Resilient Operations of Smart Electricity Networks under Security and Reliability Failures

by

Devendra Shelar

B. Tech., M. Tech., Computer Science & Engineering
Indian Institute of Technology, Bombay (2012)

M.S. in Transportation
Massachusetts Institute of Technology (2016)

Submitted to the Center for Computational Engineering
& Department of Civil and Environmental Engineering
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Computational Science and Engineering

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2019

Author . . . . . .
Devendra Shelar
Center for Computational Engineering
& Department of Civil and Environmental Engineering
May 17, 2019

Certified by . . . . . .
Saurabh Amin
Associate Professor of Civil and Environmental Engineering
Thesis Supervisor

Accepted by . . . . . .
Nicolas Hadjiconstantinou
Professor of Mechanical Engineering
Co-Director, Center for Computational Engineering

Accepted by . . . . . .
Heidi Nepf
Donald and Martha Harleman Professor of Civil and Environmental Engineering
Chair, Graduate Program Committee

Resilient Operations of Smart Electricity Networks

under Security and Reliability Failures

by

Devendra Shelar

Submitted to the Center for Computational Engineering
& Department of Civil and Environmental Engineering
on May 17, 2019, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Computational Science and Engineering

Abstract

Blackouts (or cascading failures) in Electricity Networks (ENs) can result in severe consequences for economic activity, human safety and national security. Recent incidents suggest that risk of blackouts due to cyber-security attacks and extreme weather events is steadily increasing in many regions of the world. This thesis develops a systematic approach to evaluate and improve the resilience of ENs by addressing following questions: *(a) How to model security and reliability failures and assess their impact on ENs? (b) What strategies EN operators can implement to plan for and quickly respond to such failures and minimize their overall impact? (c) How to leverage the operational flexibility of "smart" ENs to implement these strategies in a structured manner and provide guarantees against worst-case failure scenarios?*

We focus on three classes of cyber-physical failures: (i) Inefficient or unsafe economic dispatch decisions induced by an external hacker who exploits the vulnerabilities of control center software; (ii) Simultaneous disruption of a large number of customer-side components (loads and/or distributed generators) by a strategic remote adversary; (iii) Correlated failures of power system components caused by storm events (or hurricanes) with high-intensity wind fields. We develop new network models to capture the impact of these failures, while accounting for a broad range of operator response actions. These actions include: partial load control, pre-emptive disconnection of non-critical loads, active and reactive power supply by Distributed Energy Resources (DERs) capable of providing grid-forming services, and formation of microgrid islands. We develop practically relevant operational strategies to improve the ENs' resilience to failure classes (i) and (ii) (resp. (iii)) based on solutions of bilevel mixed integer programming (resp. two-stage stochastic optimization) formulations.

Our bilevel mixed integer programming formulations capture the worst-case impacts of attacks on radial distribution networks operating under grid-connected or microgrid configurations. For the case when the operator response can be modeled as continuous decision variables, we provide a greedy heuristic that exploits the radial network structure and provides near-optimal solutions. For the more general case of mixed-binary decision

variables, we develop a computationally tractable solution approach based on Benders Decomposition method. This approach can be used to evaluate the value of timely response actions in reducing various losses to the network operator during contingencies induced by attacker-induced failures. We provide some guidelines on improving the network resilience by proactive allocation of contingency resources, and securing network components in a strategic manner. Furthermore, under reasonable assumptions, we show that myopically reconnecting the disrupted components can be effective in restoring the network operation back to nominal condition.

Our two-stage stochastic optimization formulation is motivated by the need of a decision-theoretic framework for allocating DERs and other contingency resources in ENs facing the risk of multiple failures due to high-intensity storm events. The stochastic model in this formulation captures the dependence of probabilistic failure rates on the spatio-temporal wind intensities. Importantly, the formulation allows for the formation of microgrid islands (powered by the allocated DERs), and considers joint DER dispatch and component repair decisions over a multi-period restoration time horizon. We present computational results based on the classical sample average approximation method, with Benders Decomposition applied to solve the mixed-binary programs associated with the restoration stage. Finally, we compare the optimal repair decisions with a simpler greedy scheduling strategy that satisfies soft-precedence constraints.

Thesis Supervisor: Saurabh Amin
Title: Associate Professor of Civil and Environmental Engineering

Acknowledgments

I thank my advisor, Saurabh Amin, for giving me an amazing opportunity to do research at MIT, and for having all the innumerable intellectual discussions that led up to this thesis. He has been my friend, philosopher, and guide for the past six years. Apart from teaching me to ask the right research questions, he is responsible for providing confidence to an otherwise timid, novice researcher like me to present research with a calm confidence. I am grateful to Dr. Audun Botterud, Prof. Carolina Osorio, and Prof. Ali Jadbabaie for providing valuable guidance, encouragement and support as my committee members. I thank Prof. Saman Zonouz for helping me better understand the cyber vulnerabilities of energy management system software. I want to specially thank Prof. Ian Hiskens for being a collaborator on three of the main contributions that led to this thesis.

I am grateful to my fellow student collaborators Jairo Giraldo, Pengfei Sun, and Derek Chang for helping make successful contributions. I am thankful to Andrey Lokhov, Nathan Lemons, Sidhant Misra and Marc Vuffray for their helpful guidance during my summer internship at Los Alamos National Laboratory. I am thankful to my labmates Li, Manxi, Mathieu, Andrew, and Jeff for gladly providing valuable time and effort in helping me with my committee meeting presentation rehearsals as well as being my wonderful friends.

I can't be grateful enough for my friends Ashwin, Chati, Anand, Bajpayee, Tuhin, Shibani, Pritish, and Apoorvaa for being my family here in the U.S. so far away from my country India.

I thank my Didi, my parents, and my brother for their unfailing love and undying commitment towards me, which made me who I am, and helped me get to where I am today. I thank my beautiful, brilliant wife, Kshama, for being my life partner, and being an incredible source of happiness.

Finally, I thank the financial support provided by EPRI grant for "Modeling the Impact of ICT Failures on the Resilience of Electric Distribution Systems" (contract ID: 10000621), and NSF project "CPS Frontiers: Collaborative Research: Foundations Of Resilient CybEr-physical Systems (FORCES)" (award number: CNS-1239054).

Contents

1 Introduction **17**

1.1 Resilience of electricity networks 20

1.1.1 Security failures 21

1.1.2 Reliability failures 23

1.2 Operational flexibility in smart electricity networks 24

1.2.1 Contingency reserves: allocation and dispatch 25

1.2.2 Post-contingency operations: response and restoration 28

1.2.3 Key issues 29

1.3 Problem statement and research 30

1.4 Related work 35

1.4.1 Models of cyber-security attacks 35

1.4.2 Network interdiction models and algorithms 37

1.4.3 Failure detection and attack-resilient state estimation 38

1.5 Contributions and thesis outline 38

1.5.1 Attack generation and implementation 38

1.5.2 Network models 39

1.5.3 Algorithms for resource allocation, response, and recovery 40

1.5.4 Practical insights 43

2 Vulnerability Assessment of Transmission Network Control Center **47**

2.1 Compromising economic dispatch software 48

2.2 Attack generation using bilevel programming 54

2.2.1 Attacker knowledge 54

2.2.2 Attacker resources . . . 56
2.2.3 Attacker objective . . . 58
2.3 Attack implementation on control center software . . . 60
2.4 Empirical attack deployment results . . . 63
2.5 Cyber-security implications . . . 69
2.6 Online learning of transmission network dynamics . . . 70

3 Vulnerability Assessment of Smart Distribution Networks 79
3.1 Network model with "infinite" substation bus . . . 79
3.2 Defender-Attacker-Defender game . . . 83
3.3 Bilevel optimization problem . . . 94
3.4 Greedy solution approach . . . 102
3.5 Security investments in customer-side devices . . . 105
3.6 Sequential game with linear power flow . . . 125
3.6.1 Optimal attacker and defender set-points . . . 128
3.6.2 Greedy Algorithm to solve $[\widehat{\mathrm{AD}}]$ . . . 130
3.7 A distributed control strategy . . . 131
3.8 Case study . . . 136

4 Resilience-aware Optimal Power Flow 141
4.1 Network model with "finite" substation bus . . . 146
4.2 Bilevel problem . . . 150
4.2.1 Optimal attack for fixed SO response . . . 155
4.2.2 Greedy Heuristic . . . 156
4.2.3 Evaluation of the greedy heuristic . . . 158
4.3 Trilevel optimization problem . . . 160
4.3.1 Insights on optimal SO response . . . 162
4.3.2 Insights on optimal attacker strategy . . . 164
4.3.3 Insights on resource allocation . . . 166
4.3.4 Further insights on resource allocation stage (Stage 0) . . . 168
4.4 Optimal operator response and allocation . . . 169

5 Leveraging Substation Automation Systems for Network Resilience 173

5.1 Value of timely disconnects . . . 173

5.2 Disruption model . . . 182

5.3 Substation Automation system capabilities . . . 186

5.4 Bilevel mixed-binary optimization problem . . . 190

6 Leveraging Networked Microgrids for Distribution Network Resilience 203

6.1 Value of microgrid operations . . . 203

6.2 Multi-microgrid network model . . . 207

6.3 Disruption and Operator response models . . . 219

6.4 Multi-period network restoration . . . 226

7 Resource Allocation and Restoration for Storm-induced failures 233

7.1 Two-stage stochastic optimization formulation . . . 233

7.2 Stochastic failure model . . . 237

7.3 Allocation of Distributed Energy Resources . . . 239

7.4 Joint multi-period repair and dispatch problem . . . 240

7.5 Connections to job scheduling problem . . . 252

8 Conclusions 259

8.1 Summary of results . . . 259

8.2 Recommendations for building resilient grids . . . 261

8.3 Future work . . . 262

List of Figures

1-1 Major parts of power system. . . . 20
1-2 Performance under various response capabilities. . . . 24
1-3 Examples of Distributed Energy Resources. . . . 25
1-4 An illustration of power allocation. . . . 26
1-5 Timeline of events and decision stages. . . . 34

2-1 Physics-aware memory attack on control systems. . . . 50
2-2 Static vs Dynamic Line Rating 56
2-3 Flowchart for attack implementation. . . . 64
2-4 Code and data pointer-based structural memory patterns in PowerWorld. . . 65
2-5 Results of software attack on PowerWorld and Powertools 68

3-1 Precedence description of the nodes for a tree network. . . . 83
3-2 Outline of technical results in Sec. 3.6. . . . 95
3-3 Optimal attacker and defender set-points. . . . 99
3-4 Overall computational approach. . . . 104
3-5 Different defender security strategies. . . . 106
3-6 Illustration of a DER failure scenario. . . . 108
3-7 Reactive power vs Real power output of DERs. . . . 109
3-8 $\mathrm{L_{VR}}$ and $\mathrm{L_{LC}}$ vs M. . . . 111
3-9 Illustrative diagram showing how ℓ changes with sp^{a} 118
3-10 Tree topology of heterogeneous 14 nodes. . . . 137
3-11 Apparent power set points from the OPF and after the attack. . . . 138
3-12 Dynamic response of a nodal voltage and bulk generator frequency 139

