellow ellipse do not trip and the generator trips in the red ellipses are also avoided.

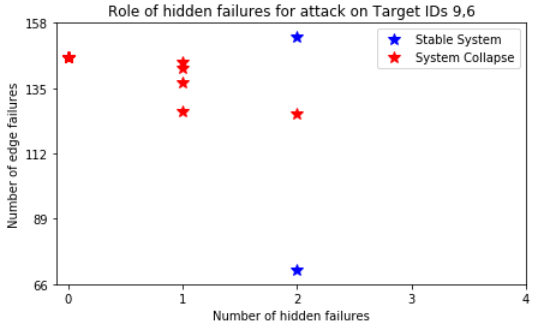
generator trips in the red ellipses. A loss of important transmission lines causes a voltage collapse in the system. This triggers the excitation control in nearby generators to increase excitation in order to deliver sufficient reactive power. If the excitation goes beyond limits, it results over-excitation protection trips. For generators failing to maintain the reactive power capacity, the voltage collapse causes under-voltage protection system of generators to trip.

However, in the second case when Target IDs 9 and 25 are attacked, the voltage at nodes in the yellow ellipse do not experience substantial voltage drop. Therefore, the lines do not trip, the system is saved from a voltage collapse and generators do not trip in the red ellipses. Within a few seconds, the system is stabilized. In the third case, the selected targets results in voltage collapse in the lines within the yellow ellipse leading to removal of these lines. This creates a similar situation as in the first case and leads to tripping of lines in the yellow ellipse. This is shortly followed by the generator trips in the red ellipses and system becomes unstable due to loss of large number of generators.

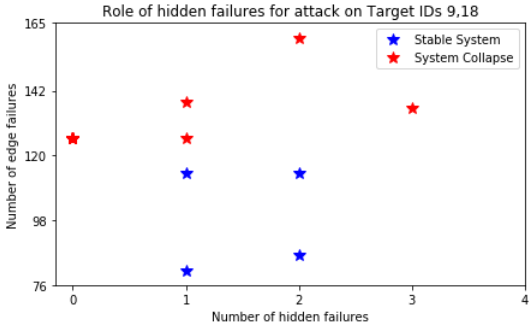
6.3 Role of hidden failures

One of the important aspects of this work is the modeling of hidden failures in the protection systems for the transmission lines and transformers. Much of the prior work on hidden failures has been concentrated on their ill impact on system stability leading to cascading events. However, line outages caused by hidden failures often saves the power grid from system collapse. The role of hidden failures on the system stability has been discussed in this section.

(a) Role of hidden failures for targeted attack on Target IDs 9 and 11.



(b) Role of hidden failures for targeted attack on Target IDs 9 and 6.



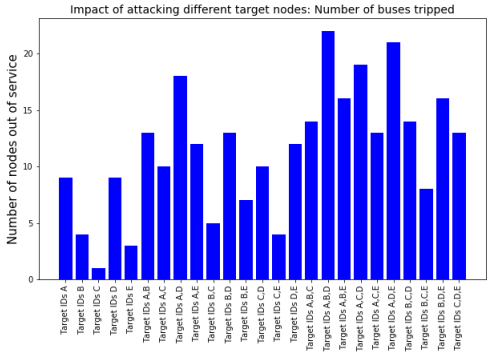
(c) Role of hidden failures for targeted attack on Target IDs 9 and 18.

Figure 6.7: Examples of power grid being saved from a system collapse due to hidden failures. In the absence of a hidden failure, the cascading events following the targeted attack leads to power system collapse. However, if one or more line trips due to presence of hidden failure, the cascading events has led to lesser number of edge outages and stabilizing the system.

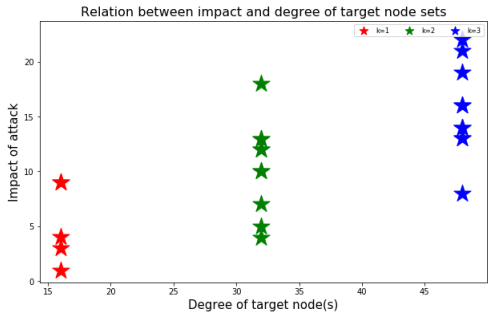
For example, consider a targeted attack on Target IDs 9 and 11. Fig. 6.7a shows the variation

of number of edge outages for 20 simulations of the targeted attack scenario. If no line trips due to a hidden failure, the simulation proceeds in a deterministic fashion and results in a fixed number of edge trips. However, of the line trips ue to hidden failures is non-zero, the outcome of the simulation is stochastic. In this scenario, if there is no line trips due to hidden failures, a system collapse occurs. However, a single outage due to the presence of a hidden failure can cause lesser number of edge trips and save the system from instability. Some other examples are depicted in Fig. 6.7b and Fig. 6.7c. More examples depicting the role of hidden failures in system stability has been included in Appendix C in Fig. C.1 - C.16. Such results indicate that it is important to identify such edges in the network whose outage can save the power grid from instability.

6.4 Comparison with DC power flow



(a) Number of node outages.

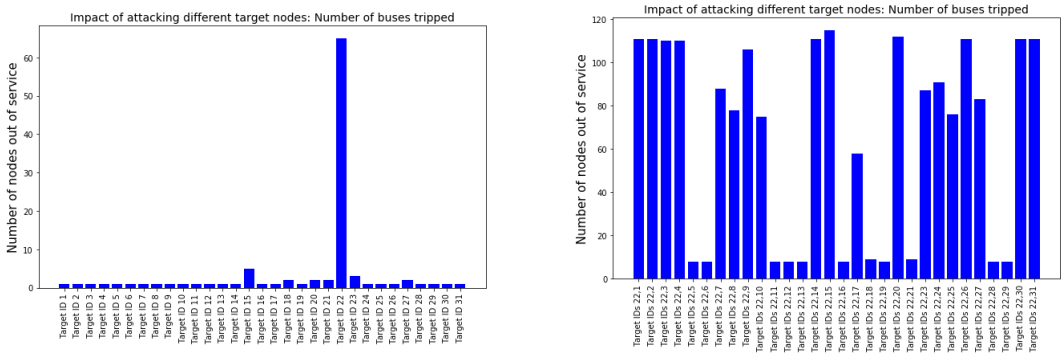


(b) Comparing impact of targeted attack with the degree of target nodes.

Figure 6.8: We observe the impact of targeted attack on high degree nodes using DC steady state analysis. The impact does not take into consideration any occurrence of power system collapse. The monotonic relation between impact and degree of target set is also observable.

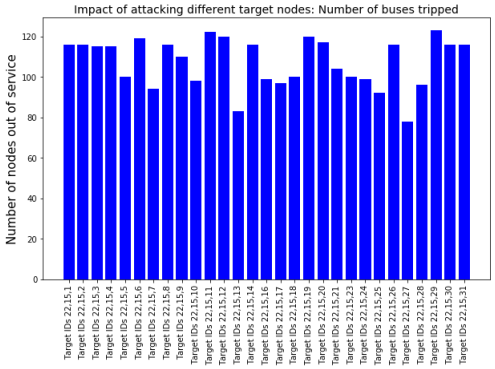
In this section, the traditional DC steady state analysis is compared with the proposed cascading failure model. For the DC power flow analysis, the admittance matrix and power injections at each bus in the power system are evaluated. With the usual assumption of

flat voltage profile at each bus and neglecting reactive power, the bus voltage angles are estimated. A transmission line is tripped if the electrical angular separation between the ends is more than 70 degrees as used in [69]. The sae set of process is executed until there are no more outages. A node with no edges connected to it is considered as a tripped node. Fig. 6.8 depicts the impact of targeted attack on high degree nodes in the network. In comparison with Fig. 5.2, the DC steady state analysis provides an underestimate to the number of node outages. Furthermore, it does not identify a power system collapse due to transient instability.



(a) Number of node outages for target set of size $k = 1$.

(b) Number of node outages for target set of size $k = 2$.



(c) Number of node outages for target set of size $k = 3$.

Figure 6.9: We compare impact of targeted attack on 500kV nodes chosen by greedy heuristic evaluated using DC steady state analysis. Since high degree nodes are seen to result in a high impact, they get included in the target set.

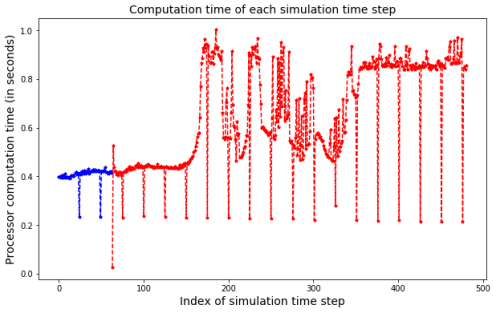
Fig. 6.9 shows the impact of targeted attack on 500kV node sets of sizes $k = 1, 2, 3$ analyzed using DC steady state analysis. Target ID 22 is evaluated to be the most critical target node when target sets of size $k = 1$ is considered. This does not agree with the transient stability analysis performed in the earlier sections since the DC power flow analysis neglects power system collapse due to transient instability. Rather, the node with highest degree (Target ID 22) is identified as the most critical node.

6.5 Computational complexity

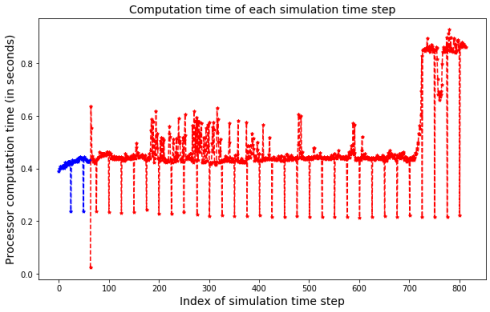
An important aspect of the research is to understand whether the proposed cascading failure model is scalable for large power systems. Since an AC power flow problem with transient stability analysis is performed at every instant of simulation, the computational time requirement is high for each cascading event scenario. Furthermore, we consider stochastic presence of hidden failures in the protective relays, which requires a large number of simulations to be performed for each cascading scenario. For this reason, a study is performed to understand the variation in computation time for each cascading scenario. This is followed by a comparison of the time required for every stochastic simulation of a single targeted attack scenario. All the simulations have been performed on an Intel Core i7-8750H CPU processor with 2.21GHz clock and RAM size of 16 GB.

6.5.1 Computational complexity of each simulation

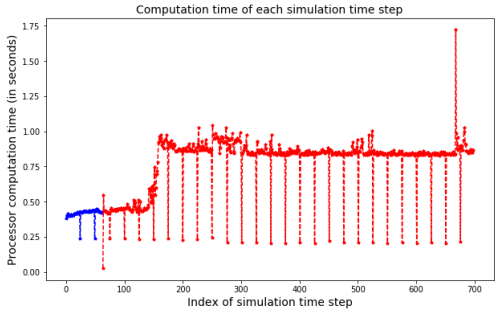
We consider the computation time required for three targeted attack scenarios in Fig. 6.10. Fig. 6.10a shows the computation time required for simulating each time step of a cascading scenario where Target ID 9 is attacked. From previous analysis in Section 6.2 that this results



(a) Computation time for targeted attack on Target ID 9.



(b) Computation time for targeted attack on Target IDs 9 and 25.



(c) Computation time for targeted attack on Target IDs 9 and 30.

Figure 6.10: We compare the computation time required for each time step in three cascading scenarios. The blue segments represent the computation time requirement for the initial steady state condition of 0.5s in each cascading scenario. Thereafter, the red segments represent the computation time required for simulating the post attack time instants. We observe that for the stable case of targeted attack on Target IDs 9 and 25, the computation time requirement is lower than that for the other two cases.

in a power system collapse. Similarly, Fig. 6.10b shows the same for targeted attack on Target IDs 9 and 25 which leads to a stable condition. Fig. 6.10c compares the computation time required for targeted attack on Target IDs 9 and 30. We know that this targeted attack leads to a power system collapse. The horizontal axis in the plots indicates indices of time instants in each simulation. The range of these indices is different because of the fact that the three simulations terminated at different time instants.

The initial time steps (denoted in blue segments) require almost the same computation time in each scenario since they simulate similar steady state conditions for 0.5s. However, the

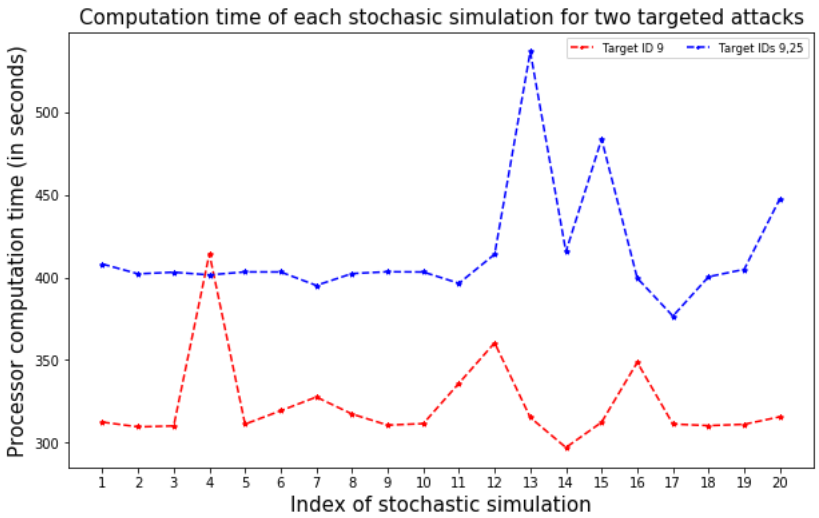


Figure 6.11: We compare the computation time required for 20 stochastic simulations of two targeted attack scenarios. The blue points indicate the time required for the stochastic simulations of the targeted attack on Target IDs 9 and 25. The red points show the time required for the stochastic simulations of the targeted attack on Target ID 9. The first attack leads to stable system conditions in most cases. Therefore, the simulations do not terminate early as in the case of the later targeted attack.

time requirement for post-attack time instants are different for each scenario. We observe that as the system tends to a collapse, the computation time requirement is high. Comparing the three attack scenarios, we can also say that the targeted attack leading to a stable system requires less computation time for each simulation time step than the unstable scenarios. However, the scenarios where power system collapse occurs, tend to terminate earlier (before 6.5s). Therefore, lesser number of time steps are required to be simulated for these cases.