4-1 An illustration of power allocation with DERs. . . . 143
4-2 Precedence description of the nodes for a tree network. . . . 154
4-3 Modified IEEE 37 Node Network. . . . 158
4-4 Evaluation of the greedy heuristic. . . . 159
4-5 Modeling framework. . . . 161
4-6 DN topologies 162
4-7 Trade-offs in in maintaining regulation objectives. . . . 163
4-8 Post-contingency losses for different weights of regulation objectives. . . . 169
4-9 Diversification of nodes for voltage vs. frequency regulation. . . . 170

5-2 Performance under various response capabilities. . . . 178
5-3 DN model. . . . 179
5-5 Computational approach to solve (Mm). . . . 193
5-6 Value of timely response ($N = 36$). . . . 200
5-7 Accuracy of BD algorithm. . . . 201

6-1 Performance under various response capabilities. . . . 205
6-2 Multi-microgrid DN model. . . . 209
6-3 Basic taxonomy of DERs. . . . 211
6-4 DER output model. . . . 216
6-5 Droop control model. . . . 218
6-6 Near-optimal performance of BD algorithm. . . . 224
6-7 DN resilience under varying attacker-operator interaction scenarios. . . . 225
6-8 Multi-period DN restoration ($N = 36$). . . . 230
6-9 Near-optimal performance of Greedy Algorithm 10. . . . 231
6-10 Modified IEEE test networks. . . . 232

7-1 Timeline of events and decision stages. . . . 235
7-2 DER model as a voltage source inverter. . . . 243
7-3 Illustrative example: Resource allocation and network repair decisions. . . . 246
7-4 Frequency of distribution line failures and network islands. . . . 249

7-5 Average system performance of the DN under the two track scenarios. . . 250
7-6 Performance of greedy algorithm for Stage 2. 251
7-7 Visualizing network restoration. 253
7-8 Illustration of recursive algorithm. 254
7-9 Illustrative example for recursive algorithm. 256
7-10 Counterexample for recursive algorithm with $m = 2$. 257

List of Tables

1.1 Summary of contributions. 45

2.1 Logical memory structure signatures for critical parameters. 64
2.2 The target parameter value recognition accuracy. 64
2.3 Memory layout (object) forensics accuracy 67

3.1 Table of Notations. 93
3.2 Parameters of the Homogeneous Network 113
3.3 ν vs Different Attack Combinations. 120

4.1 Trade-offs between FR, VR and CM. 164

5.1 Table of Notations. 180
5.2 Typical values of cost parameters. 189
5.3 Resiliency metric evaluated using BD algorithm. 202

6.1 Table of Notations. 208
6.2 Comparison of DER categories. 212
6.3 Resiliency metric evaluated using the BD algorithm. 226
6.4 Typical values of cost parameters. 231

7.1 Statistics of line failure probabilities and island size. 248

Chapter 1

Introduction

The National Academy of Engineering has regarded the electricity grid as "the greatest engineering achievement of the 20^{th} century" [105]. This is supported by the fact that the electricity grids of China and the U.S. are the two largest interconnected machines in the world. Together, these grids comprise over two million kilometers of high-voltage transmission lines and 20 million kilometers of local distribution lines which link thousands of generators to over a billion residential and industrial consumers [42, 105]. They help supply 10 tera-watt-hours of energy annually to power over hundred billion devices in the two largest economies of the world.

Aside from the physical system of generators, networks, components and devices, there is an overlaying cyber system of sensors, control centers, and actuators that form part of the Supervisory Control and Data Acquisition (SCADA) systems. Moreover, there are human agents comprising of the consumers, electricity utilities and power system operators. The consumers have time-varying consumption levels. The power plants, Transmission Networks (TNs) and Distribution Networks (DNs) are owned by profit-maximizing electricity utilities. Finally, there are power system operators, who coordinate, regulate and control the overall operation of the electricity grid.

The overall objective of power system operators is to provide safe, reliable, and affordable supply of electricity to the customers, both residential and commercial. It involves clearing of markets between electricity providers and consumers, maintenance of TNs and DNs with reasonable amount of redundancy, and maintaining supply-demand

balance while the millions of components operate within their operating bounds. The electricity grid is truly an extra-ordinarily complex machine built by humans.

Our modern society is heavily dependent on electricity with a wide range of applications varying in complexity, scale, and criticality. There are ubiquitous but relatively simple residential applications like lighting, water pumps, air-conditioners, microwave, laundry machines, laptops, mobile phones, lifts. Then, there are moderately large applications such as industrial machines, network of computer servers in offices, electronic devices in critical healthcare applications. Lastly, there are also huge and complex systems like communication networks, banking industry, (road, rail and air) transportation systems, intra- and inter-operation of (state, federal, and international) defense and security agencies, etc. Indeed, it will be a hugely cumbersome and chaotic way of life if the entire modern society was suddenly forced to operate without electricity.

Such chaos is very apparent during large-scale blackouts [9, 31, 35]. These adverse events disrupt the way of life for millions of people, sometimes for months. They have devastating consequences not only in terms of monetary loss, but also in loss of human safety, and even increased risk to national security. By the simple virtue of having a huge number of components, many of which are very large in size, the electricity network components are out there in open. It is near impossible to secure every component against reliability failure occurring because of gradual wear and tear due to mechanical movements and/or changing weather conditions. Even those components which are underground, are prone to failure due to short-circuits resulting from flooding or a rodent coming in contact with live wire.

Indeed, the power system operators are facing challenges of reliability failures on an ageing infrastructure burdened by ever-increasing demand. Failure of a small number of components leads to small scale outages which cause inconvenience to consumers. However, extreme weather events or natural disasters such as hurricanes, earthquakes, Tsunamis, etc. can lead to *correlated* failures of a large number of power system components [19]. Such large-scale disruptions can lead to loss of power supply for months. In 2018, the blackouts resulting from three major hurricanes in the US resulted in an economic loss of over 300 billion dollars to the US economy. However, natural disasters are

not the only causes of large-scale blackouts. Widespread outages can also result from lack of enough network visibility to the system operators, active or reactive power shortfall, or under-utilization of network capacity [9].

To alleviate some of these issues, there has been also modernization of grids being undertaken. At the transmission level, there are deployment of smart sensors, e.g. Dynamic Line Rating (DLR) sensors and Phasor Measurement Units (PMUs). These sensors increase the visibility of system operators to allow for improved state estimation and dispatch capabilities. On the distribution side, there has been rapid integration of novel components such as Electric Vehicles (EVs) and Distributed Energy Resources (DERs) and smart inverters in the DNs. DERs, in particular, include small-scale diesel generators, roof-top PhotoVoltaic (PV) panels, small wind turbines, storage devices. Novel functionalities such as direct load control and smart net metering are also being implemented. Additionally, the SCADA systems are being implemented by off-the-shelf Information Technology (IT) systems, instead of legacy closed communication networks. This has resulted in cheaper, faster, and flexible control of power system operations at the transmission and distribution level.

Although such modernization of grids into "smart" grids provides operational flexibility for the system operators, it has also increased the cyber-attack surface. The "open" nature of the off-the-shelf IT systems expose the smart grids to inherent as well as novel vulnerabilities that can be exploited by remote adversaries. This has been well illustrated by the recent Ukraine attacks [75], where foreign state actors were able to remotely open the circuit breakers within a few distribution grids, as well as damage the software controllers at the distribution substation in Ukraine. In [98], the power system experts have shortlisted a number of critical cyber vulnerabilities of modern DN systems.

The goal of the thesis is to develop a systematic approach to evaluate and improve the resilience of ENs by addressing following questions: *(a) How to model security and reliability failures and assess their impact on ENs? (b) What strategies EN operators can implement to plan for and quickly respond to such failures and minimize their overall impact? (c) How to leverage the operational flexibility of "smart" ENs to implement these strategies in a structured manner and provide guarantees against worst-case failure scenarios?*

In the rest of the chapter, we firstly discuss the vulnerabilities of electricity networks in the context of recent adverse events. Secondly, we discuss the operational flexibility provided by modern smart electricity networks that can be exploited by system operators. Thirdly, we describe the overarching resiliency framework and the objective of the thesis. Fourthly, we briefly state the work of related papers in existing literature. Finally, we summarize our findings and contributions, and with the thesis outline.

1.1 Resilience of electricity networks

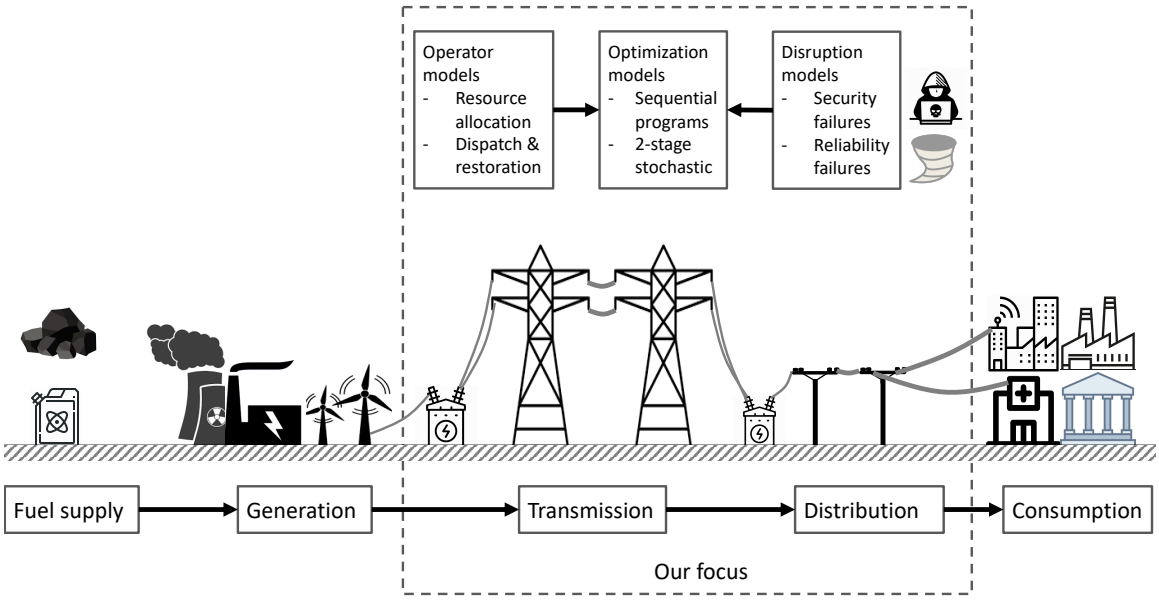


Figure 1-1: Major parts of power system. Figure shows (from left to right) conventional sources of energy, bulk power plants, transmission towers, distribution poles, and electricity consumers (smart buildings, industries, hospitals, universities).

Generically, resilience of a system is defined as "its ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events" [93]. The operation of power grid consists of five major parts: fuel supply, power generation, transmission, distribution and consumption; see Figure 1-1. For the grid to operate resiliently, each of these major parts need to be operationally resilient. Therefore, one can find several interpretations of power system resilience in the literature.

One interpretation of resilience of power systems is stated in the context of the fuel supply part. It states that the amount of fuel to be kept in reserves should at least be suffi-

cient to generate electricity for 75 days [25]. Such reserves will be crucial if the fuel supply chain is affected. For example, disruptions in fuel supply chain could result from natural disasters, accidents to the ships carrying the fuel, or sanctions on a country regarding nuclear power supply, etc [143]. Another interpretation regarding the consumption part is that the amount of electricity theft should be below a certain threshold [87]. In some regions of developing countries, electricity theft is a huge problem, and the amount of theft estimated is about 50 percent [119].

Although the resilience of other parts such as fuel supply, generation, and consumption are important, in this thesis, we limit the scope of our research to the resiliency assessment of the transmission and distribution networks. For a systematic approach to analyze network resilience, we first consider the vulnerabilities in the electricity network components, both physical as well as cyber. Then, we identify potential threat actors which include strategic adversaries that cause security failures as well as natural disasters which result in reliability failures. Finally, we assess the potential impact that would result from the exploitation of vulnerabilities of modern ENs in terms of strategic or correlated failures. Such a vulnerability assessment is crucial for identifying good proactive and reactive strategies for the system operators (Sec. 1.2).

1.1.1 Security failures

Security failures are disruptions of network components that are carried out intentionally by malicious adversaries. As stated earlier, the use of electricity is very crucial for normal day-to-day life as well as effective functioning of security agencies. This provides motivation for the threat actors (malicious adversaries) to disrupt the ENs. Our attack models are motivated by the security failure scenarios discussed in [98]. These scenarios capture the capabilities of the following threat actors: (i) cyber-hackers of an enemy nation motivated to disrupt supply to critical facilities, (ii) a malicious adversary looking to extort ransom money from the utility, or (iii) a disgruntled internal employee motivated by revenge. In this paper, we are concerned with type (i) actors. Furthermore, the sheer size and number of the network components make it near impossible to secure every component. Thus, this is a big vulnerability that malicious adversaries can exploit by physical attacks.

An example of physical attacks on the U.S. grid is the sniper attack on the California substation [1]. In this attack, the attackers damaged 17 transformers, which cost the electricity utility $15 million worth of equipment damage. Later, the utility decided to invest another $100 million in upgrading the physical security of its substations. Another example of physical attacks is that of the 2015 attack in Pakistan [127]. Reportedly, some rebels damaged two transmission lines which resulted in 80% of the country plunging in darkness. It also negatively affected operations of nearby airports. Such rebels had also previously attacked Pakistan's power grid, but the level of impact of those attacks was not as significant.

Another way to disrupt the power system is via cyberattacks onto the SCADA system or via compromise of the components which can be accessed via the Internet. Recent event which brought the cybersecurity aspect of power systems into limelight was the Ukraine attack [75] in December 2015, which was the first successful cyberattack on any electricity grid. The cyber vulnerability was that the Ukrainian utility had not implemented a two-factor authentication system. Allegedly, the cyber hackers of a foreign country exploited this vulnerability to hack into the SCADA system. They first obtained the user credentials of distribution system operator via phishing attacks. Then, they remotely caused the opening of circuit breakers on the eve of Christmas. As a result, power supply was lost for several hours. The hackers also managed to damage the software of controllers, which the utility was not able to repair for months. Therefore, the utility operators had to perform control actions manually. In December 2016, another such cyberattack was carried out on a transmission substation in Kiev. A feature of this cyberattack was that the attack was fully automated and required no intervention by the attackers.

Due to its heavy reliance on automated control operations, a response via manual control actions will not be conducive in the context of the US power grid. The US Department of Homeland Security has issued alerts to the power companies regarding the ongoing, prevalent cyberattacks [46]. Moreover, when the security experts investigated the attacked SCADA system, their findings suggested that the cybersecurity of US power grids is in fact less secure than that of the attacked Ukrainian grid. In a US Congressional service report [32], the power cybersecurity policy experts reported the cyber attacks on

the European power grids. The cyberattacks managed to hack gained a backdoor entry into the SCADA system by accessing the website of a renewable power utility. All these real-world incidents highlight the vulnerability of modern power systems to both cyber and physical attacks.

1.1.2 Reliability failures

Although the number of incidents of security attacks are on rise, the impact of weather-induced reliability failures has been even more significant. Weather-related outages in electricity networks continue to show an upward trend as utilities face the dual problems of deteriorating power grid infrastructure and higher frequency of natural disasters (such as hurricanes [31, 79]). Prolonged delays in restoring the power system of Puerto Rico in the aftermath of Hurricane Maria highlight the importance of strategic planning and efficient response to such events. In 2018, the damage to power systems due to 3 hurricanes resulted in an economic loss of over $300 billion.

In 2018, heat waves in Australia resulted in excessive demand which led the grid to become overloaded [14]. Consequently, several outages in multiple distribution networks led to half a million homes without electricity during a heat wave. Similar incident occured in India July, 2012 [35]. Excessive demand caused by a heat wave resulted in a failure of a critical transmission line because of overloading. This resulted in a blackout which caused around $1/10^{th}$ of the world's population (600 million people) to be without electricity for two days.

Another interesting incident was the 2016 blackout in South Australia [141]. Three factors resulted in this blackout [64]: (i) extreme weather events (two tornadoes happening over 170 km apart), (ii) reduced inertia of generation mix (because of increased penetration of inverter-controlled renewables), and (iii) overly sensitive protection mechanisms. This event, in particular, highlights the vulnerability of power system to both extreme weather events and the modernization of grids.

1.2 Operational flexibility in smart electricity networks

Now, we describe the increased operational flexibility available to the system operators of modern ENs due to the integration of novel components and functionalities.

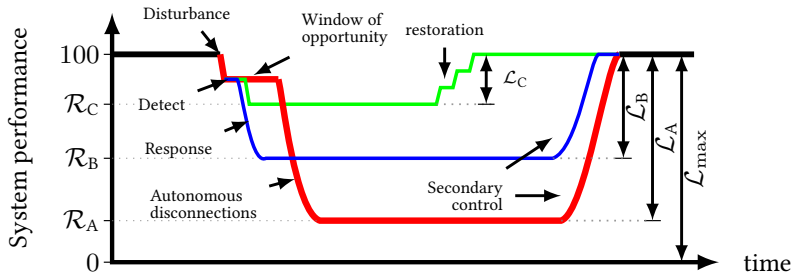


Figure 1-2: Performance under various response capabilities.

After an adverse event (i.e. a security or reliability failure), the system performance likely degrades. However, to what extent it degrades and how quickly it restores depends on the available operator proactive and reactive capabilities. Figure 1-2 shows how system performance evolves over time after an adverse event. Initially, the system is operating in nominal conditions. As a result of the disturbances resulting from the adverse event, the system performance degrades. If the operator fails to respond in a timely manner (within few seconds), then an uncontrolled cascade can occur (resulting in a post-contingency loss $\mathcal{L}_A$). Such a cascade is triggered due to activation of protection mechanisms (autonomous disconnections) that isolate the components based on local measurements. However, to regain nominal operation, the operator eventually undertakes secondary control actions (e.g. generator redispatch, changing tap settings of transformers, switching on capacitor banks). Thus, the nodal voltages and frequency recovers, allowing the possibly disconnected loads to reconnect and system performance is restored. However, with some better response capability, say B (or C), the operator may be able to reduce the post-contingency loss to $\mathcal{L}_B$ (or $\mathcal{L}_C$). Next, we consider what such response capabilities might be which the modern ENs have to offer to system operators.

1.2.1 Contingency reserves: allocation and dispatch

During the operation of any electricity network, the main constraints are as follows. There are power flow equations which are physical laws and, therefore, must be satisfied. The other constraints model the operating behaviour of the components, e.g. power consumed by loads. Finally, there are operating constraints, which model the frequency and voltage regulation as well as line capacities. However, one or more of these operating constraints may be violated as a result of the adverse event. We argue that such violations result in a contingency. Thus, we view a *contingency* as a sudden, unplanned incident caused due to failure of one or more components that has a direct effect on the operating constraints of the EN [22]. Based on the number of failed components, contingencies can be classified as

- *single contingency* - if there is a loss or failure of a single component; or
- *multiple contingency* - if there is a simultaneous loss of multiple components [22].

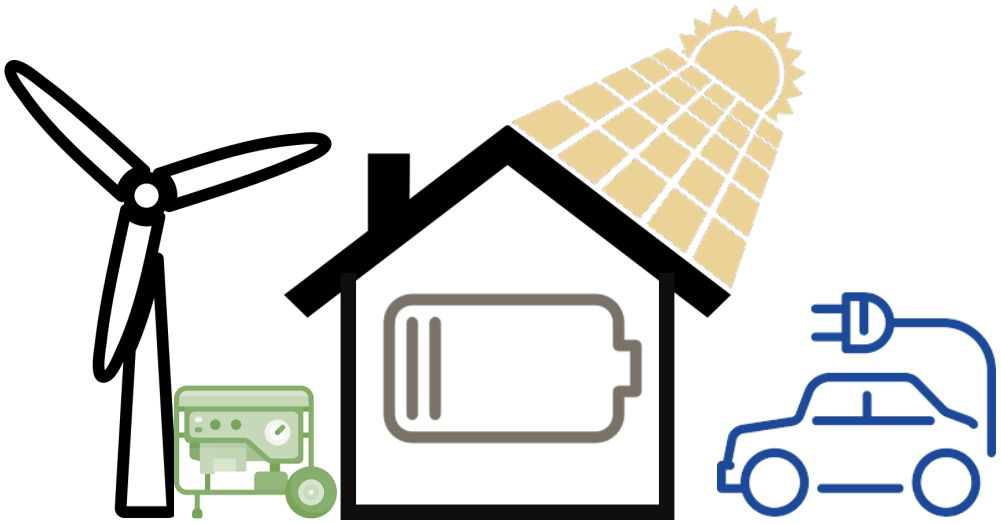


Figure 1-3: Examples of Distributed Energy Resources. Figure shows (from left to right) a small wind turbine, diesel generator, a residential storage device, rooftop solar panel, and an electric car.

The integration of DERs (see Figure 1-3) into the DNs has allowed sources of power to be closer to the demand nodes, which results in lower transmission and distribution losses [50, 129]. In addition, they can also be used as contingency reserves which can be

dispatched during contingencies [133]. To prevent or limit the impact of contingencies, the spatially distributed DERs within a DN and a big generator (BG) supplying power to the DN via the substation can be redispatched; see Figure 1-4. Any point on the supply-demand balance line is a resource allocation that determines the amount of power supplied by the BG and the amount of power supplied by the DERs. If the power consumed by loads is curtailed, then the supply-demand line shifts inwards due to reduction in aggregate demand. The capacity of an energy resource (BG or the DERs) in *excess* of the power supplied by the resource determines the *reserves* provided by that energy resource.