6.5.2 Computational complexity of each targeted attack scenario

Now, we consider the computation time requirement for each stochastic simulation of the same targeted attack scenario. This study is performed to understand how presence of hidden failures tend to alter the computation time of the cascading event simulation. Fig. 6.11 shows the variation of computation time for 20 stochastic simulations of two targeted attack

scenarios. The blue plot indicates the time required for the stochastic simulations of the targeted attack on Target IDs 9 and 25. We know that most of these simulations have resulted in stable system conditions. Therefore, they have terminated at simulation time of 6.5s. In order to simulate the system for this duration, the computation time required is close to 7 minutes for each simulation. The red plot shows the time required for the stochastic simulations of the targeted attack on Target ID 9. Most of these simulations have led to a power system collapse much earlier than the simulation time of 6.5s. Therefore, the simulations were terminated much earlier. In this case, the computation time varies between 5 and 7 minutes for each simulation.

Chapter 7

Conclusions and Future Work

This work investigates the cascading events which follow as a consequence of a targeted adversarial attack on certain nodes in the power grid of Washington DC. In contrast to earlier work, a synthetic power system network along with the control and protection systems has been considered to ensure a realistic representation of the power grid. An AC power flow based transient stability assessment is performed to obtain a complete picture of the impact of such an attack on the power grid. This is evident from the comparison with DC steady state analysis which clearly provides an under-estimate of impact and neglects the occurrence of a system collapse.

The problem of identifying a set of k critical nodes is also considered. The goal of this problem is to identify the set of nodes which, if protected from adversarial attacks, can avoid the occurrence of cascading failures and system collapse. Due to the complexity of the problem, three simple strategies were used: a node degree-based selection, a greedy strategy and a random selection of nodes. It is observed that the greedy choice of target nodes often leads to more impact than a target set of high degree nodes. This is evident from the observation that a targeted attack on the highly connected nodes of the power grid causes a large number of node outages, yet the system is stabilized eventually. On the other hand, a targeted attack on certain selected high voltage nodes can cause blackouts in the grid due to instability. Furthermore, it is observed that increasing the number of targets does not necessarily increase the impact on the power grid. Such conclusions indicate that cascading

events in the power grid cannot be simply modeled using failure models inspired by self organized criticality like the sandpile dynamics model. The role of protective elements and the generator control systems need to be effectively modeled to analyze the cascading events accurately.

The effect of stochastic occurrence of hidden failures in the protection system on system stability on the post-attack scenario is an important contribution of this research. In general, hidden failures result in nuisance tripping and exacerbate disturbances in the power system. However, during cascading events, an unnecessary trip of a line due to a hidden failure can ultimately lead to a stable system.

The non-monotonicity of criticality indicates that the greedy strategy does not necessarily ensure the optimal set of k target nodes to maximize the attack. An adaptive greedy strategy of choosing target nodes might generate the optimal critical node set. This would include combining the greedy strategy with high degree heuristic. A detailed study of such a strategy is one direction for future work.

Another important aspect of cascading events in the power system is the order of transition as discussed in Pahwa et.al [43]. The impact of targeted attack depends on the choice of target nodes which has been studied in this research work. The impact also varies with different loading conditions of the power system network. This study would enable us to understand the nature of transition and identify the critical loading level of the network. The variation of impact with different rates of occurrence of hidden failures is another important aspect. Such a study would help us to identify the critical rate of occurrence of hidden failures at which a small targeted attack can lead to widespread outages.

However, such detailed study requires sufficient number of stochastic time-domain simulations to be performed. Therefore, the computational complexity of the cascading failure

model is an important aspect of the work. At present, the computational time for each stochastic simulation is sufficiently high. This can be reduced by parallel processing algorithms to solve the differential algebraic transient power flow equations at every instant. Another way to reduce the computation time is to use approximate models like steady state analysis with DC/AC power flow. However, these models do not capture the entire dynamics of the power system accurately. Therefore, these methods can be used along with decision tree based cascading failure models to study large number of cascading event scenarios. The existing simulation results can be used to formulate the decision trees to identify failure paths in the network. Many prior works use the loading of a transmission line to determine its tripping probability. However, the apparent impedance or current flowing through the line can be a better alternative since protective devices operate on these variables. Such considerations along with steady state analysis can also reduce the computation time and make the model scalable for large systems. These are some possible directions of future research work.

Bibliography

[1] White Paper. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive, 1998. URL https://clintonwhitehouse4.archives.gov/WH/EOP/NSC/html/documents/NSCDoc3.html.

[2] R. Meyur, A. Vullikanti, M. V. Marathe, A. Pal, M. Youssef, and V. Centeno. Cascading Effects of Targeted Attacks on the Power Grid. In *Complex Networks and Their Applications VII*, pages 155–167, Dec 2018.

[3] C. Barrett, R. Beckman, K. Channakeshava, F. Huang, V. S. A. Kumar, A. Marathe, M. V. Marathe, G. Pei, and S. Saha. Human Initiated Cascading Failures in Societal Infrastructures. *Public Library of Science*, 7(10):1–20, Oct 2012.

[4] S. Panzieri and R. Setola. Failure Propagation in Critical Interdependent Infrastructures. *International Journal of Modeling, Identification and Control*, 3(1):69–78, May 2008.

[5] G. S. Vassell. Northeast Blackout of 1965. *IEEE Power Engineering Review*, 11(1):4–8, Jan 1991.

[6] R. Sugarman. Power/Energy: New York City's blackout. *IEEE Spectrum*, 15(11):44–46, Nov 1978.

[7] P. Pourbeik, P. S. Kundur, and C. W. Taylor. The Anatomy of a Power Grid Blackout - Root Causes and Dynamics of Recent Major Blackouts. *IEEE Power and Energy Magazine*, 4(5):22–29, Sept 2006.

[8] US-Canada Power System Outage Task Force. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, Apr 2004.

[9] J. J. Romero. Blackouts illuminate India's power problems. *IEEE Spectrum*, 49(10): 11–12, Oct 2012.

[10] Protection System Misoperations Task Force. State of Reliability 2016, May 2016.

[11] National Academies of Sciences, Engineering, and Medicine. *Analytic Research Foundations for the Next-Generation Electric Grid*. The National Academies Press, Washington, DC, 2016.

[12] S. Thorve, S. Swarup, A. Marathe, Y. Chungbaek, E. K. Nordberg, and M. V. Marathe. Simulating Residential Energy Demand in Urban and Rural Areas. In *Winter Simulation Conference 2018*, Dec 2018.

[13] R. Subbiah, A. Pal, E. K. Nordberg, A. Marathe, and M. V. Marathe. Energy Demand Model for Residential Sector: A First Principles Approach. *IEEE Transactions on Sustainable Energy*, 8(3):1215–1224, July 2017.

[14] J. Chen, J. S. Thorp, and I. Dobson. Cascading Dynamics and Mitigation Assessment in Power System Disturbances via a Hidden Failure Model. *International Journal of Electrical Power & Energy Systems*, 27(4):318 – 326, May 2005.

[15] B. A. Carreras, D. E. Newman, I. Dobson, and A. B. Poole. Initial Evidence for Self-organized Criticality in Electric Power System Blackouts. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Jan 2000.

[16] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman. An Initial Model for Complex Dynamics in Electric Power System Blackouts. In *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, pages 710–718, Jan 2001.

[17] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman. Dynamics, Criticality and Self-organization in a Model for Blackouts in Power Transmission Systems. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, Jan 2002.

[18] I. Dobson, J. Chen, J. S. Thorp, B. A. Carreras, and D. E. Newman. Examining Criticality of Blackouts in Power System Models with Cascading Events. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, Jan 2002.

[19] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman. Critical Points and Transitions in an Electric Power Transmission Model for Cascading Failure Blackouts. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 12(4):985–994, Sept 2002.

[20] M. A. Rios, D. S. Kirschen, D. Jayaweera, D. P. Nedic, and R. N. Allan. Value of Security: Modeling Time-Dependent Phenomena and Weather Conditions. *IEEE Transactions on Power Systems*, 17(3):543–548, Aug 2002.

[21] Y. Xu, Z. Y. Dong, K. Meng, J. H. Zhao, and K. P. Wong. A Hybrid Method for Transient Stability-Constrained Optimal Power Flow Computation. *IEEE Transactions on Power Systems*, 27(4):1769–1777, Nov 2012.

[22] R. Zarate-Minano, T. Van Cutsem, F. Milano, and A. J. Conejo. Securing Transient Stability Using Time-Domain Simulations Within an Optimal Power Flow. *IEEE Transactions on Power Systems*, 25(1):243–253, Feb 2010.

[23] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(1):1025–1028, Apr 2010.

[24] Roni Parshani, Sergey V. Buldyrev, and Shlomo Havlin. Interdependent networks:

Reducing the coupling strength leads to a change from a first to second order percolation transition. *Physical Review Letters*, 105(4):048701 1–4, Jul 2010.

[25] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley. Robustness of interdependent networks under targeted attack. *Physical Review E*, 83(6):065101 1–4, Jun 2011.

[26] C. D. Brummitt, R. M. D'Souza, and E. A. Leicht. Suppressing Cascades of Load in Interdependent Networks. *Proceedings of the National Academy of Sciences*, 109(12): E680–E689, Mar 2012.

[27] D. N. Kosterev, C. W. Taylor, and W. A. Mittelstadt. Model validation for the August 10, 1996 WSCC system outage. *IEEE Transactions on Power Systems*, 14(3):967–979, Aug 1999.

[28] S. Tamronglak, S. H. Horowitz, A. G. Phadke, and J. S. Thorp. Anatomy of Power System Blackouts: Preventive Relaying Strategies. *IEEE Transactions on Power Delivery*, 11(2):708–715, Apr 1996.

[29] J. S. Thorp, A. G. Phadke, S. H. Horowitz, and S. Tamronglak. Anatomy of power system disturbances: Importance Sampling. *International Journal of Electrical Power & Energy Systems*, 20(2):147 – 152, Feb 1998.

[30] J. Xu and X. F. Wang. Cascading failures in scale-free coupled map lattices. In *2005 IEEE International Symposium on Circuits and Systems*, volume 4, pages 3395–3398, May 2005.

[31] J. Wu, Z. Gao, and H. Sun. Cascade and breakdown in scale-free networks with community structure. *Phys. Rev. E*, 74:066111, Dec 2006.

[32] Hui Ren, Xiaozhou Fan, D. Watts, and Xingchen Lv. Early warning mechanism for power system large cascading failures. In *2012 IEEE International Conference on Power System Technology (POWERCON)*, pages 1–6, Oct 2012.

[33] L. Ding and Z. Bao. Analysis on the Self-Organized Critical State with Power Flow Entropy in Power Grids. In *2009 Second International Conference on Intelligent Computation Technology and Automation*, volume 3, pages 18–21, Oct 2009.

[34] W. Xu, Z. Jianhua, W. Linwei, and Z. Xingyang. Power system key lines identification based on cascading failure and vulnerability evaluation. In *2012 China International Conference on Electricity Distribution*, pages 1–4, Sept 2012.

[35] Y. Jia and Z. Xu. Risk assessment based on information entropy of cascading failure in power systems. In *2012 IEEE Power and Energy Society General Meeting*, pages 1–5, July 2012.

[36] Protection System Misoperations Task Force. Misoperations Report, Apr 2013.

[37] Protection System Misoperations Task Force. NERC Staff Analysis of System Protection Misoperations, Dec 2014.

[38] Protection System Misoperations Task Force. Analysis of System Protection Misoperations, Dec 2015.

[39] D. C. Elizondo and J. De La Ree. Analysis of hidden failures of protection schemes in large interconnected power systems. In *IEEE Power Engineering Society General Meeting, 2004.*, volume 1, pages 107–114, June 2004.

[40] K. Bae and J. S. Thorp. A Stochastic Study of Hidden Failures in Power System Protection. *Journal of Decision Support Systems*, 24(3):259–268, Jan 1999.

[41] M. Chertkov, F. Pan, and M. G. Stepanov. Predicting Failures in Power Grids: The Case of Static Overloads. *IEEE Transactions on Smart Grid*, 2(1):162–172, Dec 2011.

[42] Y. Zhang and O. Yağan. Optimizing the robustness of electrical power systems against cascading failures. *Scientific Reports*, 6:27635 1–15, Jun 2016.

[43] S. Pahwa, C. Scoglio, and A. Scala. Abruptness of Cascade Failures in Power Grids. *Scientific Reports*, 4(1):3694 1–9, Jan 2014.

[44] S. Soltan, D. Mazauric, and G. Zussman. Cascading Failures in Power Grids: Analysis and Algorithms. In *Proceedings of the 5th International Conference on Future Energy Systems*, e-Energy '14, pages 195–206, New York, NY, USA, Jun 2014. ACM.

[45] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman. Sensitivity Analysis of the Power Grid Vulnerability to Large-scale Cascading Failures. *SIGMETRICS Performance Evaluation Review*, 40(3):33–37, Jan 2012.

[46] W. Wang, S. Yang, F. Hu, H. E. Stanley, S. He, and M. Shi. An Approach for Cascading Effects within Critical Infrastructure Systems. *Physica A: Statistical Mechanics and its Applications*, 510(1):164 – 177, Nov 2018.

[47] P. Hines, E. Cotilla-Sanchez, and S. Blumsack. Do Topological Models provide good information about Electricity Infrastructure Vulnerability? *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 20(3):033122 1–5, Sept 2010.

[48] H. Cetinay, S. Soltan, F. A. Kuipers, G. Zussman, and P. Van Mieghem. Comparing the Effects of Failures in Power Grids Under the AC and DC Power Flow Models. *IEEE Transactions on Network Science and Engineering*, 5(4):301–312, Oct 2018.

[49] S. Soltan, M. Yannakakis, and G. Zussman. REACT to Cyber Attacks on Power Grids. *IEEE Transactions on Network Science and Engineering*, pages 1–15, May 2018.

[50] J. Yan, Y. Tang, H. He, and Y. Sun. Cascading Failure Analysis With DC Power Flow Model and Transient Stability Analysis. *IEEE Transactions on Power Systems*, 30(1): 285–297, Jan 2015.

[51] G. L. Nemhauser, L. A. Wolsey, and M. L. Fisher. An Analysis of Approximations for Maximizing Submodular Set Functions. *Mathematical Programming*, 14(1):265–294, Dec 1978.

[52] J. Song, E. Cotilla-Sanchez, G. Ghanavati, and P. Hines. Dynamic Modeling of Cascading Failure in Power Systems. *IEEE Transactions on Power Systems*, 31(3):2085–2095, May 2016.

[53] PJM. PJM Manual 03: Transmission Operations, April 2011.

[54] PJM. PJM Transmission Providers Facilities List, Jan 2012.