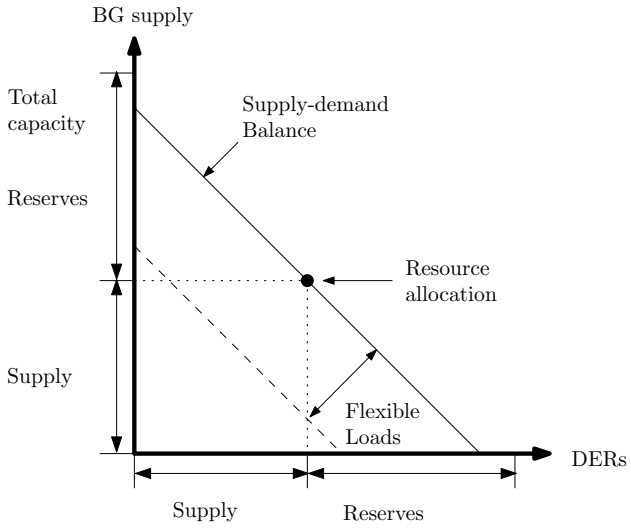


Figure 1-4: An illustration of power allocation through a BG and spatially distributed DERs.

In the post-contingency situation, violations of operational constraint(s) must be contained by the operator. If such violations are not resolved in a timely manner, additional components may fail, which can result in new contingencies. For example, significant loss of DER supply in highly loaded DNs may result in a drop in node voltages below a critical threshold causing other supply sources to trip, potentially resulting in a network effect (or cascade) [101]. Thus, planning for sufficient resources is essential so that the SO is able to meet regulation objectives in contingency situations. Typically, these objectives include voltage regulation (VR), frequency regulation (FR), and capacity management (CM) [30]. In particular, lack of adequate active power resources can cause loss of frequency regulation, and the scarcity of reactive power resources can lead to voltage fluctuations. In

addition, in many situations, the capacity of one or more lines limits the reallocation of power that is needed to serve demand during contingencies [22, 35]. These factors have been identified as crucial for resilience of electricity grids [9, 22, 131], and are poised to become significant even for DNs.

In recent years, thanks to technological improvements and reduced cost of deployment, DERs have emerged as a promising solution for provision of reserves; in particular, by means of active and reactive power control [30, 128]. These functionalities are enabled by the appropriate power electronics and allow the DERs to respond to a range of fluctuations in a fast manner (order of milliseconds) as opposed to the slower response via traditional means, which is typically in the order of few seconds to few minutes. Thus, allocation of DERs as reserves to facilitate fast response for meeting regulation objectives is both an interesting and important problem; which we consider in the context of DN resilience.

Another significant aspect of modern DNs is that there are opportunities to allow for partial DN operation in situations when bulk supply (from the transmission side) is no longer available. In such cases, microgrids can be operationalized during the recovery and repair period. Indeed, extensive literature is available on the allocation of repair crew and optimal response operations [11, 126, 132, 137]. These contributions primarily focus on resource limitations, failure uncertainties, and physical constraints. However, the problem of proactive allocation of temporary generators in the pre-storm stage has received limited attention in the literature. This opportunity becomes especially relevant given the technological progress in portable DERs and microgrid technologies [39]. The significance of proactive DER allocation in the face of natural disasters has already been acknowledged by federal agencies [65, 129]. A strategic placement of DERs at a subset of DN nodes in the pre-storm stage, given the uncertainty in component failures can be done to minimize the resulting lost load. Such proactive resource allocation strategies can significantly support the post-contingency response and restoration operations.

1.2.2 Post-contingency operations: response and restoration

After an adverse event, if the operator fails to respond in a timely manner, the protection devices get triggered resulting in autonomous disconnection of the components. The operation of these devices is based on local checks of operating bounds, and thus does not rely on the collected voltage and power consumption/generation readings from all over the EN. This is typically the case for legacy EN management systems where the operator does not have access to node-level data. Consequently, an operator relying solely on this response capability does not have the ability to timely detect, accurately identify, and promptly respond to coordinated or correlated disturbances in an EN during an adverse event. As such, one can view this capability simply as "no response" from the operator, since the disconnect operations are local and do not benefit from network-level coordination by the operator.

The traditional operator response actions in a DN include control of voltage regulators and capacitors, and network reconfiguration. However, the time-scale of disturbance created by the adverse event can be very small (few seconds), and can trigger the autonomous disconnections due to operating bound violations. Typically, voltage regulators and capacitor banks require a larger response time; in fact, frequent activation of these devices is not preferred as they are subject to mechanical wear and tear [3]. On the other hand, thanks to advancements in the Substation Automation (SA) systems and power electronics based control of loads/DGs, a response strategy can be implemented within a few milliseconds after the information about the timing and extent of disruption is obtained by the Substation Automation (SA) system.

We consider an emergency response exploits the capabilities of modern SA systems that have the visibility of node-level consumption, distributed generation, and nodal voltages. Many of the newer installations of smart meters are already equipped with data logging and communication capabilities. The temporal frequency of data collected by low-voltage residential meters can vary from 15 minute to 24 hour intervals, depending on the desired control functionalities, customer privacy levels provided by the operator as well as the available communication bandwidth between DN nodes and the SA. However,

the smart meters installed at medium voltage to low voltage transformers at DN nodes can be utilized to provide aggregated node-level data from the customer meters in real-time (every second). With this capability, sudden supply demand changes in the nodes can also be detected by the SA. This level of monitoring does not involve individual customer meter readings, and hence, does not violate privacy regulations. We posit that the currently available capabilities of collection and processing of node-level data can be exploited by the operator to implement fast response strategies through SA.

The use of microgrid technologies such as microgrid islanding and dispatch of DERs [84, 100, 133] toward improving DN resilience. Historically, the idea of DER-powered microgrids as a response mechanism has been considered for responding to reliability failures [63, 100, 133]. Indeed, microgrids have been implemented to support the reliability targets of critical facilities such as hospitals, industrial plants, and military bases. However, their technological feasibility (and related operational aspects) in responding to security failures has received limited attention. We address this issue by building, and focus on evaluating the effectiveness of DER-powered microgrids in limiting post-contingency losses after a disruption. Furthermore, we also consider the use of microgrids in facilitating power supply while the EN restoration process is taking place after security or reliability failures.

1.2.3 Key issues

As illustrated from the incident reports of the security and reliability failures listed in Sections 1.1.1 and 1.1.2, the power systems are vulnerable to simultaneous disruptions of multiple components resulting from correlated or strategic failures. The operators do N-k security-constrained optimal power flow, where N is the number of components in the network, and k is the number of components which can get disrupted simultaneously. However, the value for k is chosen typically 1 or 2, to account for reliability failures resulting from single or double contingencies due to normal wear and tear of individual components. However, the nature of correlated/strategic failures necessitate the consideration of multiple contingencies (i.e. $k \geqslant 3$). However, as the value of k increases, the number of potential N-k contingencies grows combinatorially.

Secondly, the power flow constraints which are integral to operation of ENs are highly non-convex. As a result, even the relatively simpler problem of determining an optimal response for a given contingency is non-trivial. When we consider the task of determining the worst N-k contingency assuming optimal response by the operator, the problem becomes even more computationally expensive. Therefore, the scalability of solution approaches is a huge consideration.

Thirdly, the solution approaches for the vulnerability assessment problems do not provide any structural insights into the critical components or optimal response. As a result, if there are even minor modifications to the network (in terms of addition/deletion or securing of a small subset of components), then the worst-case vulnerability or optimal operator response strategies can change drastically. Therefore, it is desirable to develop solution approaches that provide some practical insights so that we can systematically approach the problem of improving resilience of ENs.

1.3 Problem statement and research

Now, we describe the problem formulations considered in this thesis. Since the disruption model of security and reliability failures are inherently different, we consider two separate classes of problem formulations. First, we describe the main formulations for case of security failures, which we pose as bilevel optimization problems.

The first problem which we consider is that of a semantic-aware attack generation against the electricity transmission networks. In this problem, the attacker exploits his partial knowledge of power system operations to compute target malicious power system parameters. The attacker's goal is to implement the optimal attack using a targeted manipulation of specific power system parameters that reside within a control process's dynamic memory space. We pose the problem of generating a physics-aware attack is posed as a sequential game between the attacker (leader) and the follower (grid operator). In the first stage, the attacker chooses power system parameter manipulations with the objective of maximizing the violation of capacity limits; in the second stage, the operator solves the Economic Dispatch (ED) problem to determine generator output levels while facing the manipulated parameters chosen by the attacker in the first stage. Our goal is

to show that the optimal power injections and nodal voltages computed using the manipulated parameters yield suboptimal and unsafe power flow allocations. Moreover, this can significantly increase the possibility of cascading failures and the risk of subsequent emergency actions.

Next, we consider a class of bilevel optimization problems for resiliency assessment in distribution networks with radial topologies [109, 110, 114, 115]. The Stage 1 problem represents a disruption model that captures impact of attacker-induced disruptions on the DN. In Stage 2, the operator implements a range of available response strategies. In the two stages of the game, the objective of the attacker (resp. operator) is to maximize (resp. minimize) the post-contingency loss (i.e. weighted sum of cost incurred due to operating bound violations) and cost of operator control actions subject to constraints due to power flow, and DER/load models. A generic form of the bilevel problem is as follow:

$$\begin{aligned} \mathcal{L}_{\text{Mm}} \quad := \quad & \max_{d \in \mathcal{D}_{\text{k}}} \min_{u \in \mathcal{U}(d)} \quad C_{\text{post-contigency}}(u, \mathrm{x}) \\ & \text{s.t.} \quad \mathrm{x}(d, u) \in \mathcal{X}, \end{aligned} \tag{1.1}$$

where $\mathcal{L}_{\text{Mm}}$ denotes the Max-min (Mm) post-contingency loss used for evaluating DN's resilience; d an attacker-induced failure; k the attacker's resource constraint; $\mathcal{D}_{\text{k}}$ the set of attacker's strategies; u an operator response; $\mathcal{U}(d)$ the *coupling* constraints that define the set of feasible operator responses under the impact of attack-induced failures; x the post-contingency network state, i.e. the state after the attacker-operator interaction is completed; $\mathcal{X}$ the set of constraints that model physical constraints (power flows), component constraints (loads and DGs), and nodal voltage and frequency constraints. For a given disruption $d \in \mathcal{D}_{\text{k}}$, the operator's objective is to minimize the post-contingency loss $L(u, \mathrm{x})$, and the attacker's objective is to choose an attack that maximizes the post-contingency loss assuming an optimal response by the operator. Suppose that $(d^\star, u^\star)$ is an optimal solution to this maximin problem which results in the network state $\mathrm{x}^\star$. Then $\mathcal{L}_{\text{Mm}} = L(u^\star, \mathrm{x}^\star)$ is the post-contingency loss that is incurred by the operator when he implements $u^\star$ in response to the attack $d^\star$.

These formulations differ in the specific disruption models, operator response capabil-

ities, and the post-contingency loss under consideration. In these bilevel problems, the attacker problem (Stage 1) consists of either binary variables [110, 114, 115] or mixed-binary variables [109, 111]. The inner problem either consists of continuous variables [109, 109] or mixed-binary variables [114, 115]. The disruption model considers the joint impact of attacker-induced supply demand-disturbances at the DN nodes as well as the impact of TN-side disturbances at the substation voltage and system frequency. On the other hand, the operator model consists of a range of capabilities which include load control, component disconnects, DER dispatch, and microgrid islanding. The post-contingency losses capture the cost of operator control actions (load control/shedding) and cost of operating bound violations (loss of voltage or frequency regulation). The exact post-contingency loss function depends on the specific operator response capability under consideration.

By solving the problems in stages 1 and 2, we obtain optimal strategies for the attacker and the SO, which provides insights into answering two Stage 0 problems:

- Optimal allocation of power and contingency reserves in DERs, and
- Optimal security strategy for securing DN nodes against remote node compromises.

We refer to the first problem as Resilience-Aware Optimal Power Flow (RAOPF) [110]; see Chapter 4. The Stage 0 problem represents the operator's problem of resource allocation for optimal power flow and planning of reserves in anticipation of an attack. The operator's objective in Stage 0 is to minimize the sum of cost of resource allocation and the maximin post-contingency loss. On the other hand, we refer to the optimal security problem as a Defender-Attacker-Defender (DAD) game. In this game, in Stage 0, the operator invests in securing a subset of DER nodes but cannot ensure security of all nodes due to his budget constraint [109]; see Chapter 3. In this problem, the operator's goal in Stage 0 is to minimize the maximin post-contingency loss incurred in Stages 1 and 2.

Overall, the decisions in each of the three stages of the two problems (RAOPF and DAD game) can be summarized as follows:

- *Stage 2*: Given a fixed Stage 0 operator strategy (reserve allocation or secure a subset of DN nodes) and a fixed contingency, what is the optimal operator response in terms of dispatch of available resources?

- *Stage 1*: Given a Stage 0 operator strategy, and the assumed attacker model, what is the optimal attack that maximizes the post-contingency cost, assuming the operator will respond optimally?

- *Stage 0*: What should be the optimal allocation/security strategy, assuming the optimal strategies of the attacker and the operator in Stages 1 and 2, respectively?

These bilevel formulations enable the evaluation of DN resilience in terms of its ability to minimize the impact of attacker actions.

Additionally, when the DNs consist of microgrids, we introduce a problem about restoration of DN performance over multiple time periods; see Chapter 6. In each time period, the operator can, subject to some resource constraints, restore the functionalities of the components disrupted by the attacker actions. The operator's objective is to determine an optimal restoration strategy which minimizes the sum of post-contingency losses over the multiple time periods. This problem enables the resiliency assessment of the DN in terms of its ability to restore system performance after a security failure.

Now, we describe the problem formulation pertaining to the weather-induced failures in the DNs, in particular the failures induced by tropical storms. We formulate a two-stage stochastic mixed-integer problem which considers the strategic DER placement decisions in Stage 1 (pre-storm), and a multi-period repair problem with DER dispatch within each microgrid in Stage 2 (post-storm); see (1.2). For the ease of exposition, we refer to this problem as 2-SMIP problem. The objective is to minimize the sum of the cost incurred in DER allocation and the expected cost of unmet demand during the time period of repair and recovery operations. For a given DER allocation (placement) and for a realization of DN component disruptions, Stage 2 is a deterministic multi-period problem in which line repair schedules and dispatch within each microgrid are jointly determined. From a practical viewpoint, each period can be viewed as one work shift of the repair crews. In the 0^{th} period, the subnetworks formed as a result of disruptions start to operate as microgrids using the available DER supply. In the subsequent time periods, damaged lines are repaired, permitting connections between smaller microgrids to progressively form larger microgrids. In the last time period, the DN is connected back to the main grid,

and normal operation is restored. Crucially, the Stage 2 problem relies on an estimate of the total number of time periods needed for full recovery. It also utilizes a novel model of linear power flow within a microgrid island with parallel operation of multiple DER inverters. Figure 7-1 summarizes the order of events and decisions in our formulation.

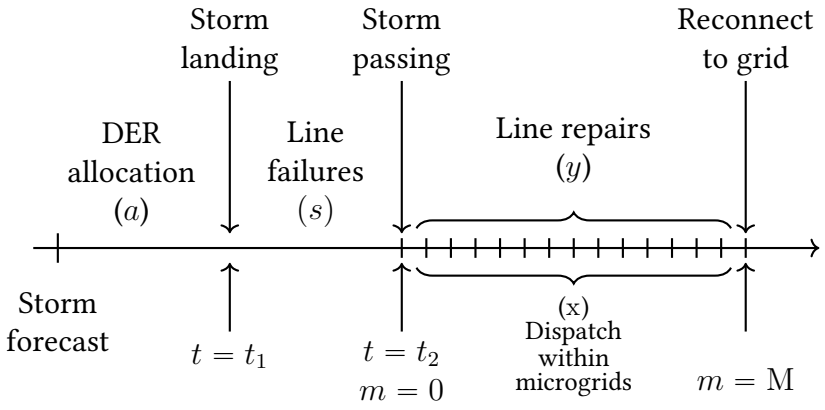


Figure 1-5: Timeline of events and decision stages. The DER placement decision (a) is made before the storm hits the network ($t = t_1$). Uncertainty s is realized over the course of the storm. After passing of the storm ($t = t_2$, $m = 0$), optimal power flow and line repair decisions (x, y) are made. At $m = \mathrm{M}$ (end of repair time horizon), the network is fully restored.

Our formulation considers a tree DN with nodes and distribution lines $\mathcal{G} = (\mathcal{N} \bigcup \{0\}, \mathcal{E})$, where $\mathcal{N}$ denotes the set of all DN nodes. The substation node is labeled as 0, and it also forms the connection to the bulk supply through a transmission network. The set $\mathcal{E}$ denotes the set of directed edges, such that the edges are directed away from the substation node. The first-stage problem is as follows [4]:

$$\min_{a \in \mathcal{A}} \left\{ g(a) := {\mathrm{W}_{\text{alloc}}}^T a + \mathbb{E}_{S \sim \mathcal{P}} J(a, S) \right\}, \tag{1.2}$$

where a denotes a resource allocation strategy to be chosen from the set of feasible strategies $\mathcal{A}$. The uncertainty in the random vector S characterizes the random failures of distribution lines and has a probability distribution $\mathcal{P}$ defined over the set of possible line failure scenarios $\mathcal{S} := \{0, 1\}^{\mathcal{E}}$. In (1.2), $\mathrm{W}_{\text{alloc}}$ is a length-$|\mathcal{N}|$ vector of the allocation cost per unit resource at the nodes, ${\mathrm{W}_{\text{alloc}}}^T a$ is the cost of resource allocation and $\mathbb{E}_{S \sim \mathcal{P}} J(a, S)$ is the expected cost of unmet demand under allocation scheme a.

To model the post-storm multi-period dispatch with repair scheduling, we consider an a priori fixed time horizon with M periods. Let $\mathcal{M} := \{0, 1, \cdots, \mathrm{M}\}$ denote the set of all periods. We denote a period by m. For a specific realization of line failures $s \in \mathcal{S}$, $J(a, s)$ denotes the optimal value of the second-stage problem which is given as follows:

$$\begin{aligned} J(a,s) := \min_{\mathrm{x}^s, y^s} \quad & \sum_{m=0}^{\mathrm{M}} {\mathrm{W}_{\text{dem}}}^T \mathrm{x}^{m,s} \\ \text{s.t.} \quad & y^s \in \mathcal{Y}(s), \quad \mathrm{x}^s \in \mathcal{X}(a,s,y), W \begin{bmatrix} x \\ y \end{bmatrix} \geqslant h - Ua \end{aligned} \tag{1.3}$$

where W, h, and U correspond to constraint parameters. where the scenario-specific second-stage decision variables $\mathrm{x}^s = \{\mathrm{x}^{m,s}\}_{m \in \mathcal{M}}$ and $y^s = \{y^{m,s}\}_{m \in \mathcal{M}}$ respectively denote the collection of dispatch and line repair actions for each period. For a failure scenario $s \in \mathcal{S}$, $\mathcal{Y}(s)$ denotes the set of feasible repair schedules, and $\mathcal{X}(a, s, y)$ denotes the set of feasible power flows under the DER allocation a, and chosen line repair schedule $y \in \mathcal{Y}(s)$.

1.4 Related work

Our work is motivated by recent progress in three topics: **(T1)** Cyber-security attacks of networked control systems [6, 34, 54, 80, 89, 97, 121, 146]; **(T2)** Interdiction and cascading failure analysis of power grids (especially, transmission networks) [20, 102, 103, 142]; and **(T3)** Control of distribution networks with DERs and microgrids [40, 53, 67, 130, 133].[1]

1.4.1 Models of cyber-security attacks

The adversary model in Chapter 3 considers simultaneous DER node compromises by false-data injection attacks. Thanks to the recent progress in **(T1)**, similar models have been proposed for a range of cyber-physical systems [89, 97]. Our model is motivated by the DER failure scenarios proposed by power system security experts [98]. These scenarios consider shutdown of DER systems when an external threat agent compromises the DERs by a direct attack, or by manipulating the power generation set-points sent from the control center to individual DER nodes/controllers.

[1] The topic (T3) has been discussed in detail in Sec. 1.2.

Our approach to model DN-side disruptions can be extended to other types of attacks, including disruption of loads or circuit breakers. Despite its simplicity, our approach to model DN-side disruptions can be applied to capture the physical impact of a broad class of security failure scenarios. This class includes Distributed Denial-of-Service (DDoS) attacks on the power grid components that can result in simultaneous failures [49, 120, 144]. Another relevant attack scenario is motivated by the vulnerabilities of Internet connected customer-side devices (e.g. smart inverters, air conditioners, water heaters), also known as Internet-of-Things (IoT) devices [49]. An adversary can hack into these components via a cyberattack, create an IoT botnet, and can acccess them via Internet. Indeed, recent work in cyber-security of power systems has identified risk of correlated failures (e.g. simultaneous on/off events) induced/caused by IoT botnets [120]. In our disruption model, the impact of such an attack can be straightforwardly modeled by load/DG/line disconnects, leading to sudden supply-demand disturbance. However, a single point of failure such as a cyberattack on DGMS is perhaps a more critical threat to DNs with significant penetration of DGs.

One specific related line of research is proposed false data injection (FDI) attacks [80, 125, 135] that have been explored over the past few years. FDI assumes compromised set of sensors and make them send corrupted measurements to electricity grid control centers to mislead the state estimation procedures. The authors propose a system *observability* [80] analysis to determine the required minimal subset of compromised sensors to evade the electricity grid's bad data detection algorithms [86]. The power system stability has also been studied under corrupted real-time pricing signals [124]. As a fundamental domain-specific monitoring tool for cyber-physical platforms, state estimation is to fit sensor data to a system model and determine the current state [2, 6]. Existing real-world solutions to analyze power system stability [61] run every few minutes [118]. These solutions do not consider the cyber-side controllers and/or adversarial settings [12, 138]; hence they may miss malicious incidents such as the controller code execution attacks. Risk assessment techniques, e.g., contingency what-if analyses [123] investigate potential power system failures speculatively. However, enumeration of all *possible* incidents is a combinatorial problem and does not scale up efficiently in practical settings [43].