[55] Dominion Virginia Power. Arlington Area Upgrade Fact Sheet, Jan 2012.

[56] PEPCO. Comprehensive Reliability Plan for District of Columbia, Sept 2010.

[57] J. A. Fonseca and A. Schlueter. Integrated Model for Characterization of Spatiotemporal Building Energy Consumption Patterns in Neighborhoods and City Districts. *Applied Energy*, 142:247–265, Mar 2015.

[58] F. McLoughlin, A. Duffy, and M. Conlon. Characterizing Domestic Electricity Consumption Patterns by Dwelling and Occupant Socio-economic Variables: An Irish Case Study. *Energy and Buildings*, 48:240–248, May 2012.

[59] A. Marszal-Pomianowska, P. Heiselberg, and O. K. Larsen. Household Electricity Demand Profiles – A High-Resolution Load Model to Facilitate Modeling of Energy Flexible Buildings. *Energy*, 103:487–501, May 2016.

[60] M. Zhang, Y. Song, P. Li, and H. Li. Study on Affecting Factors of Residential Energy Consumption in Urban and Rural Jiangsu. *Renewable and Sustainable Energy Reviews*, 53(Supplement C):330–337, Jan 2016.

[61] M. Bedir and E. C. Kara. Behavioral Patterns and Profiles of Electricity Consumption in Dutch Dwellings. *Energy and Buildings*, 150:339–352, Sept 2017.

[62] G. Bustos-Turu, K. H. van Dam, S. Acha, C. N. Markides, and N. Shah. Simulating Residential Electricity and Heat Demand in Urban Areas using an Agent-based Modeling Approach. In *2016 IEEE International Energy Conference (ENERGYCON)*, pages 1–6, Apr 2016.

[63] S. H. Horowitz and A. G. Phadke. *Power System Relaying*. Research Studies Press, 2nd Edition, Taunton, UK, 1995.

[64] IEEE Power System Relaying Committee. Application of overreaching distance relays, 2009.

[65] M. J. Thompson. Percentage restrained differential, percentage of what? In *2011 64th Annual Conference for Protective Relay Engineers*, pages 278–289, April 2011.

[66] 53 FR 9430. Final commission policy statement on maintenance at nuclear power plants, Mar 1988.

[67] P. W. Sauer and M. A. Pai. *Power System Dynamics and Stability*. Prentice Hall, 1998.

[68] P. S. Kundur. *Power System Stability and Control*. McGraw Hill Education, 1994.

[69] North American Reliability Corporation. NERC Reliability Standard TPL-001-1, Apr 2012.

[70] A. Pinar, J. Meza, V. Donde, and B. Lesieutre. Optimization Strategies for the Vulnerability Analysis of the Electric Power Grid. *SIAM Journal on Optimization*, 20(4): 1786–1810, 2010.

[71] Siemens Power Technologies Inc. PSS/E-34 Program Operation Manual, Mar 2015.

[72] Siemens Power Technologies Inc. PSS/E-34 Application Program Interface, Mar 2015.

[73] SIEMENS. Numerical machine protection 7um512 instruction manual, 1996.

Appendices

Appendix A

Pickup Values for Relay Operation

A.1 Settings for transmission line relays

A.1.1 Directional overcurrent relay setting

Let $\mathsf{I}_{\mathsf{e,A}}^{\mathsf{pick}}$ and $\mathsf{I}_{\mathsf{e,B}}^{\mathsf{pick}}$ be the pickup current for transmission line (edge) e at the two ends A and B respectively. The pickup current is evaluated for the operation of directional overcurrent relays which are designed to detect ground faults. Assuming that the positive ($\mathsf{Z}_{\mathsf{e}}^{(1)}$), negative ($\mathsf{Z}_{\mathsf{e}}^{(2)}$) and zero ($\mathsf{Z}_{\mathsf{e}}^{(0)}$) sequence impedances are equal for a transmission line, a line-ground fault at the remote end would result a measured fault current of

$$\mathsf{I}_{\mathsf{e,A}}^{\mathsf{pick}} = \frac{\mathsf{V}_{\mathsf{A}}}{3\left|\mathsf{Z}_{\mathsf{e}}^{(1)}\right|}; \quad \mathsf{I}_{\mathsf{e,B}}^{\mathsf{pick}} = \frac{\mathsf{V}_{\mathsf{B}}}{3\left|\mathsf{Z}_{\mathsf{e}}^{(1)}\right|} \tag{A.1}$$

where V_{A} and V_{B} are the voltages at ends A and B in normal operating condition. Let the phase angles of voltage and currents measured at end A be $\phi_{\mathsf{v,A}}$ and $\phi_{\mathsf{i,A}}$ respectively and $\phi_{\mathsf{v,B}}$ and $\phi_{\mathsf{i,B}}$ at end B. The phase angle difference between measured current and voltage at end A and B are respectively ϕ_{A} and ϕ_{B}. The operating region for a relay without any

hidden failure is given by

$$\begin{aligned}\mathsf{M}_{\mathsf{e,A}} &= \{(r,\theta)\big||r| \geq \mathsf{I}^{\mathsf{pick}}_{\mathsf{e,A}},\ |\phi_{\mathsf{A}}| \leq \frac{\pi}{2}\}\\ \mathsf{M}_{\mathsf{e,B}} &= \{(r,\theta)\big||r| \geq \mathsf{I}^{\mathsf{pick}}_{\mathsf{e,B}},\ |\phi_{\mathsf{B}}| \leq \frac{\pi}{2}\}\end{aligned} \tag{A.2}$$

For an overcurrent relay without any directional element, the operating region is given by

$$\begin{aligned}\mathsf{M}_{\mathsf{e,HFA}} &= \{(r,\theta)\big||r| \geq \mathsf{I}^{\mathsf{pick}}_{\mathsf{e,A}}\}\\ \mathsf{M}_{\mathsf{e,HFB}} &= \{(r,\theta)\big||r| \geq \mathsf{I}^{\mathsf{pick}}_{\mathsf{e,B}}\}\end{aligned} \tag{A.3}$$

A.1.2 Mho distance relay setting

In order to determine the Zone-1 operating characteristic for the edge e, we consider a reach of 80% of the positive sequence impedance of the line to be protected. Therefore, the diameter of Zone-1 mho circle is $0.8|\mathsf{Z}^{(1)}_{\mathsf{e}}|$ with center at $(0.4|\mathsf{Z}^{(1)}_{\mathsf{e}}|\cos\theta_e, 0.4|\mathsf{Z}^{(1)}_{\mathsf{e}}|\sin\theta_e)$, where $\tan\theta_e = \dfrac{\mathbf{Im}(\mathsf{Z}^{(1)}_{\mathsf{e}})}{\mathbf{Re}(\mathsf{Z}^{(1)}_{\mathsf{e}})}$ is the impedance angle of the line to be protected. Similar circles can be evaluated for Zone-2 and Zone-3. Let $\mathsf{M}_{\mathsf{e,A1}}$,$\mathsf{M}_{\mathsf{e,B1}}$ denote the Zone-1 operating regions for the mho distance relay at the two ends of the transmission line e. Similarly, the Zone-2 operating regions are denoted by $\mathsf{M}_{\mathsf{e,A2}}$,$\mathsf{M}_{\mathsf{e,B2}}$ and the Zone-3 by $\mathsf{M}_{\mathsf{e,A3}}$,$\mathsf{M}_{\mathsf{e,B3}}$. Therefore, we have

$$\mathsf{M}_{\mathsf{e,A1}} = \mathsf{M}_{\mathsf{e,B1}} = \big\{(r,x):\quad (r-0.40|\mathsf{Z}^{(1)}_{\mathsf{e}}|\cos\theta_e)^2 + (x-0.40|\mathsf{Z}^{(1)}_{\mathsf{e}}|\sin\theta_e)^2 \leq \big(0.40|\mathsf{Z}^{(1)}_{\mathsf{e}}|\big)^2\big\} \tag{A.4}$$

$$\mathsf{M}_{\mathsf{e,A2}} = \mathsf{M}_{\mathsf{e,B2}} = \big\{(r,x):\quad (r-0.75|\mathsf{Z}^{(1)}_{\mathsf{e}}|\cos\theta_e)^2 + (x-0.75|\mathsf{Z}^{(1)}_{\mathsf{e}}|\sin\theta_e)^2 \leq \big(0.75|\mathsf{Z}^{(1)}_{\mathsf{e}}|\big)^2\big\} \tag{A.5}$$

$$\mathsf{M}_{\mathsf{e,A3}} = \mathsf{M}_{\mathsf{e,B3}} = \big\{(r,x):\quad (r-1.25|\mathsf{Z}^{(1)}_{\mathsf{e}}|\cos\theta_e)^2 + (x-1.25|\mathsf{Z}^{(1)}_{\mathsf{e}}|\sin\theta_e)^2 \leq \big(1.25|\mathsf{Z}^{(1)}_{\mathsf{e}}|\big)^2\big\} \tag{A.6}$$

A.1.3 PLC based directional comparison blocking relay setting.

The PLC based directional comparison block relays are designed such that if a fault is detected in Zone-1 or Zone-2 of the relays at both ends of line e, a trip signal is sent. Let $\mathsf{M}_{\mathsf{e,Trip\ A}}$ and $\mathsf{M}_{\mathsf{e,Trip\ B}}$ be the tripping regions for the relays at ends A and B of line e.

$$\mathsf{M}_{\mathsf{e,Trip\ A}} = \mathsf{M}_{\mathsf{e,A1}} \bigcup \mathsf{M}_{\mathsf{e,A2}}; \quad \mathsf{M}_{\mathsf{e,Trip\ B}} = \mathsf{M}_{\mathsf{e,B1}} \bigcup \mathsf{M}_{\mathsf{e,B2}} \tag{A.7}$$

A.2 Settings for transformer relays

The percentage differential relays for the transformers are set with a sensitivity factor of 20% and a minimum pickup value of 0.2pu. Let $\mathsf{M}_{\mathsf{e,min}}$ denote the region which causes the transformer e to trip if the differential current is above the minimum pickup value.

$$\mathsf{M}_{\mathsf{e,min}} = \left\{ (\mathsf{I}_{\mathsf{e,A}}, \mathsf{I}_{\mathsf{e,B}}) \middle| \left(\mathsf{I}_{\mathsf{e,A}} - \mathsf{I}_{\mathsf{e,B}}\right) \geq 0.2\text{pu} \right\} \tag{A.8}$$

The total operating region of the percentage differential relay is given by

$$\mathsf{M}_{\mathsf{e,op}} = \left\{ (\mathsf{I}_{\mathsf{e,A}}, \mathsf{I}_{\mathsf{e,B}}) \middle| \left(\mathsf{I}_{\mathsf{e,A}} - \mathsf{I}_{\mathsf{e,B}}\right) \geq 0.2\left(\frac{\mathsf{I}_{\mathsf{As}} + \mathsf{I}_{\mathsf{Bs}}}{2}\right) + 0.2\text{pu} \right\} \tag{A.9}$$

A.3 Settings for generator relays

Let $\mathsf{V}_{\mathsf{G}} \subset \mathsf{V}$ be the set of generator buses. The voltage at bus $g \in \mathsf{V}_{\mathsf{G}}$ is given by U_{g}. Three different voltage limits are set for the generator at bus g. Let the timer count for each voltage limit be given by $\mathsf{T}_{\mathsf{g,1}}$, $\mathsf{T}_{\mathsf{g,2}}$ and $\mathsf{T}_{\mathsf{g,3}}$. Let Δt be the time step at which the voltage measurements are taken.

A.3.1 Moderate overvoltage limit

This is set for small overvoltages at the generator bus. If the bus voltage $\mathsf{U_g} \geq 1.1$ pu for more than 1.5 seconds, the overvoltage relay issues a trip signal. Since the relay operates for moderate overvoltages, the time delay of operation is also high.

$$\mathsf{T_{g,1}} = \begin{cases} 0, & \text{if } \mathsf{U_g} < 1.1 \\ \mathsf{T_{g,1}} + \Delta t, & \text{if } \mathsf{U_g} \geq 1.1 \end{cases}; \quad \mathsf{M_{g,Trip1}} = \begin{cases} 1, & \mathsf{T_{g,1}} \geq 1.5 \\ 0, & \mathsf{T_{g,1}} < 1.5 \end{cases} \tag{A.10}$$

A.3.2 Severe overvoltage limit

A separate limit is set for severely high voltages at the generator bus. If the bus voltage $\mathsf{U_g} \geq 1.3$ pu for more than 0.1 seconds, the overvoltage relay issues a trip signal. Since the relay operates for severe overvoltages, the time delay of operation is small.

$$\mathsf{T_{g,2}} = \begin{cases} 0, & \text{if } \mathsf{U_g} < 1.3 \\ \mathsf{T_{g,2}} + \Delta t, & \text{if } \mathsf{U_g} \geq 1.3 \end{cases}; \quad \mathsf{M_{g,Trip1}} = \begin{cases} 1, & \mathsf{T_{g,2}} \geq 0.1 \\ 0, & \mathsf{T_{g,2}} < 0.1 \end{cases} \tag{A.11}$$

A.3.3 Undervoltage Limit

The undervoltage limit is set at 0.7 pu with a clearance time of 1.5 seconds.

$$\mathsf{T_{g,3}} = \begin{cases} 0, & \text{if } \mathsf{U_g} > 0.7 \\ \mathsf{T_{g,3}} + \Delta t, & \text{if } \mathsf{U_g} \leq 0.7 \end{cases}; \quad \mathsf{M_{g,Trip3}} = \begin{cases} 1, & \mathsf{T_{g,3}} \geq 1.5 \\ 0, & \mathsf{T_{g,3}} < 1.5 \end{cases} \tag{A.12}$$

The tripping condition fo generator g is given by $\mathsf{M}_{\mathsf{g,Trip}}$

$$\mathsf{M}_{\mathsf{g,Trip}} = \mathsf{M}_{\mathsf{g,Trip1}} \vee \mathsf{M}_{\mathsf{g,Trip2}} \vee \mathsf{M}_{\mathsf{g,Trip3}} \tag{A.13}$$

The limits and the clearance times were chosen based on the specifications provided in a standard overvoltage and undervoltage relay manufacturers' manual [73]. In order to analyze the worst possible scenario in the aftermath of a human initiated attack, the most strict voltage limits are considered for the generators.

Appendix B

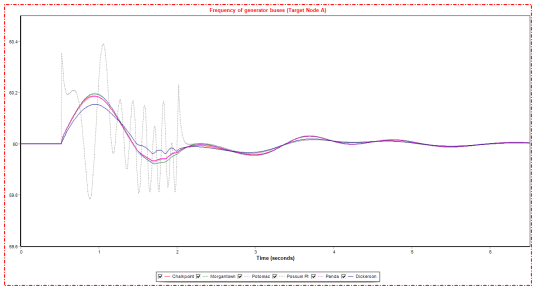
Generator bus frequencies

We now consider the impact of these targeted attacks on the generators in and around Washington DC. There are six principal generating stations in this region, viz. Chalkpoint, Morgantown, Potomac, Possum Point, Panda and Dickerson. We observe frequency monitored at the generator buses under the attack scenarios. Due to limitation of using the frequency values as control parameters during simulation, generator relays like over/under-speed relays and frequency relays could not be implemented. However, variation in the monitored frequencies at these generator buses would shed light on the stability of power grid in the event of such attacks. The variation of generator frequency for all target scenarios are presented in Appendix B.

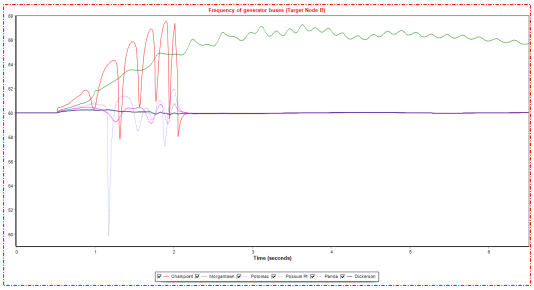
From Fig. 5.2 in Chapter 5, Target ID B and C are observed to result in maximum impact when target set size of $k = 1$ is chosen using high degree heuristic. This is further validated from the generator frequency curves in Fig. B.1. When node with Target ID B or C is attacked, the generator frequency exceeds the normal operating limits soon after the target nodes are attacked. This indicates that the over-speed and over-frequency relays would result in generator trips resulting in an unstable power swing or system collapse.

When target set size of $k = 2$ is considered, the maximum impact is resulted when Target IDs A and B are attacked simultaneously. It is interesting to note that though targets B and C result in more impact when attacked individually, a combined attack on B and C results in lesser impact than when each of them is combined with target ID A. This indicates that the

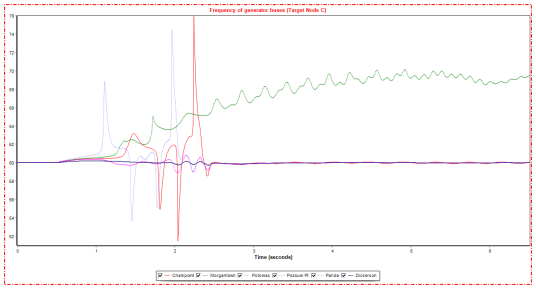
impact does not monotonically increase when target nodes are combined. From Fig. B.2 it is observed that a simultaneous attack on Target IDs A and B causes the isolation of Panda generating station (evident from the constant bus frequency different from 60Hz). However, when Target IDs B and C are attacked together, the large generating stations (Chalkpoint and Morgantown) are affected while the other generators operate at synchronous frequency of 60Hz. Though large generator nodes are removed in this case, an unstable power swing is not resulted as in the case when combined attack on Target IDs A and B is performed.



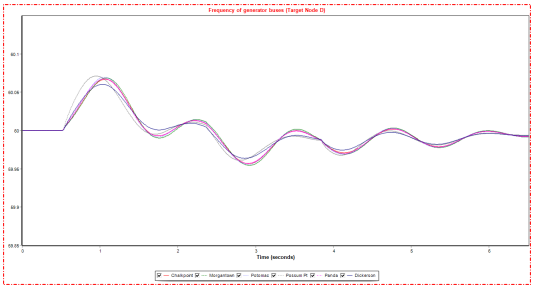
(a) Generator bus frequencies for attacking Target A.



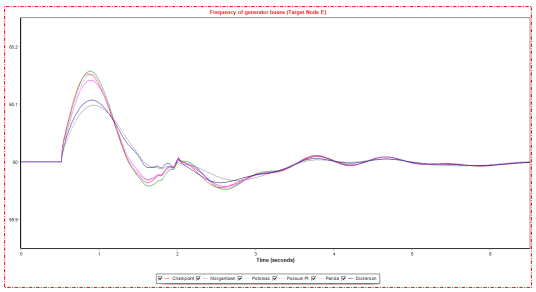
(b) Generator bus frequencies for attacking Target B.



(c) Generator bus frequencies for attacking Target C.

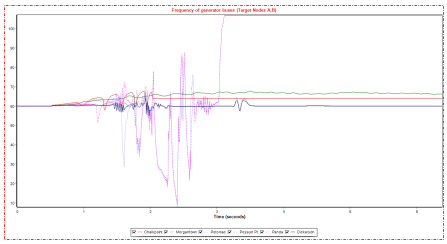


(d) Generator bus frequencies for attacking Target D.

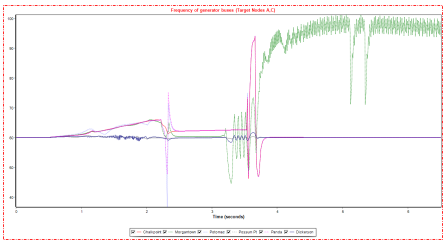


(e) Generator bus frequencies for attacking Target E.

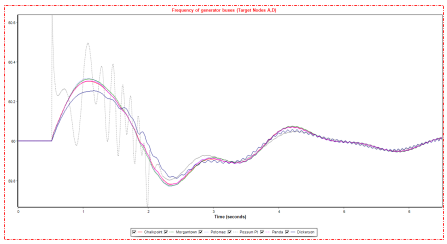
Figure B.1: Generator bus frequencies for target set size $k = 1$ selected by high degree heuristic.



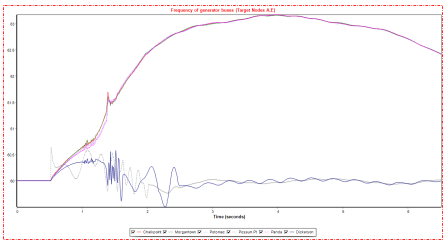
(a) Generator bus frequencies for attacking Targets A and B.



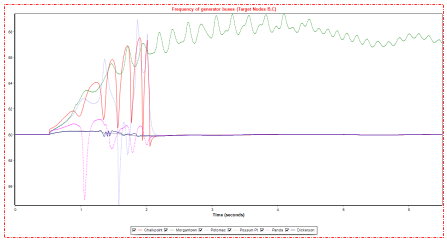
(b) Generator bus frequencies for attacking Targets A and C.



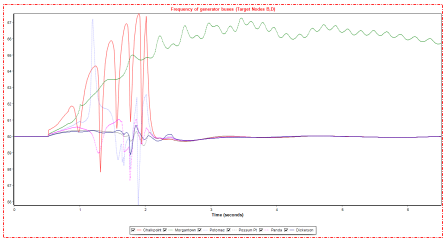
(c) Generator bus frequencies for attacking Targets A and D.



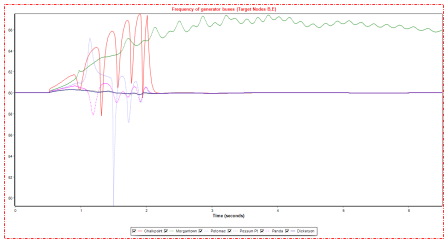
(d) Generator bus frequencies for attacking Targets A and E.



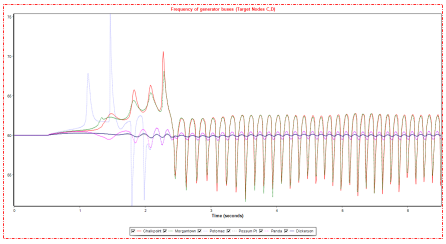
(e) Generator bus frequencies for attacking Targets B and C.



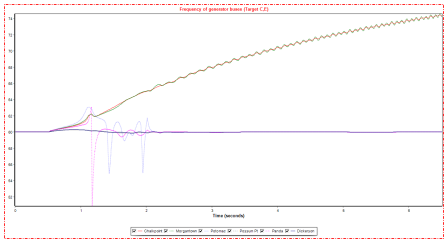
(f) Generator bus frequencies for attacking Targets B and D.



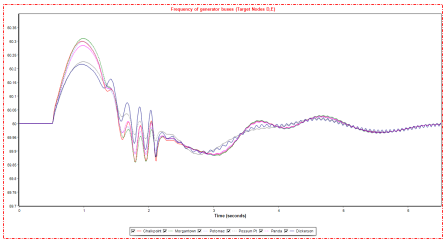
(g) Generator bus frequencies for attacking Targets B and E.



(h) Generator bus frequencies for attacking Targets C and D.

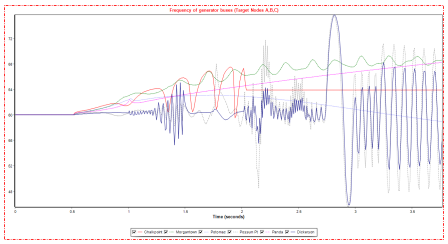


(i) Generator bus frequencies for attacking Targets C and E.

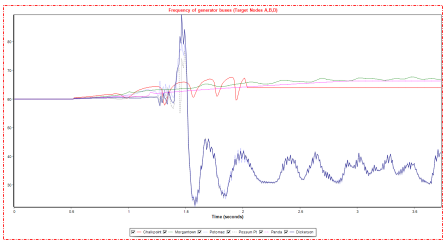


(j) Generator bus frequencies for attacking Targets D and E.

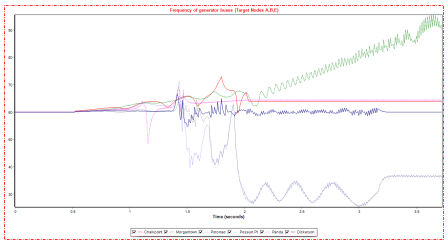
Figure B.2: Generator bus frequencies for target set size $k = 2$ selected by high degree heuristic.



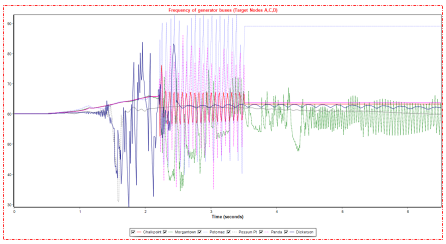
(a) Generator bus frequencies for attacking Targets A,B and C.



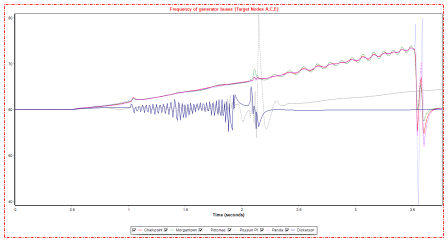
(b) Generator bus frequencies for attacking Targets A,B and D.



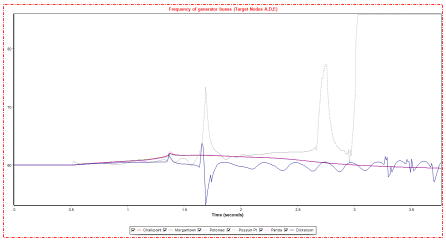
(c) Generator bus frequencies for attacking Targets A,B and E.



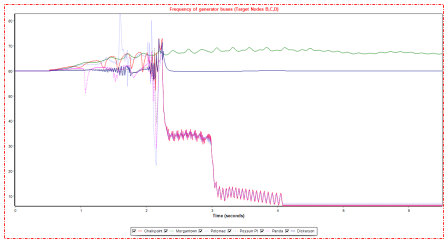
(d) Generator bus frequencies for attacking Targets A,C and D.



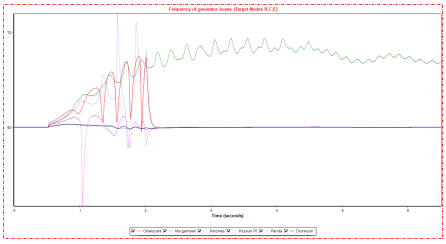
(e) Generator bus frequencies for attacking Targets A,C and E.



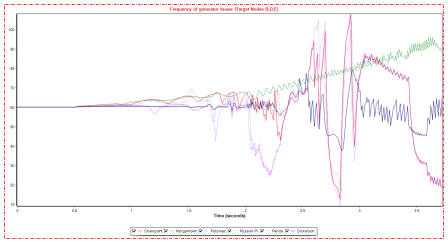
(f) Generator bus frequencies for attacking Targets A,D and E.



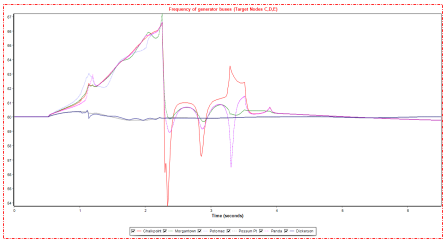
(g) Generator bus frequencies for attacking Targets B,C and D.



(h) Generator bus frequencies for attacking Targets B,C and E.



(i) Generator bus frequencies for attacking Targets B,D and E.



(j) Generator bus frequencies for attacking Targets C,D and E.

Figure B.3: Generator bus frequencies for target set size $k = 3$ selected by high degree heuristic.