1.4.2 Network interdiction models and algorithms

Indeed, previous literature has dealt with issues related to resilience of power systems [77, 103, 121]. Existing work in **(T2)** employs state-of-the-art computational methods for solving large-scale, mixed integer programs for interdiction/cascade analysis of transmission networks assuming direct-current (DC) power flow models. Several papers have used bilevel optimization formulations for vulnerability assessment of TNs to adversarial disruptions [24, 97, 103, 121]. Another notable application is the generalization of the classical N-1 security problem to an N-k problem [24, 121]. These formulations typically assume the DC power flow approximation and continuous decision variables in the inner problem. The latter enables a KKT-based solution approach reformulation, and leads to single-level Mixed-Integer Program (MIP).

However, when the inner problem consists of binary variables, the solution approaches become scarce. In this case, the bilevel problem is called a Bilevel Mixed-Integer Program (BiMIP), with an additional feature of having conflicting objectives in the inner (operator) and outer (attacker) problems. In general, one can reformulate a BiMIP into single level MIP (for example, using high-point relaxation (HPR) problem [92, 140]), and use advanced branch-and-bound algorithm to solve the problem. However, the HPR is a weak relaxation of the original BiMIP due to directly conflicting objectives [69, 72]. More recent work has developed intersection cuts [55, 56] and disjunction cuts [85, 134] – these approaches introduce stronger cuts for the HPR problem. However, these approaches are suitable for BiMIPs in which the inner problem has integer coefficients in the constraints. On the other hand, the BiMIP interdiction problems on power systems infrastructure which we consider have fractional coefficients. A recent paper by Hua et. al [69] addresses this issue by applying Generalized Benders decomposition method. Another approach by Zeng and An [145] uses Column Constraint Generation (CCG) method, whose iterations progressively add variables and constraints (particularly, the disjuntive constraints resulting from the KKT conditions for the inner problem with fixed binary variables). While these approaches are certainly of interest in solving (1.1), we find that our proposed approach achieves desirable computational performance as discussed in Chapters 5 and 6.

1.4.3 Failure detection and attack-resilient state estimation

Another well-studied attack model in the literature considers false-data injection attacks to a (small) subset of sensors in order to inject biases in state estimates, while being undetected by anamoly detectors [54, 59, 81]. Available results include identification and security of "critical" sensors and attack-resilient state estimation. However, a less commonly studied aspect is that of incorrect control actions that could be implemented as a result of biased state estimation. Based on our previous work [112], one can argue that our disruption model can be tailored to capture the changes in supply/demand of network nodes due to disruption of DGs/loads and/or component disconnect actions that may be induced by successfully bypassed false-data injection attacks on sensor data used by the control center.

1.5 Contributions and thesis outline

In this thesis, we develop a quantitative framework to evaluate the resilience of smart ENs in the wake of cyberphysical disruptions. Developing this framework involved: (a) identifying appropriate resiliency metrics for the ENs (e.g. value of lost demand or increased operating costs), (b) modeling of smart grid control capabilities (e.g. dispatch of distributed energy resources [109, 110], component disconnects [114, 115] or microgrid islanding [115]); and (c) developing relevant disruption models (adversary-induced strategic disruptions of components [109]-[112] or weather-induced random failures [38]). We formulate the problem of resilient control by network operators as sequential, multi-stage deterministic [109]-[112] or stochastic optimization problems [38]. These multi-stage problems are computationally hard to solve. By utilizing the tools in optimization theory and the domain knowledge of power systems, we develop a computational approach to approximately solve these hard problems. Our work contributes to the fields of resilient control, and network and combinatorial optimization.

1.5.1 Attack generation and implementation

In Chapter 2, we introduce a new semantic-aware data injection attack against power grid controllers. The attack leverages an approximate model of power system to manip-

ulate the controller runtime memory such that the execution of the legitimate controller software, using partially corrupted values, drives the physical plant towards unsafe states. We formulate the problem using a game-theoretic framework to optimize the attack strategy in terms of which available data regions in the controller memory space should be modified. The adversary-optimal values are calculated using fast bilevel optimization procedures.

Recall from Sec. 1.3 that we consider a 2-stage attacker-defender game and formulate a mixed-binary bilevel convex optimization problem. In Stage 1, the attacker chooses a strategy to decide which line rating parameters to compromise, and by how much. In Stage 2, the system operator who is unaware of the attack, computes an optimal economic dispatch solution by solving a convex program with assumed compromised line rating parameters. The inner operator problem is a convex problem, which enables us to solve the bilevel problem using a KKT-based single level mixed-binary reformulation.

Finally, we show that implemented working prototypes of the proposed controller attack against real-world large-scale and widely-used energy management systems. Our implementations leverage logical memory invariants to locate the sensitive power system parameters in the controller's memory space. The evaluation results prove the feasibility of domain-specific data corruption attacks to optimize for the physical damage.

1.5.2 Network models

In order to solve the DAD game (Chapter 3), we first consider the sub-game involving Stages 1-2 resulting from fixed operator security strategy in Stage 0. We develop a novel $\epsilon-$linear power flow (LPF) approximation along with the classical LPF approximation which allows us to pose bilevel linear programs. Now, the optimal losses under $\epsilon-$LPF and LPF approximations upper and lower bound the optimal loss under non-linear power flows, respectively. In [110, 111] we show that these results also hold true if we model the deviations in the system frequency.

In Chapter 6, we develop a novel network model for radial DNs consisting of one or more microgrids. This model enables us to capture different microgrid regimes (interconnected vs islanded) as well as the DER operating modes (single-master vs. multi-master)

using a mixed-integer linear network model. This modeling approach enables us to formulate a Bilevel Mixed-Integer Problem (BiMIP). In Chapter 5, we show that (1.1) can be solved using a Benders Decomposition (BD) algorithm. In Chapter 6, we show that the same BD method can be applied to the extended BiMIP formulation for the multi-microgrid radial DN model.

Our network model is also well-suited for formulating a DN restoration problem as a multi-period Mixed-Integer Problem (MIP). In our restoration problem, the network state in any period only depends on the operator response actions in that period, and the network state in the previous period. We exploit this feature and propose a greedy heuristic that seeks to reconnect the disrupted components in each period such that the post-contingency losses for that period are minimized (Chapter 6). We further utilize the same network model to consider DN restoration after storm-induced failures in the 2-SMIP problem (Chapter 7).

1.5.3 Algorithms for resource allocation, response, and recovery

While solving the DAD game, the $\epsilon-$LPF and LPF approximations enable us to characterize for fixed attacker (resp. operator) strategy, the optimal strategy of the operator (resp. attacker). These results lead to a greedy approach, which efficiently computes the optimal attack and defender response. We prove optimality of the greedy approach for DNs with identical resistance-to-reactance ratio, and show that the approach efficiently obtains optimal attack strategy and defender response for a broad range of conditions. We also show that our greedy approach has significantly better computational performance than the standard techniques to solve bilevel optimization problems (e.g., Bender's decomposition [103]).

In the RAOPF problem, we utilize a similar solution approach as described above. We primarily focus on the last two stages and considered the first-stage resource allocation as fixed. For the sake of simplicity, we only consider linear power approximations. Then, we show that our greedy approach can be extended to solve for optimal solutions of Stages 1-2. This approach again enables much faster computation of attack strategy to maximinimize the SO's post-contingency loss. Furthermore, the optimal attacker and operator

strategies in the sub-game only depend on the net active and reactive power flowing into the DN. By implementing a search algorithm (e.g. binary search) over a few values for the net inflow, we can minimize the weighted sum of cost of resource allocation and the post-contingency cost under worst-case scenario.

In Chapters 5 and 6, we further extend the attacker-operator sub-game. In this case, the operator response problems consists of mixed-binary variables for which the greedy heuristic is no longer applicable. The bilevel formulation is a BiMIP. Therefore, we develop a new solution approach which comprises of reformulating the BiMIP into an equivalent Min-cardinality disruption problem. A key feature of our formulation is that the coupling constraints which model the effect of attacker's actions on the operator response consist only of binary variables. As a result, a straightforward application of Benders Decomposition (BD) method does not rendering useful Benders cuts. Hence, we apply the BD method on a BiMIP with reformulated coupling constraints, and show the effectiveness of the modified method.

In Chapter 6, we show that the problem of DN restoration by gradually connecting the disrupted components can be posed as a large-scale MIP, and can be solved using off-the-shelf MIP solvers. However, due to the large number of binary variables, it can become computational expensive to solve for larger networks. Instead, we solve for the restoration actions using a simple greedy algorithm. In each period, the operator simply chooses that response which minimizes the post-contingency loss during that time period subject to the monotonicity and resource constraints. Our computational results, show the effectiveness of this greedy restoration algorithm.

In the 2-SMIP problem (see (1.2)), calculating $\mathbb{E}_{S\sim\mathcal{P}}J((x,y),S)$ is computationally intractable for large networks because the number of all possible scenarios grows exponentially for a network with the number of edges. Using the sample average approximation (SAA) method [4], one can obtain an approximate solution to the stochastic optimization problem. This solution can be obtained by solving the following problem:

$$\min_{a\in\mathcal{A}}\left\{\hat{g}_{\hat{\mathcal{S}}}(a) := {\mathrm{W}_{\text{alloc}}}^{T}a + \frac{1}{K}\sum_{s\in\hat{\mathcal{S}}}J(a,s)\right\}, \tag{1.4}$$

where $\widehat{\mathcal{S}} \subset \mathcal{S}$ is a suitably chosen (preferably small) subset of the set of failure scenarios, $K := |\widehat{\mathcal{S}}|$, and $\hat{g}_{\widehat{\mathcal{S}}}(a)$ is the SAA objective value obtained using K samples drawn from the distribution $\mathcal{P}$. $\widehat{\mathcal{S}}$ is chosen using a scenario reduction method described in [48]. The resulting problem is a large-scale MIP, and we solve using a modified version of the Benders Decomposition method described in [114]; see Chapter 7.

As part of our ongoing work, we are investigating other approaches for solving 2-stage stochastic MIP problems [107, 116]. In [116], a Reformulation-Linearization Technique (RLT) and lift-and-project cuts are used if we restrict variables in the Stage 2 to be binary. This allows the regular BD method to be directly applicable. In [107], it is shown that the scenario-specific Stage 2 problems have similar structure. This characterization is known as Common-Cuts-Coefficients (C^3) Theorem, based on which a Disjunctive Decomposition (D^2) algorithm is developed. This algorithm enables to utilize the Benders cut obtained for one scenario to be modified for other scenarios by using a simple translation. In Chapter 7, we will describe how the results in [107, 116] might be used for solving (1.2). Another approach, which is also part of our ongoing work, is that for a fixed allocation of portable DERs, the problem of optimal restoration strategy in Stage 2 is closely related to optimal scheduling problem of jobs with unit execution times and soft precedence constraints [126]. Our hope is to utilize the insights from scheduling theory to generate fast algorithms to solve for Stage 2 problems, which will ultimately enable improved resource allocation in Stage 1.