Appendix C

Role of hidden failures on outcome of targeted attacks

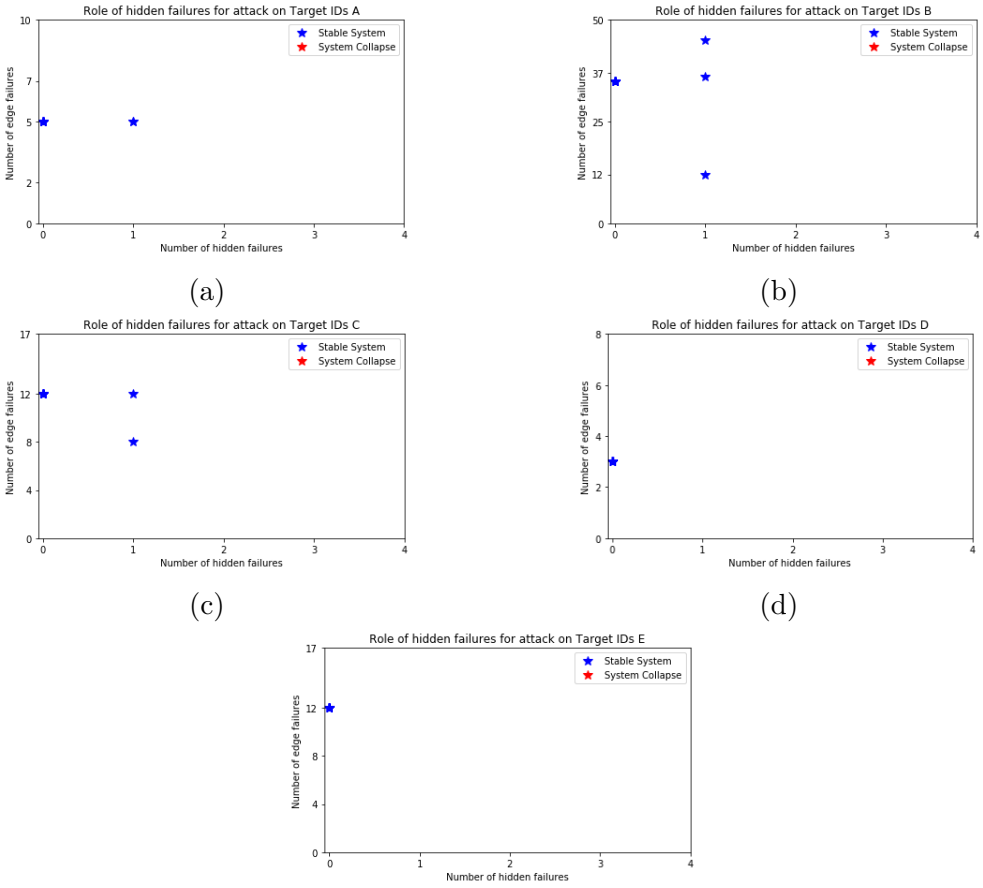


Figure C.1: Role of hidden failures on system stability for target sets of size $k = 1$ with highly connected nodes.

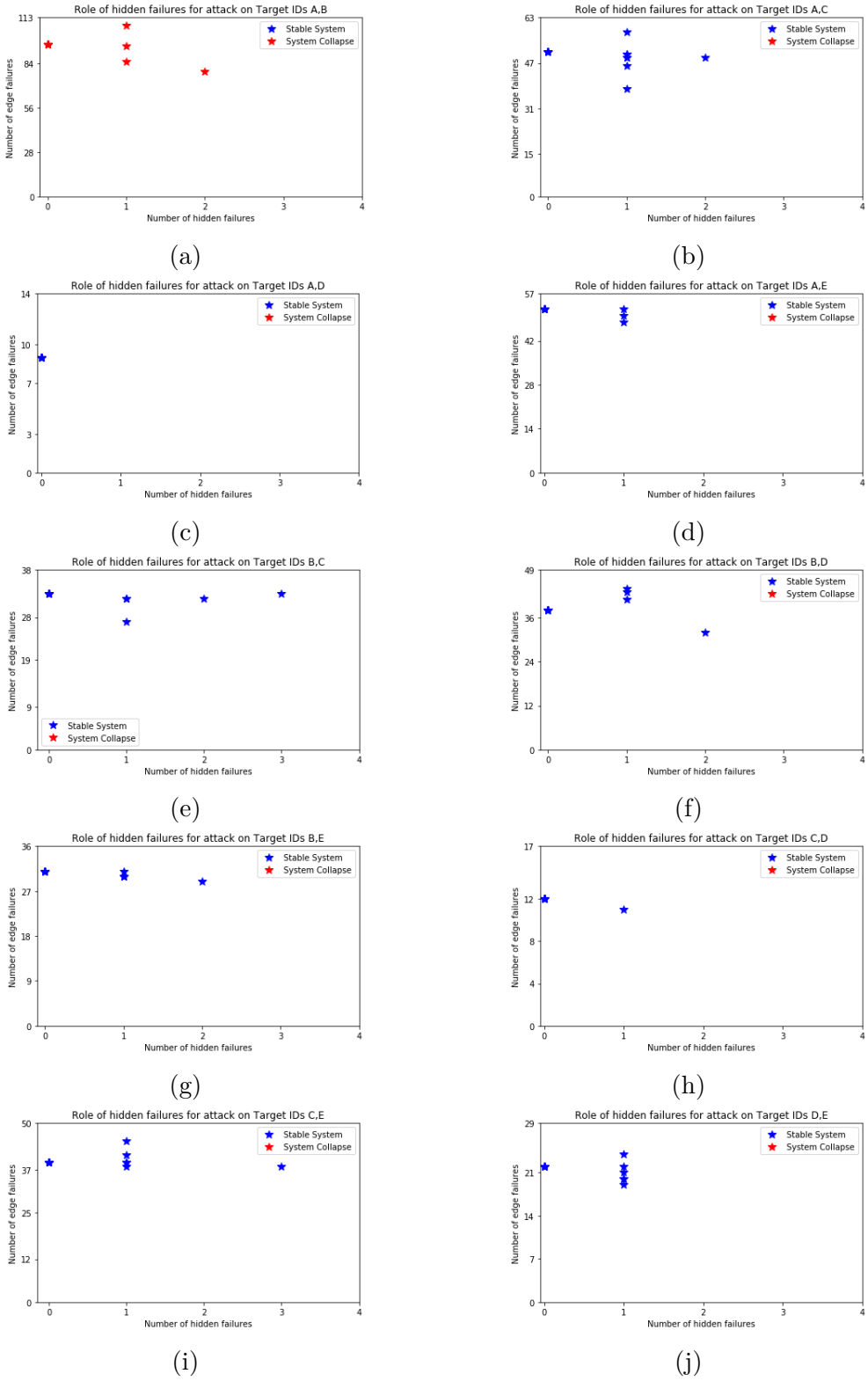


Figure C.2: Role of hidden failures on system stability for target sets of size $k = 2$ with highly connected nodes.

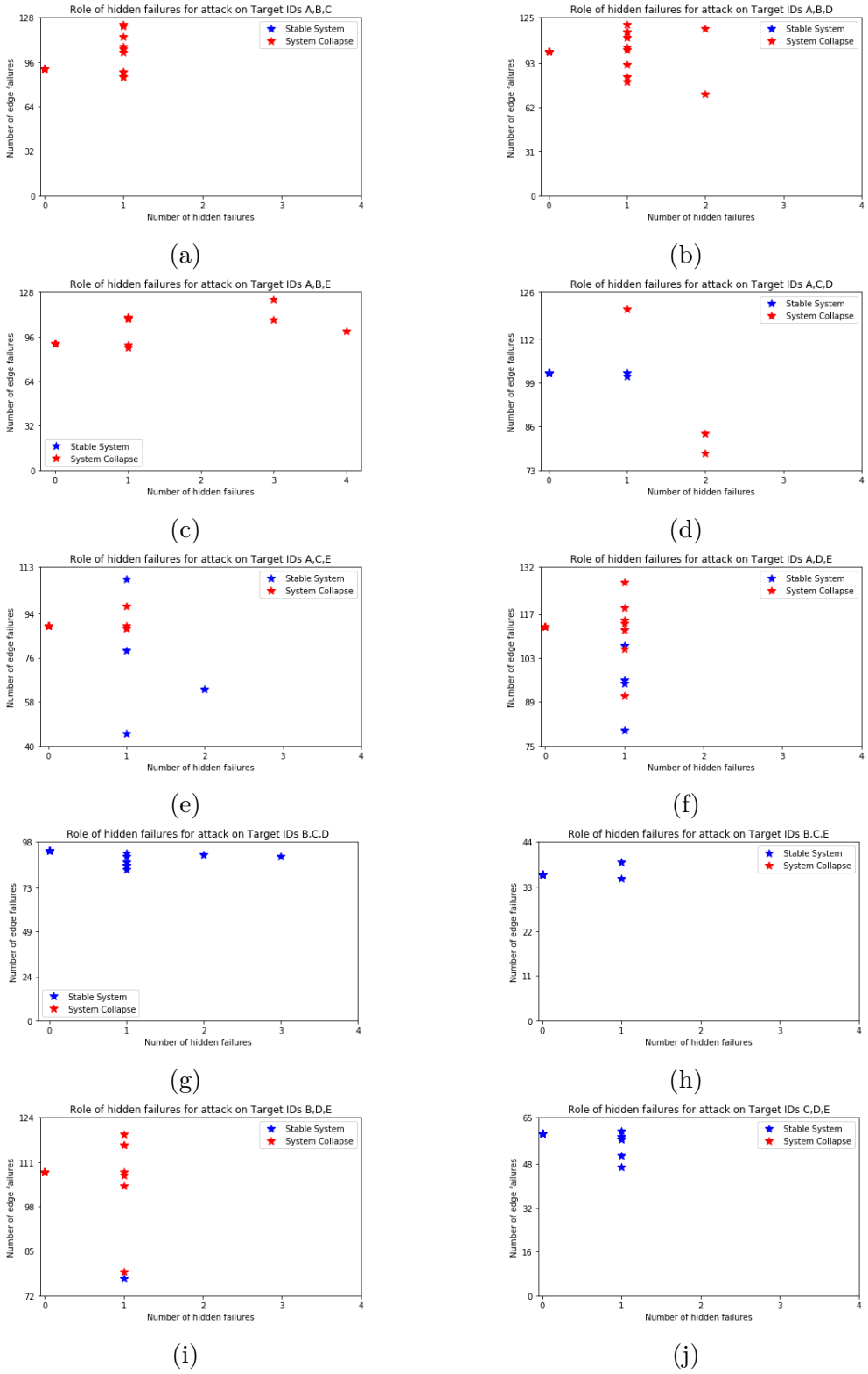


Figure C.3: Role of hidden failures on system stability for target sets of size $k = 3$ with highly connected nodes.

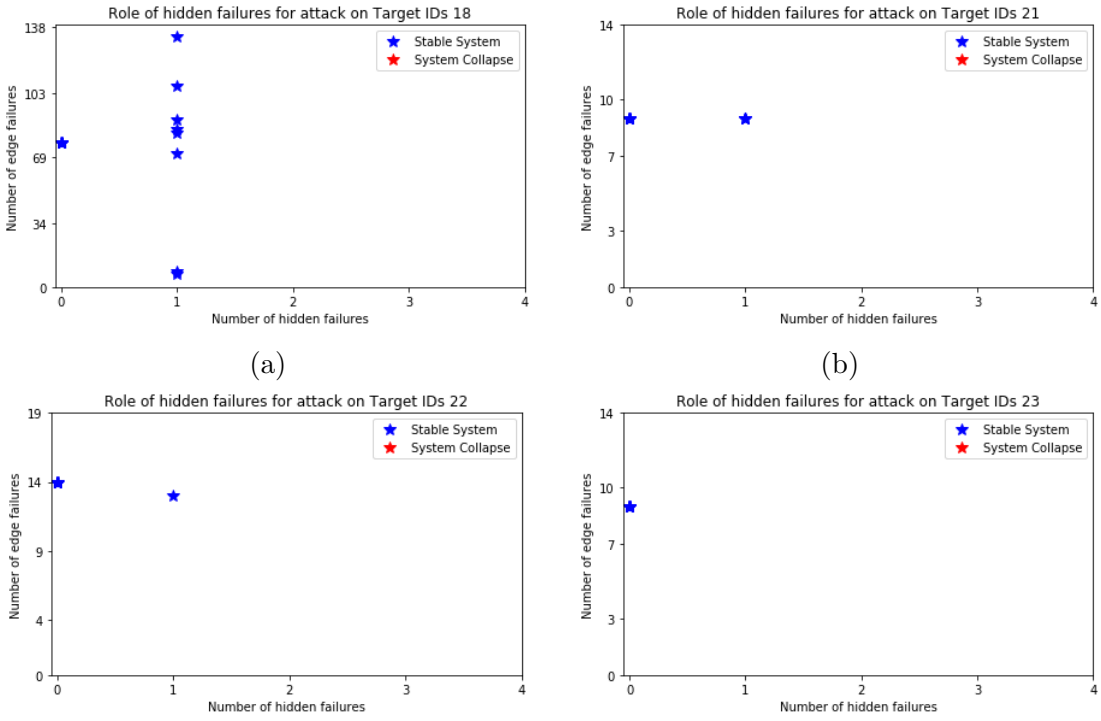


Figure C.4: Role of hidden failures on system stability for target sets of size $k = 1$ with highly connected 500kV nodes.

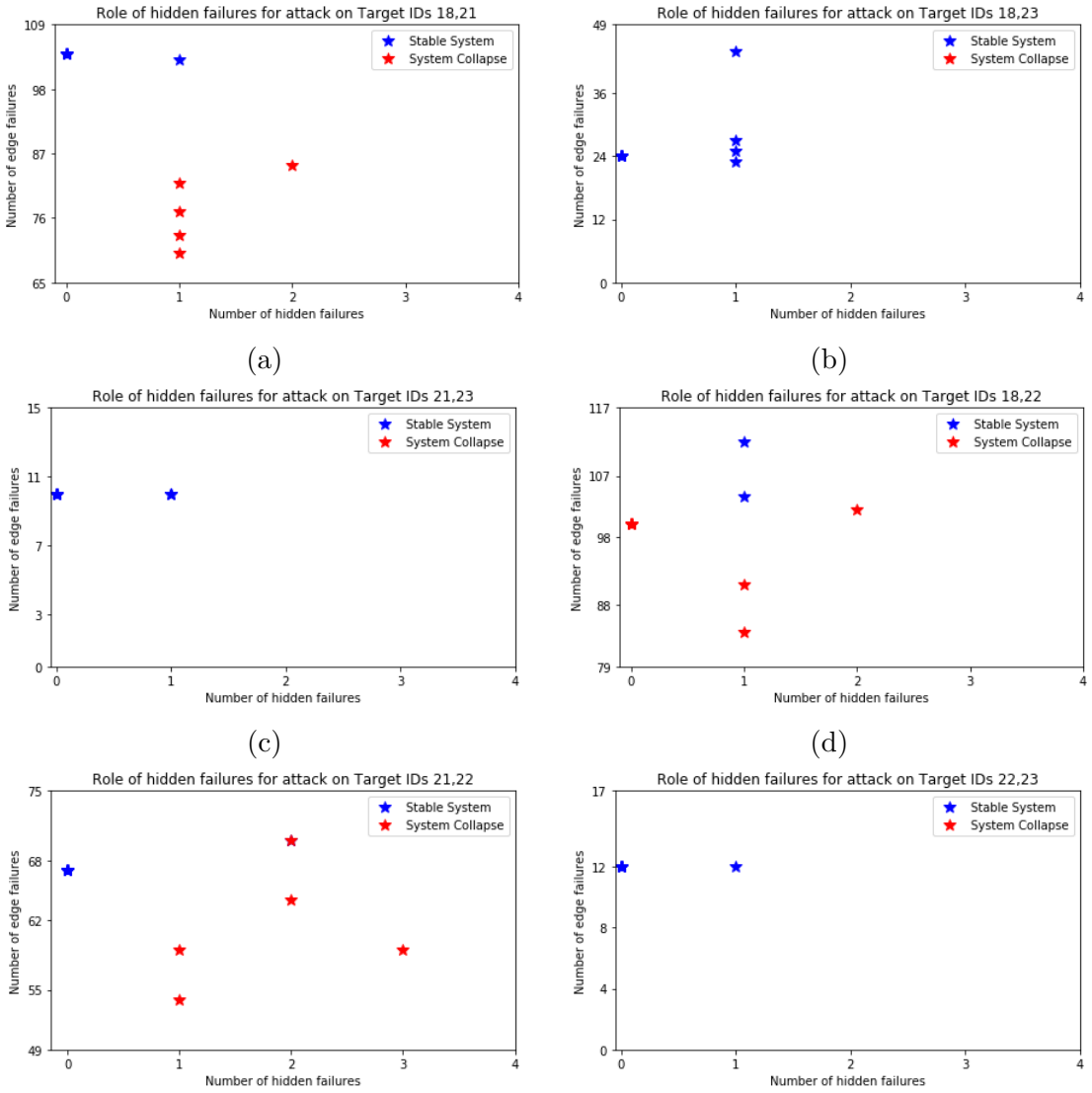


Figure C.5: Role of hidden failures on system stability for target sets of size $k = 2$ with highly connected 500kV nodes.

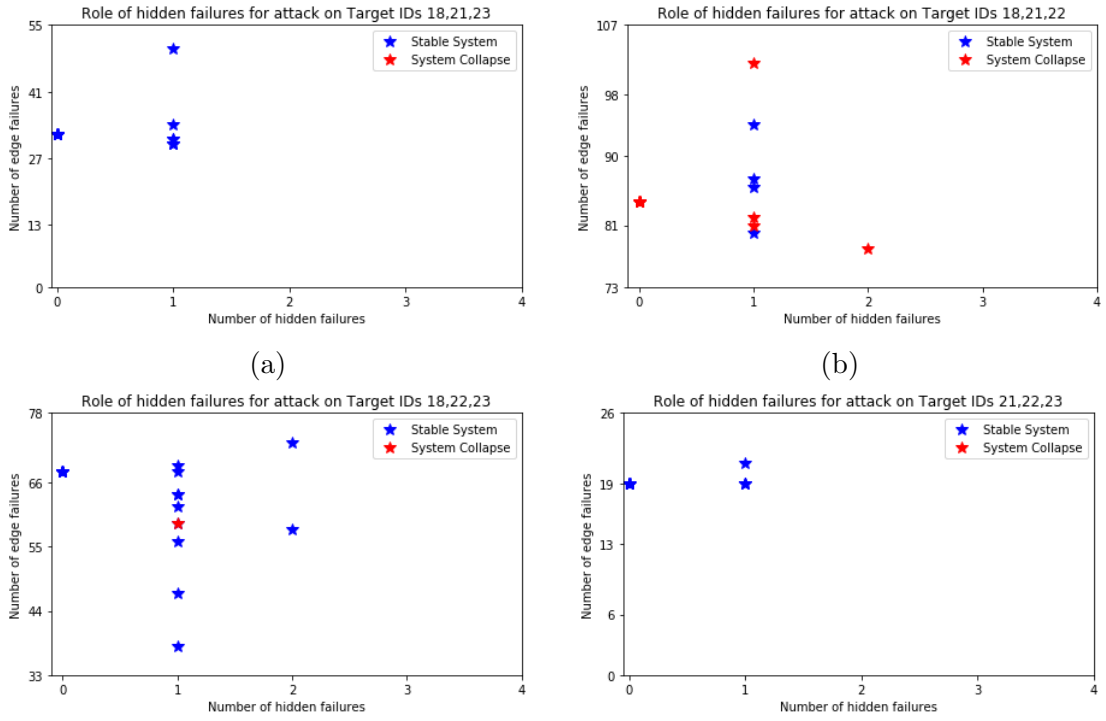


Figure C.6: Role of hidden failures on system stability for target sets of size $k = 3$ with highly connected 500kV nodes.

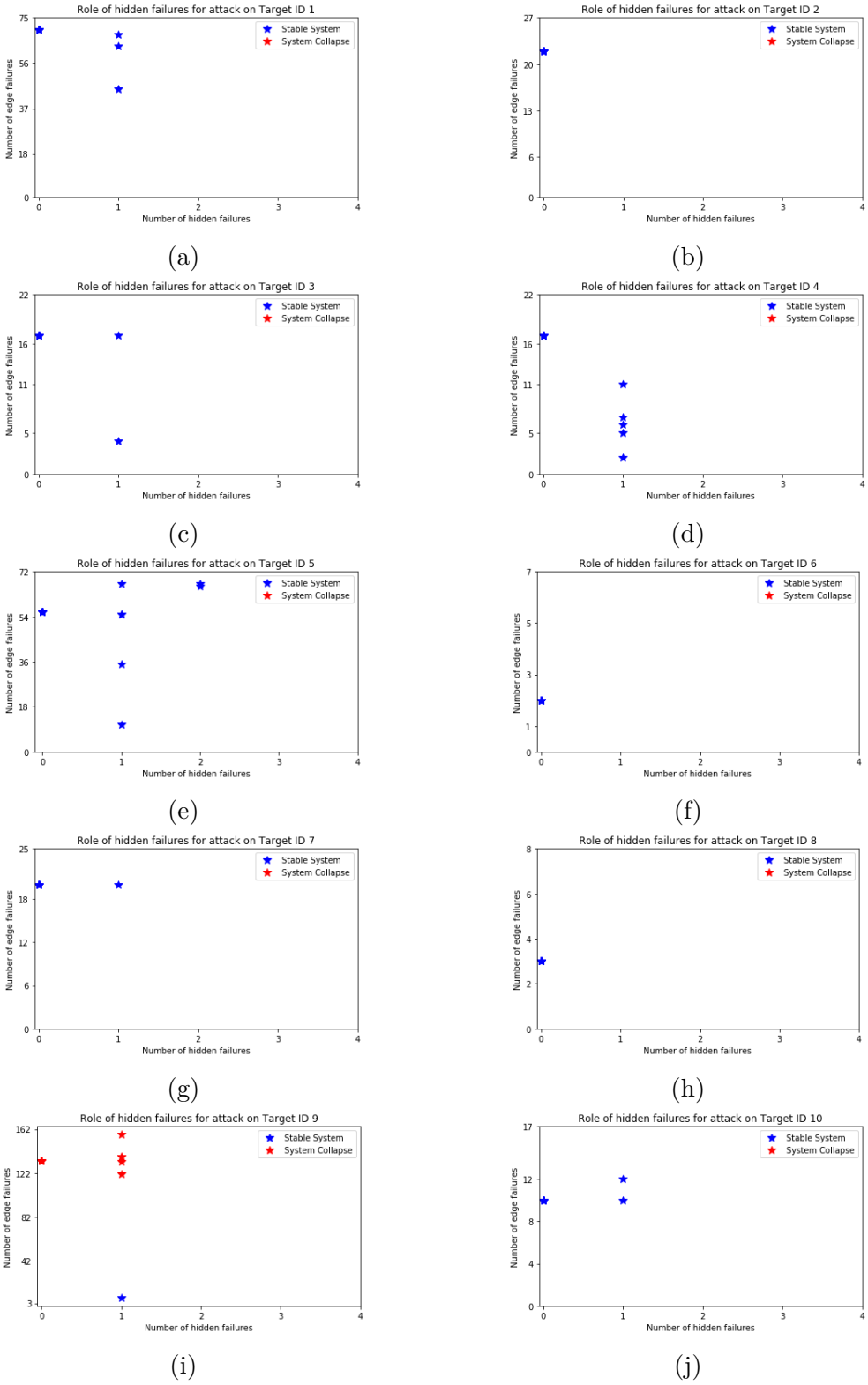


Figure C.7: Role of hidden failures on system stability for 500kV target sets of size $k = 1$.

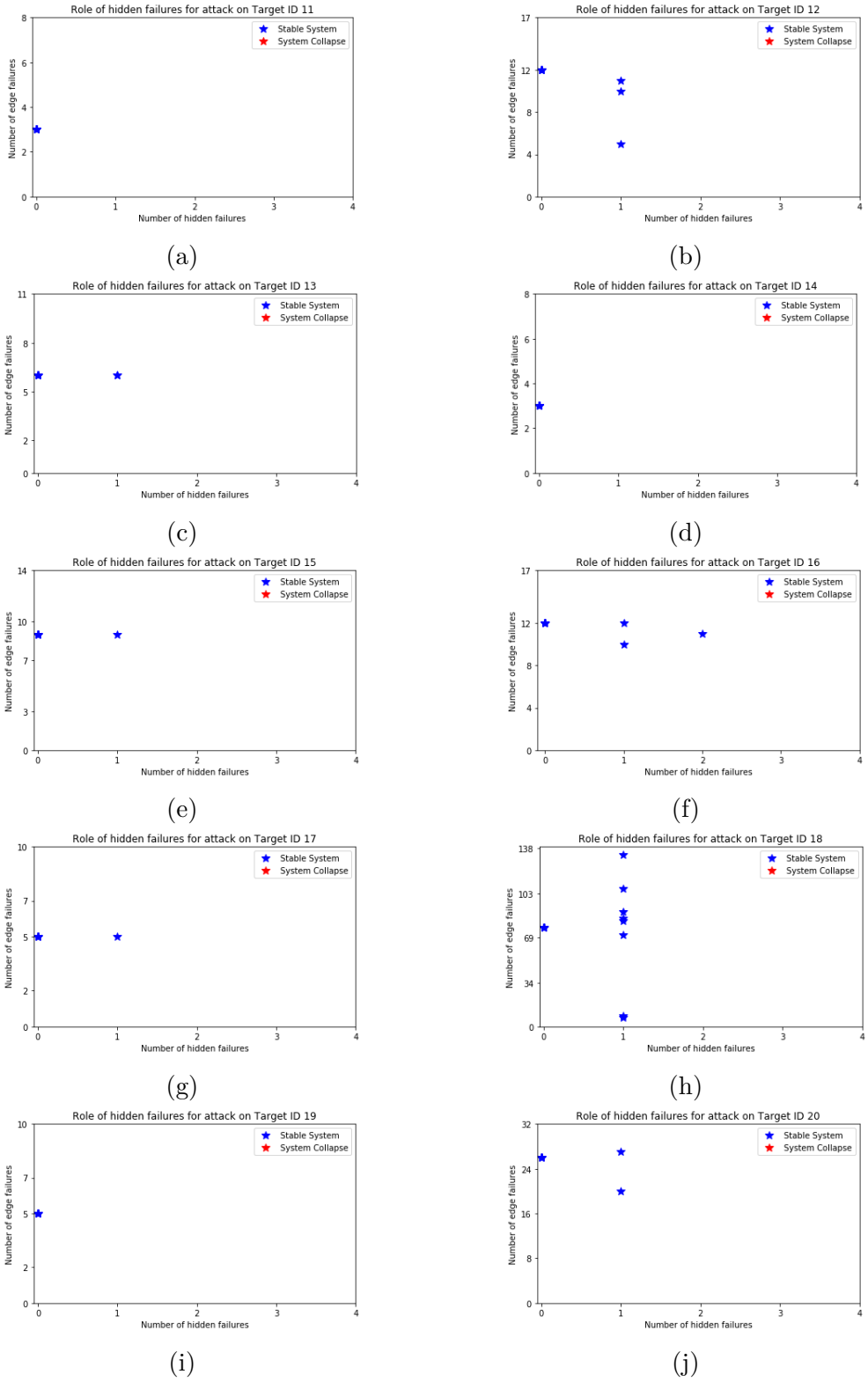


Figure C.8: Role of hidden failures on system stability for 500kV target sets of size $k = 1$.

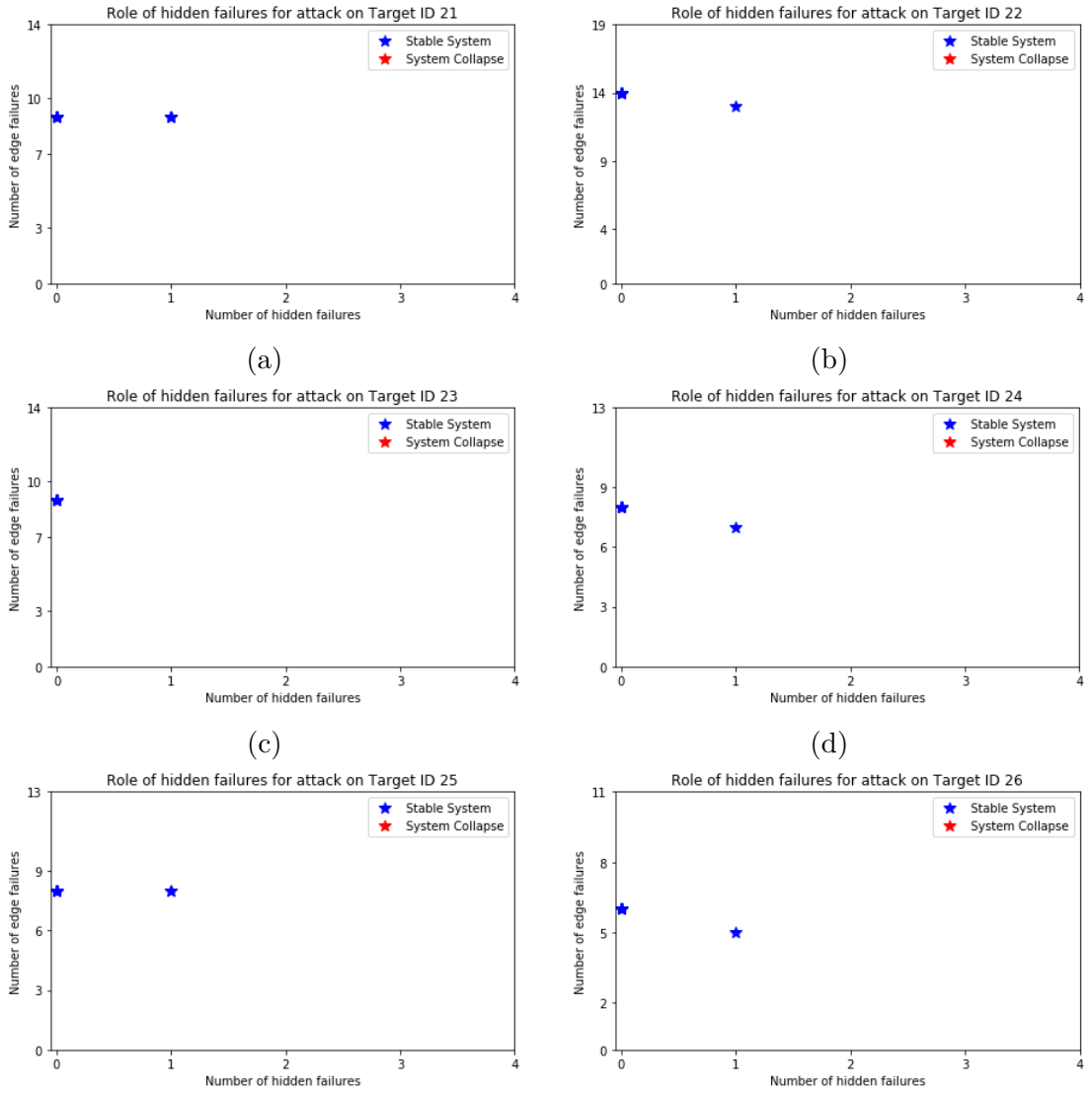


Figure C.9: Role of hidden failures on system stability for 500kV target sets of size $k = 1$.