In all of the above-described works, full and accurate knowledge of the system parameters is important, which is why we wanted to develop a data-centric method which would enable obtaining these parameters based on sensor measurements. This work is also part of our ongoing research. In Chapter 2, we describe an online learning method to learn the power transmission dynamics. In particular, the goal is to reconstruct the dynamic state matrix of a transmission network using sensor data from Phasor Measurement Units (PMUs) consisting of time-stamped values of the phase angle and the frequency for each bulk generator. This work is motivated by the fact that the accuracy of the assumed system model and its parameters in TNs is very important for a range of nominal applications such as state estimation, generation re-dispatch, detection of forced oscillations,

etc. An accurate system model can also be used to timely detect and identify of a security attack, as well as to determine an optimal operator response to the attack-induced disturbance.

The challenge is to develop a data-efficient learning framework for performing an online reconstruction of the dynamic network model using minimal number of assumptions and exclusively relying on the PMU measurements. Previous work on this problem showed that with just the knowledge of network topology and complete PMU observations, it is possible to reconstruct the dynamic state matrix using a maximum likelihood based approach [82]. However, we show that this approach can also be extended to the case of partial PMU observability, when the PMU data of certain (hidden) nodes is not available. Specifically, if each hidden node is connected to exactly one observable node and each observable node is connected to at most one hidden node, then by exploiting the structure of swing equation model, the entire dynamic matrix can be reconstructed. Our hope is that the results provide insights into optimal sensor placement of the PMUs in the TNs.

In summary, our main algorithmic contributions are: (a) an approach to speed up the computation of attacker-SO strategies (relative to classical MILP approach) by utilizing properties of power flow on radial DNs; (b) insights into optimal resource allocation and DER dispatch when the SO faces tradeoffs in maintaining regulation objectives during contingencies that resulting from simultaneous node compromises; and (c) optimal DN restoration strategies which model joint DER dispatch and network repairing operations.

1.5.4 Practical insights

There are several practical insights which we gain from our resilience assessment of electricity networks. Firstly, the power flows and the radial topology of DNs leads to implications on optimal attacker strategy. In Chapter 3, we show that if the attacker's goal is to cause the loss of voltage regulation, then the attacker's optimal strategy shows a preference to attack downstream nodes in a clustered manner. As a result, the optimal security strategy of the operator would be to secure the upstream nodes in a distributed manner. Finally, we provide a characterization of the optimal security strategy for Stage 1 decision

by the defender, albeit for symmetric DNs.

In Chapter 4, we show that if the attacker's objective is to cause loss of frequency regulation, then the attacker's optimal strategy involves compromise of nodes with larger capacity [110]. This tradeoff between the loss of voltage vs. frequency regulation results in a diversification of optimal operator response. The optimal operator's response is to provide more reactive (resp. active) power as opposed to active (resp. reactive) power from downstream (resp. upstream) DER nodes, to reduce voltage (resp. frequency) regulation. In [111], we show that this knowledge can be used to implement a distributed control strategy that pre-assigns the downstream (resp. upstream) DERs to contribute to voltage (resp. frequency) regulation, and yet performs well in comparison to the centralized control strategy.

Another insight is regarding the allocation of contingency reserves in DERs within the DNs in the RAOPF problem. In Chapter 4, we show that regardless of what DER setpoints are chosen, as long as the net active and reactive power going into the DN remains constant, the optimal attacker strategy and optimal operator response remains the same. This insight can be used to choose the DER setpoints that minimize the cost of resource allocation in the pre-contingency stage (as stated in Sec. 1.5.3).

The greedy restoration algorithm described in Chapter 6 is based on the insight that the network state in any period depends only on the operator actions in that period, and the network state in the previous period. The algorithm returns with the operator actions, resulting network state, and corresponding post-contingency loss for each time period. Our experiments show that the greedy algorithm does produce near-optimal restoration actions.

We refer the reader to Table 1.1 for a summary of our contributions.

The outline of the thesis is as follows. In Chapter 2, we present an end-to-end framework for attack generation and attack implementation on an EMS software to perform vulnerability assessment of the transmission networks under attacks on control center functionalities. In Chapter 5, we develop a resilience assessment framework, and present how the Substation Automation Systems can be leveraged to improve the resilience of distribution networks. In Chapter 6, we extend the framework to assess resilience of dis-

Disruption model	Defense model	Problem formulation	Solution Approach	Results / Insights
Data injection attacks	Hardware-based protection	Bilevel Linear Convex Program	KKT-based MILP	End-to-end attack framework [112]
DER node disruptions	DER response, load control	Bilevel NLP	$\epsilon-$LPF, Greedy heuristic	Downstream preference for attacker [109]
EV node disruptions	DER response, load control	Trilevel LP	$\epsilon-$LPF, Greedy heuristic	Diversification in response and allocation [110]
DER disruptions, TN-side disturbances	DER response, microgrid islanding, load control, component disconnections	Bilevel MIPs	Benders Decomposition	Value of timely response, greedy algorithm for restoration [114, 115]
Stochastic line failures	Portable DER allocation, dispatch in microgrids, line repair scheduling, load control, component disconnections	2-stage stochastic MIP	Benders decomposition	Recursive scheduling algorithm for network restoration [38]

Table 1.1: Summary of contributions.

tribution networks consisting of one or more microgrids. We also develop a novel network model for DNs with one or more microgrids. In Chapter 7, we consider the problem of improving DN resilience to storm-induced component failures. Finally, in Chapter 8, we present a summary of results and a few practical recommendations based on the findings of the thesis.

Chapter 2

Vulnerability Assessment of Transmission Network Control Center

In this chapter, we present a semantics-aware attack against a widely used power grid network control functionality, and demonstrates its practical feasibility on well-known *Energy Management System (EMS)* softwares. Specifically, we conduct a vulnerability assessment of an important functionality provided by all EMSs – the so-called *Economic Dispatch (ED)* problem. In critical infrastructures, ED is routinely solved to set the generator output levels over a control area of a regional transmission grid. We show that software security vulnerabilities in power system controllers can be exploited by an attacker (an external hacker or a strategic market participant) to gain a backdoor entry into power grid operations.[1] By utilizing the knowledge of an approximate power flow model – specifically, DC approximation – the attacker can launch a semantic memory attack to change the critical parameters such as transmission line ratings (capacities). A transmission line's rating reflects the maximum amount of power that it can carry without violating safety codes or damaging the line. We design experiments using ED implementation on real-world EMS software packages to demonstrate the economic and safety risks posed by use of manipulated line ratings.

[1]Throughout the chapter, we use the term *controller* as the ED implementation software packages that solve economic dispatch problem.

2.1 Compromising economic dispatch software

Despite the failures, the past intrusions had two features: *i)* they mostly required full ownership of the target controllers (e.g., Siemens Step7 server compromise by Stuxnet [51]) to perform the attacks; and *ii)* they did not fully optimize their adversarial impact via utilization of the underlying physical model. A semantics-based attack can do a lot more using much less resources. For instance, an attacker with access to only few power system parameters can leverage its dynamical model to calculate the malicious replacing parameter values such that the ultimate damage to the power system is maximized.

In the literature, there has been an extensive body of work on false data injection attacks [80], where the compromised sensors send corrupted measurements to mislead the operators regarding the power system state. Such attacks assume the attacker can compromise a large number of geographically and logically distributed set of sensors remotely. In addition to the scalability barrier, remote malicious access to (analog) sensors with serial connections may not be feasible in practice. Additionally, by design, false data injection attacks target sensors or actuators only, and cannot manipulate core system parameters such as the network topology and line parameters (e.g., capacities). This information often resides within the control center servers and are used for power system operations such as state estimation and operational control. However, almost all the past real attacks (e.g., [13, 51]) against critical infrastructures have targeted control center assets (as opposed to individual sensors or actuators).

The core of our attack generation approach against the power grid infrastructure is a bilevel optimization problem that encodes the attacker's partial knowledge of power system operations to compute the target malicious power system parameters. This physics-aware attack generation approach enables us to identify key features of power system data and software operations whose exposure can significantly increase security risks. The implementation of our optimal attack against power system operation involves targeted manipulation of specific power system parameters that reside within the EMS's dynamic memory space. The exploit performs an online memory data search using lightweight pattern matching to locate the sensitive power system parameters used by the ED soft-

ware to calculate the generation output levels. The use of manipulated parameter values makes the EMS issue incorrect dispatch (generation and power flow) commands, and consequently drive the power system towards unsafe states. The merit of our overall approach lies in the combination of the semantics-based optimal attack generation and a generic implementation procedure for EMS's memory data corruption.

The bilevel problem for attack generation can be viewed as a sequential game between the attacker (leader) and the follower (grid operator). In the first stage, the attacker chooses power system parameter manipulations with the objective of maximizing the violation of capacity limits; in the second stage, the operator solves the ED to determine generator output levels while facing the manipulated parameters chosen by the attacker in the first stage. We show that the optimal power injections and nodal voltages computed using the manipulated parameters yield suboptimal and unsafe power flow allocations. This significantly increases the possibility of cascading failures and the risk of subsequent emergency actions.

Our main contributions in this chapter are as follows:

- We introduce a new domain-specific semantic data attack against power grid controllers. The attack leverages an approximate model of power system to manipulate the controller runtime memory such that the execution of the legitimate controller software, using partially corrupted values, drives the physical plant towards unsafe states.

- We formulate the problem using a game-theoretic framework to optimize the attack strategy in terms of which available data regions in the controller memory space should be modified. The adversary-optimal values are calculated using fast bilevel optimization procedures.

- We implemented working prototypes of the proposed controller attack against real-world large-scale and widely-used energy management systems. Our implementations leverage logical memory invariants to locate the sensitive power system parameters in the controller's memory space. The evaluation results prove the feasibility of domain-specific data corruption attacks to optimize for the physical damage.

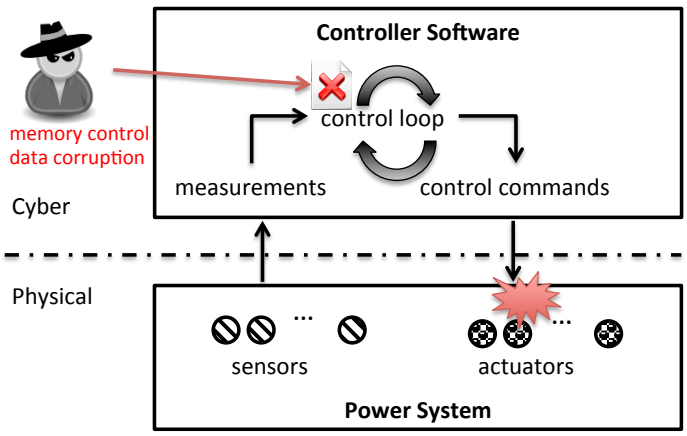


Figure 2-1: Physics-aware memory attack on control systems.