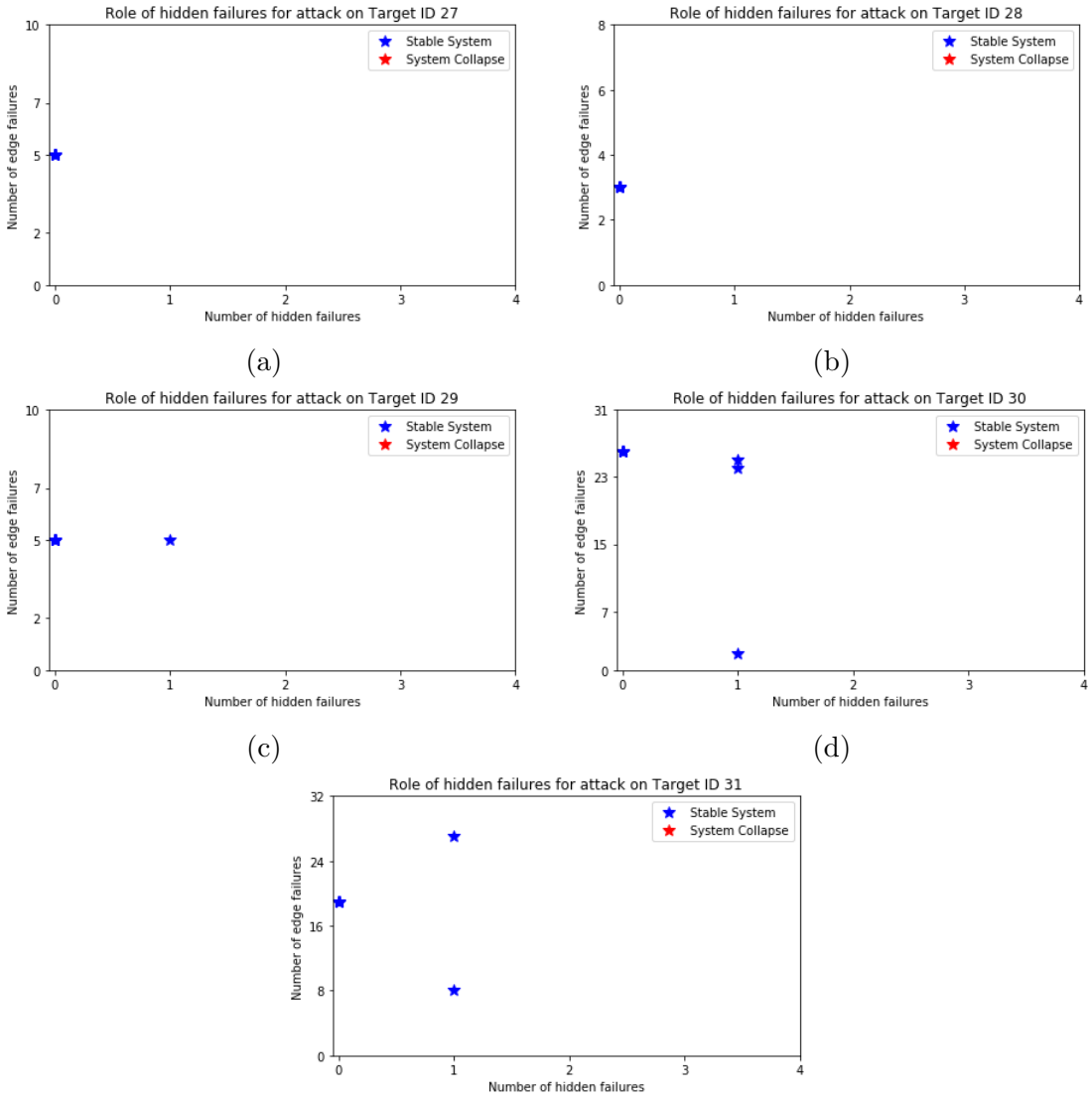


Figure C.10: Role of hidden failures on system stability for 500kV target sets of size $k = 1$.

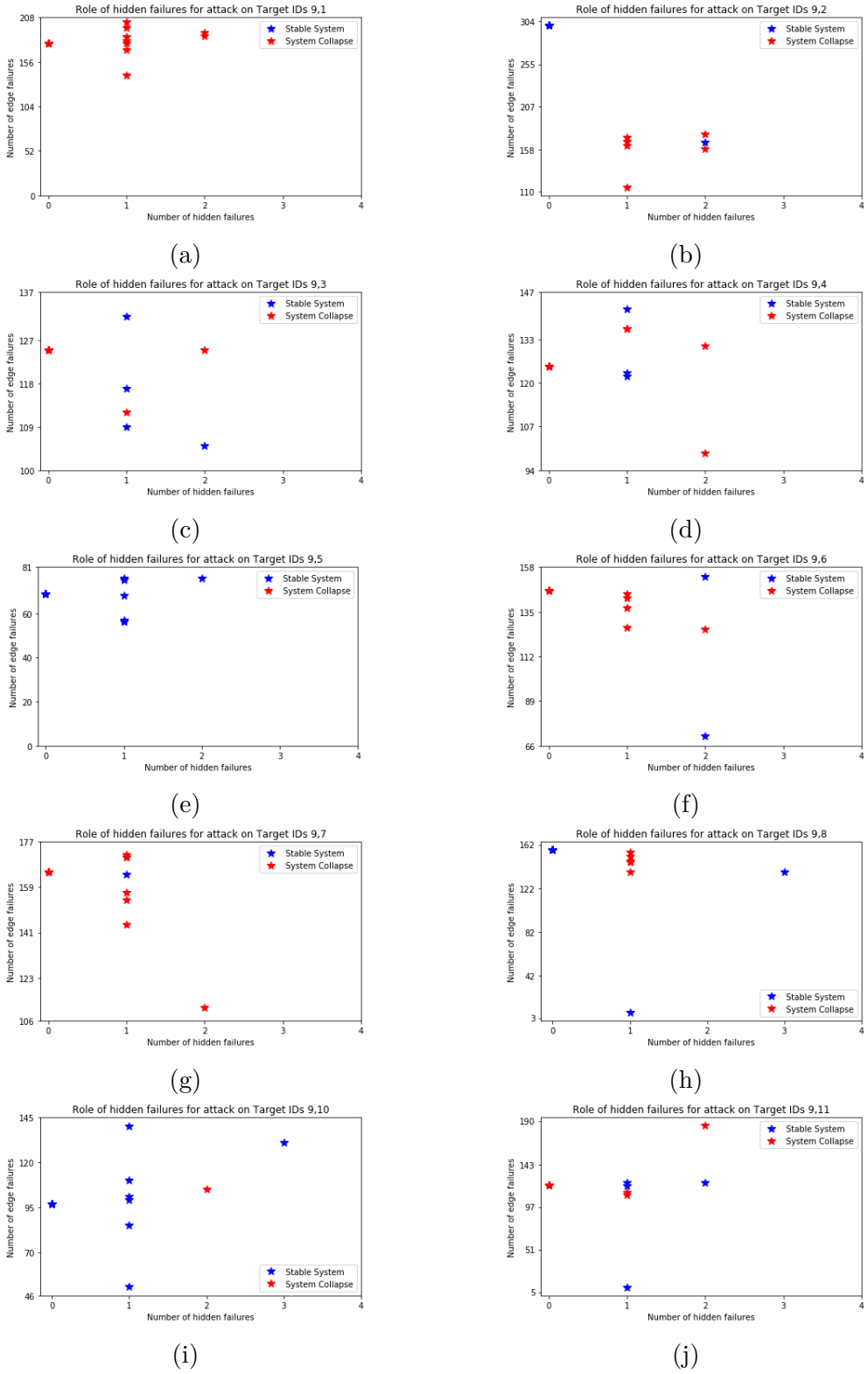


Figure C.11: Role of hidden failures on system stability for 500kV target sets of size $k = 2$.

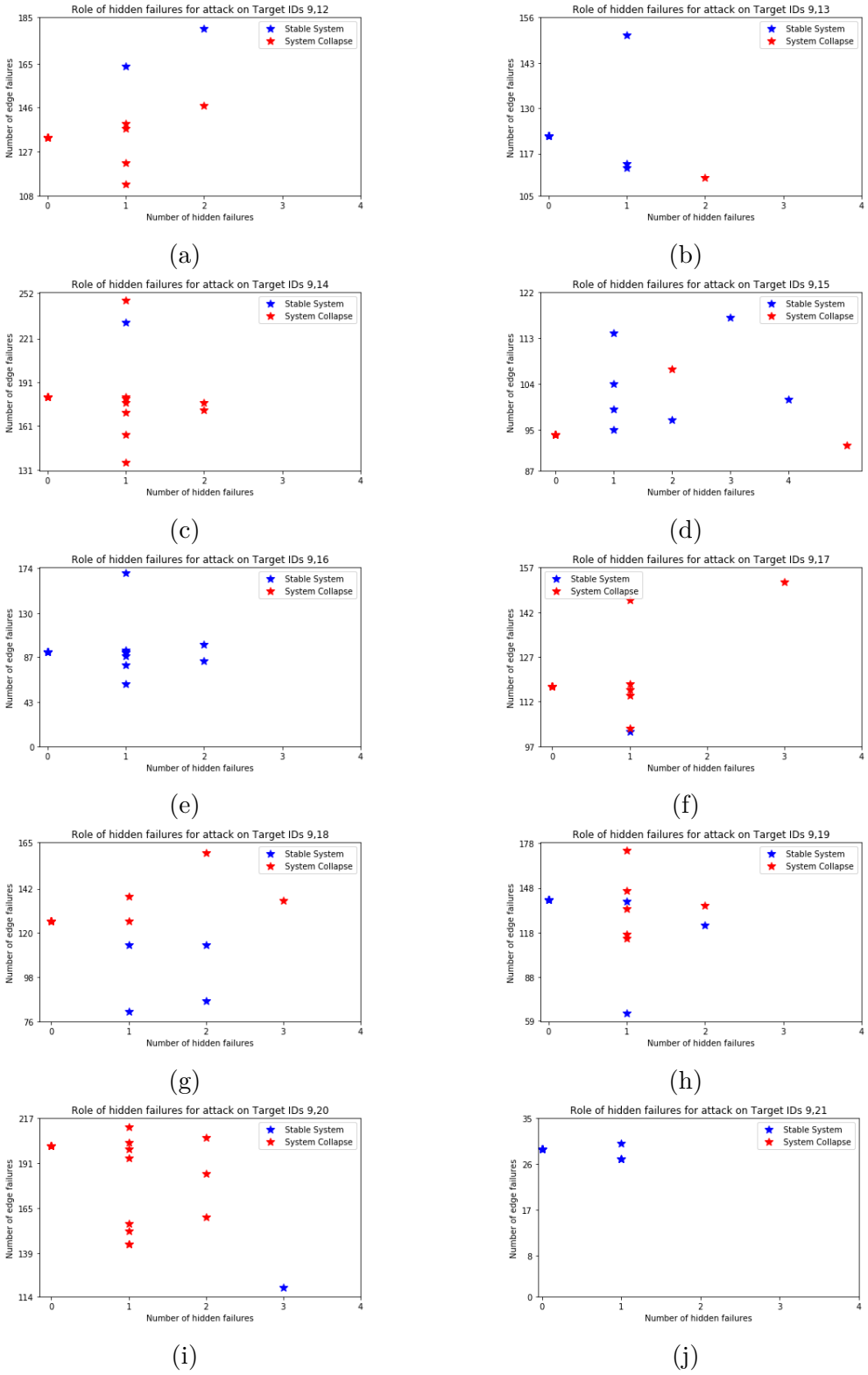


Figure C.12: Role of hidden failures on system stability for 500kV target sets of size $k = 2$.

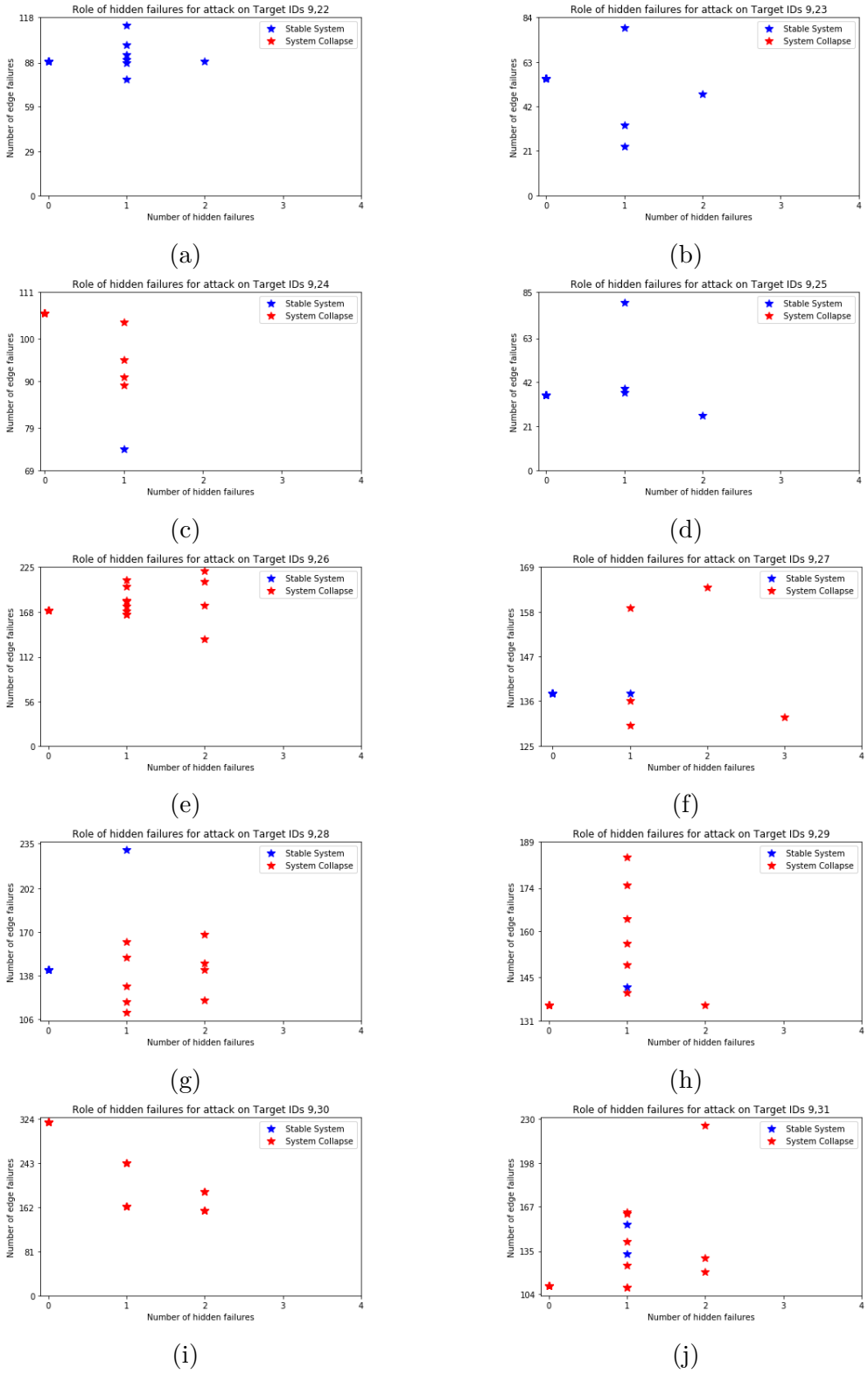


Figure C.13: Role of hidden failures on system stability for 500kV target sets of size $k = 2$.

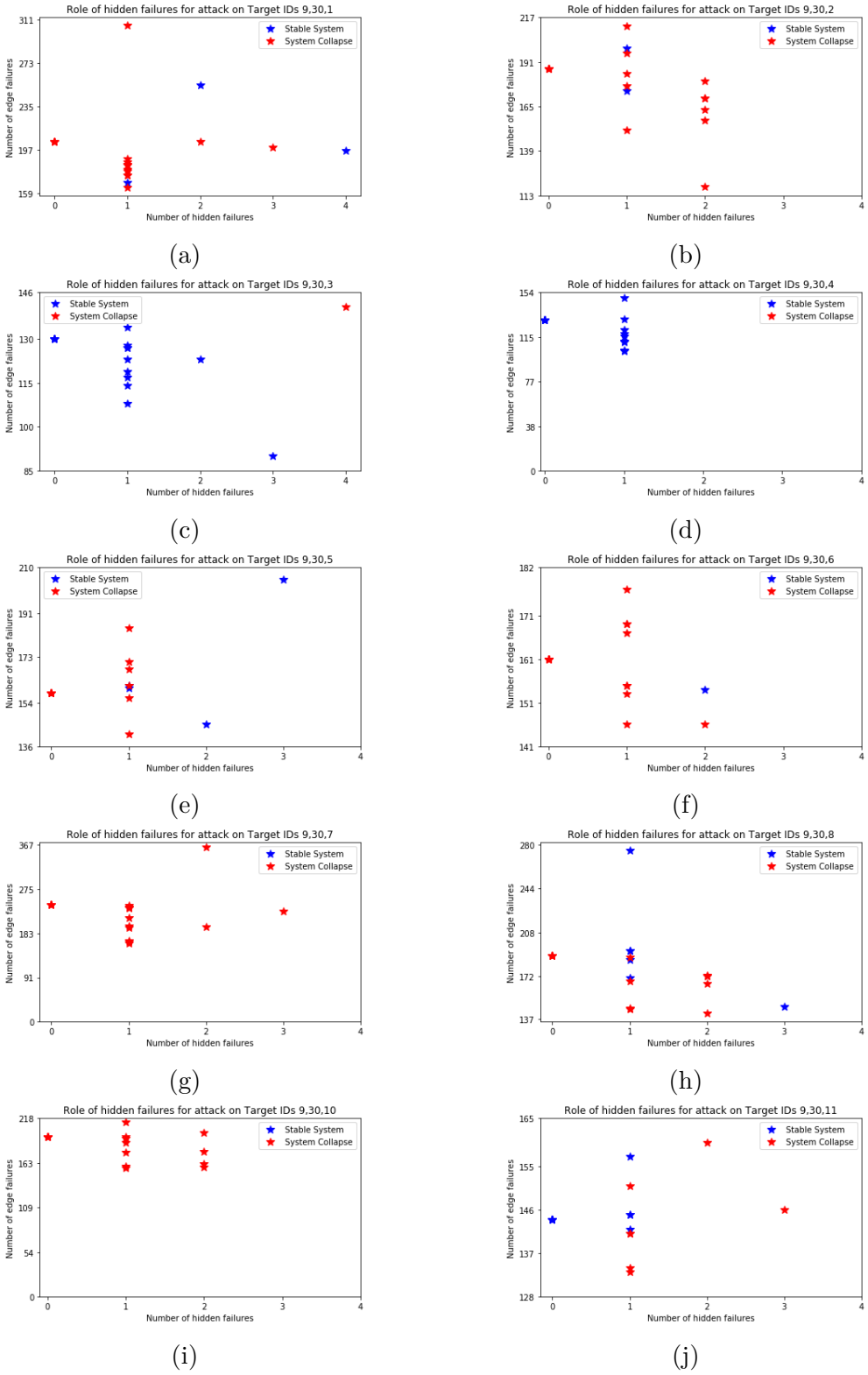


Figure C.14: Role of hidden failures on system stability for 500kV target sets of size $k = 3$.

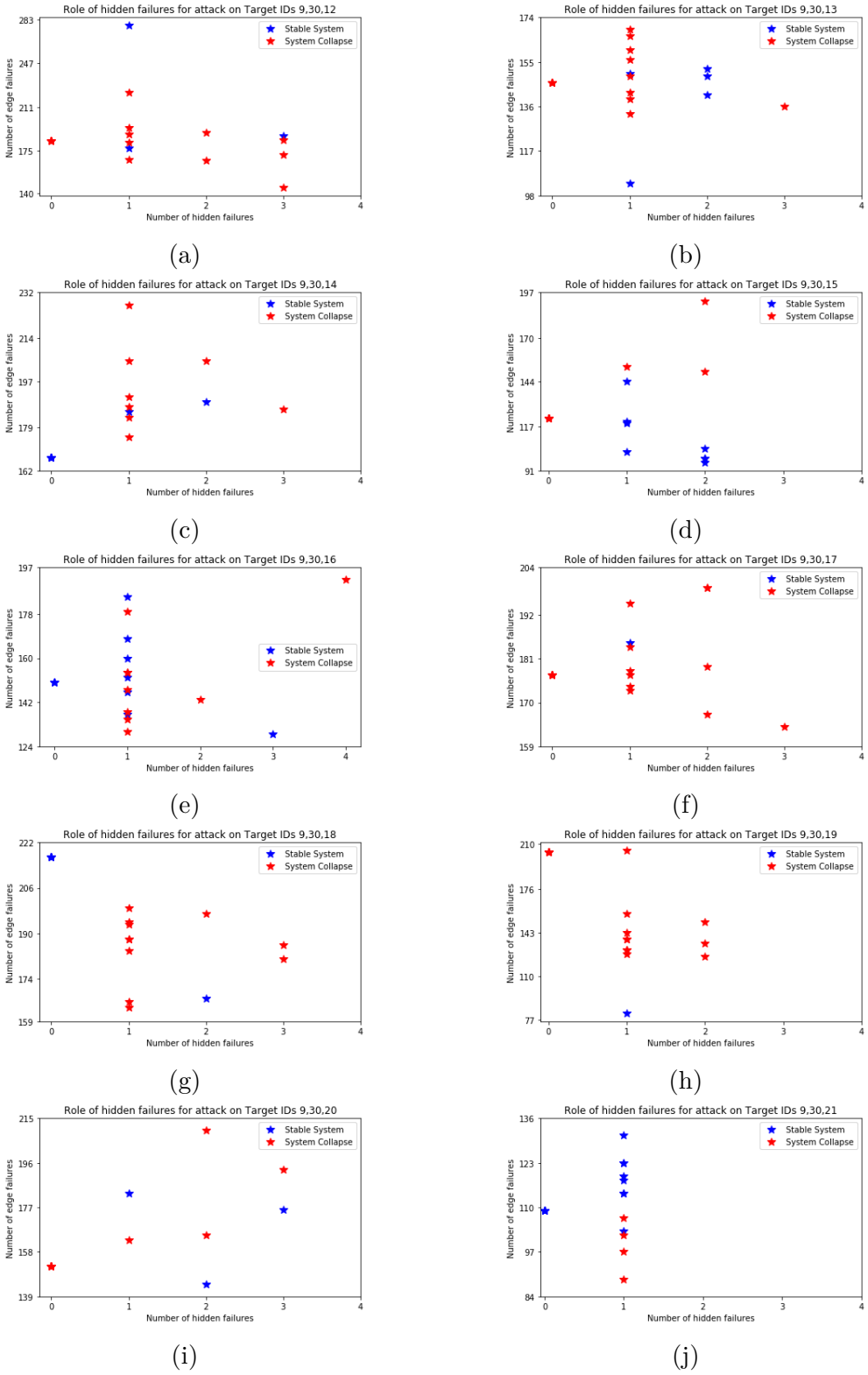


Figure C.15: Role of hidden failures on system stability for 500kV target sets of size $k = 3$.

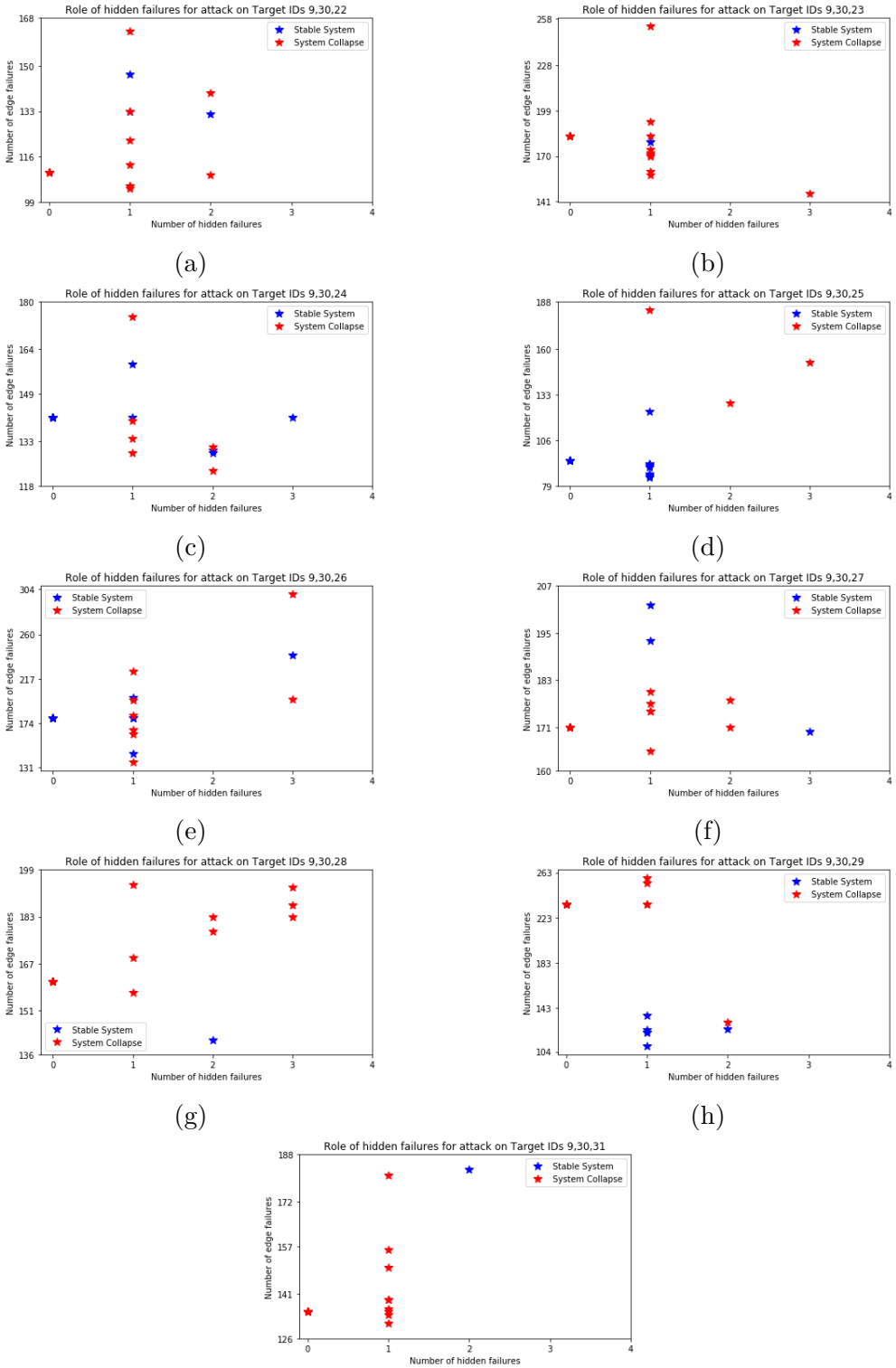


Figure C.16: Role of hidden failures on system stability for 500kV target sets of size $k = 3$.