In the remaining of this section, we present an overview of our proposed attack. Sec. 2.2 presents the attack model and optimization algorithm to calculate the parameter manipulations that will maximize the ultimate adversarial impact of resulting power flows. Sec. 2.3 presents our empirical experiments with real-world commercial power grid monitoring and control software solutions. Sec. 2.5 discusses the potential mitigation strategies.

Solution Overview

Our contribution builds on two perspectives that have evolved in the emerging field of cybersecurity of networked control systems. The first perspective involves the analysis of state estimation and control algorithms under a class of attacks to sensor measurements or actuator outputs [104]. These attack models reflect the loss of availability (resp. integrity) of measurements/outputs when the communication network linking the physical system and remote devices is compromised. Recent work has studied how the physical system's performance and stability can be compromised by such attacks [80]. Typically the attacker is assumed to be a resource-constrained adversary with only partial (or possibly full) knowledge of system, and a resilient control design problem is to ensure a reliable and safe performance against arbitrary actions that can be performed by the attacker. These results are grounded in the theory of robust and intrusion tolerant control, which provides a quantitative framework to study the tradeoffs between efficiency in nominal conditions and robustness during non-nominal ones including the attacker-induced failures.

In contrast, as illustrated in Figure 2-1, our attack model considers direct data corruption (specifically, manipulation of power system critical parameters) in the live memory of EMS software, where all distributed sensor measurements are received and processed, i.e., single point of compromise. Hence, individual infections of distributed sensors are not required unlike previous work on false data injection attacks [86]. This allows us to study how the vulnerabilities in control software implementations and in their links to external data sources can be exploited by the attackers.

A second perspective has emerged in the vulnerability assessment of large-scale power grids against physical attacks [23]. Here the objective is to find worst-case disturbance or an *adversary-optimal attack* to physical components that can maximize the impact on grid functionality, even under perfect observability and best response by the operator (defender). Various classes of failures have been considered, for e.g., line failures, sudden loss of generation, and load disconnects. Typically, these problems are formulated as bilevel optimization problems, and involve explicit consideration of both physical constraints (e.g., power flows, generation constraints, and line capability limits) as well as resource constraints of the attacker. Examples of physical security problems that have been considered using this framework include $N-k$ contingency analysis problem [43], network interdiction under line failures, and modeling of cascading failures that originate due to local component failures in one sub-network and progressively propagate to other sub-networks of the grid. However, existing work on adversary-optimal attack does not consider how such an attack can be executed in controller software. In our work, we combine the computation of adversary-optimal attack with analysis of EMS software to execute the attack.

Security threats to optimal power flow

The operator (i.e. Independent System Operator) control software typically solves an ED problem every 10-15 mins, or even more frequently, to schedule the delivery of electricity through the high-voltage transmission lines. The decision variables in the ED problem are the complex voltages at each node ("bus") and power injections at each generator bus. In its basic form, the ED can be stated as an optimization problem which minimizes the

operating costs subject to the power flow constraints on transmission lines, constraints on power injections and voltages at generator buses, and capacity ratings of transmission lines. The generic ED problem is non-convex and NP-hard. Many practical algorithms are available to find a "reasonable" solution (e.g., gradient methods, linear and quadratic programming, Newton's method, interior point methods, etc.). More recently, an approach based on semidefinite programming relaxation has been proposed, which can guarantee either a global optimum or provide a certificate of infeasibility. The ED module is the main implemented component of EMS software to ensure an optimal and reliable power flow.

The ability of ED to serve as a dependable tool for power system operations relies on the inputs including the measurement of the state of power system (e.g., transmission lines capacity, state of circuit breakers). The integrity of these measurements is essential for the operator's ability to direct power generation schedules, route power flows across capacity-constrained transmission networks, and continuously balance the electricity demand of consumers across a large geographical region using least costly generation sources. If the integrity of these power system parameters that ED uses is compromised, the ED problem is bound to produce infeasible or potentially unsafe solutions. For example, the specified generator injections may produce power flows that significantly exceed the line capacity ratings; some market participants may gain market power (and huge economic benefits) by influencing the locational marginal prices, especially in peak demand conditions.

To the best of our knowledge, the existing literature in cybersecurity of control systems does not focus on how fine-grained memory attacks despite existing layout randomization mitigations with an approximate knowledge of power system topology can compromise its safety-critical operation, the flow allocations or influence the market prices. We call such memory attacks that leverage the underlying physical dynamics (i.e., power system mathematical models) to maximize their impact, semantic attacks.

Threat model. Our adversary model is concerned with stealthy memory data corruption of EMS (that typically sits within the control center); thus, we require a compromised controller process within the EMS server. This is a realistic assumption, because it requires lesser privileges compared to the past real incidents such as Stuxnet [51] and BlackEn-

ergy [13] that took complete control of the servers. With the access to EMS dynamic memory, the exploit targets the true memory-resident power system critical parameters, and implements calculated adversary-optimal incorrect values in EMS memory.

We emphasize two aspects of our model: Firstly, our attack generation and implementation approach is *generalizable*. However, to concretely illustrate our approach and to evaluate its feasibility, we assume that the attacker is concerned with generating "optimal" dynamic line ratings (DLRs) to maximize capacity violations. Indeed, other variations of attack generation are possible, for e.g. manipulation of other parameters such as generator/loads/voltage bounds, etc. Secondly, our implementation approach is motivated by server-side attacks to EMS software and emphasizes the *stealthiness* of the attack. Specifically, the in-memory parameter manipulations are still within acceptable limits and hence pass the typical out-of-bound checks for false data injections. Thus, they can remain dormant in controller's memory and can produce the intended consequences (e.g. thermal overloading, or even physical damage) before the last line of defense (i.e., physical fail-safe mechanisms) are triggered. Again, other ways of implementing our attack are possible, for e.g. intercepting network communication and injecting false data.

Implementations. We perform off-line binary analysis to locate the power system parameters in the controller's memory space. We use this information to extract logic-based structural pattern signatures (invariants) about the memory around power system parameter value addresses. The signature predicates are checked during attack-time to identify the real parameters on the victim controller memory space. Such pattern-based search (as opposed to absolute memory address-based search) is required because analysis-time (offline) and attack-time (online) parameter value addresses in memory often differ. This is because of unpredictable execution paths (due to potentially different workloads) across different runs that result in different heap memory allocation function call/return sequences, and hence different allocated memory addresses. Finally, the attack achieves a certain level of stealthiness by ensuring that the incorrect parameters reflect similar general trends as the true ones.

2.2 Attack generation using bilevel programming

In this section, we describe how the attacker generates a semantic attack that utilizes the knowledge of an approximate model of power flow to manipulate the model parameters used by the ED software. We choose DC model as the approximate model known by the attacker, and line capacities as the targeted model parameters.

We show that under our adversary model, the allocation generated by the ED implementation under the manipulated capacity ratings, causes the power flows on the transmission lines to exceed the actual line capacity ratings. Specifically, its implementation on the power system will lead to the violation of safe thermal limits of the lines. This can cause the lines to rapidly deteriorate or degrade, increasing their likelihood of tripping. The sudden disconnection of power lines can cause an outage. It may cause a short circuit between two lines that can ignite a fire. Coming in contact with a line that is live, can also kill people, seriously injure them. Thus, such a semantic attack increases both reliability and safety risks in power system operations to a significant degree.

In our attack model, the attacker chooses the DLR manipulations in a way such that his actions are not obvious to the System Operator (SO). If the effect of the attack is not visible to the SO (for e.g., via line flow measurements or emergency signals), the SO will not invoke generation curtailment and/or line disconnect operations. In fact, under partial network observability, the operator may not be able to implement the necessary preventive actions in a timely manner. As a result, the SO will implement the false ED solution that will violate the line limits.

2.2.1 Attacker knowledge

We first describe the attacker's system knowledge which consists of DC-approximation of the actual nonlinear AC power flow equations. The topology of a transmission network can be described as a connected graph with the set of nodes $\mathcal{N}$ and the set of edges $\mathcal{E}$. In power systems terminology, each node refers to a bus and each edge refers to a transmission line. We let $n = |\mathcal{N}|$. Let $\{i, j\}$ denote the line joining the nodes i and j, and its susceptance (inverse of reactance) be denoted as β_{ij}. The set of generators at a bus i is

denoted as $\mathcal{G}_i$. The set of all generators is denoted by $\mathcal{G} := \mathcal{G}_i$. For each $i \in \mathcal{G}$, p_i^{min} and p_i^{max} are the lower and upper generation bounds that are specific to the $i-$th generator. The generation bounds can be expressed as constraints on individual p_i:

$$p_i^{min} \leqslant p_i \leqslant p_i^{max}. \tag{2.1}$$

Following the standard formulation of economic dispatch, the cost of power generation for the $i-$th generator is modeled as a convex quadratic function $C_i(p_i)$ in p_i. Let $p \in \mathbb{R}^{\mathcal{G}}$ and $d \in \mathbb{R}^{\mathcal{N}}$ denote the generation and demand vectors, respectively. The total cost of generating p is:

$$C(p) = \sum_{i \in \mathcal{G}} C_i(p_i), \tag{2.2}$$

where

$$C_i(p_i) = a_i {p_i}^2 + b_i p_i + c_i. \tag{2.3}$$

$a_i, b_i, c_i \in \mathbb{R}_+ \; \forall \; i \in \mathcal{G}$. a_i and b_i are not simultaneously zero, i.e., the cost of generation is an increasing function of power (MWs) supplied.

The power flow f_{ij} from node i to node j can be expressed as a linear function of the difference between the voltage phase angles at nodes i and j [23]:

$$f_{ij} = \beta_{ij}(\theta_i - \theta_j), \tag{2.4}$$

where $\theta \in \mathbb{R}^{\mathcal{N}}$ is the vector of voltage phase angles.

The conservation law for the power flows is:

$$\sum_{j:\{i,j\} \in \mathcal{E}} f_{ij} = \sum_{k \in \mathcal{G}_i} p_k - d_i, \tag{2.5}$$

which states that the net generation at a node i is equal to the sum of outflows from node i to its neighbors. The DC power flow (2.4)-(2.5) is said to be feasible if and only if total

supply is equal to total demand (see [23]), i.e.,

$$\sum_{i \in \mathcal{G}} p_i - \sum_{j \in \mathcal{N}} d_j = 0. \tag{2.6}$$

The power flows satisfy the capacity line constraints, i.e.,

$$|f_{ij}| \leqslant u_{ij}. \tag{2.7}$$

Thus the DC-optimal power flow problem faced by the SO can be posed as follows:

$$\min_{p,\theta} \quad C(p) \qquad \text{s.t. } (2.1) - (2.6), (2.7). \tag{2.8}$$

2.2.2 Attacker resources

The true capacities of the transmission lines dynamically vary over time due to weather conditions (ambient temperature, wind, etc.) [45], and are, in fact, greater than the static line ratings assumed by the SO for economic dispatch problem (Figure 2-2). Dynamic Line Rating (DLR) lines are the transmission lines with DLR sensors that report the true line capacities to the system operator.

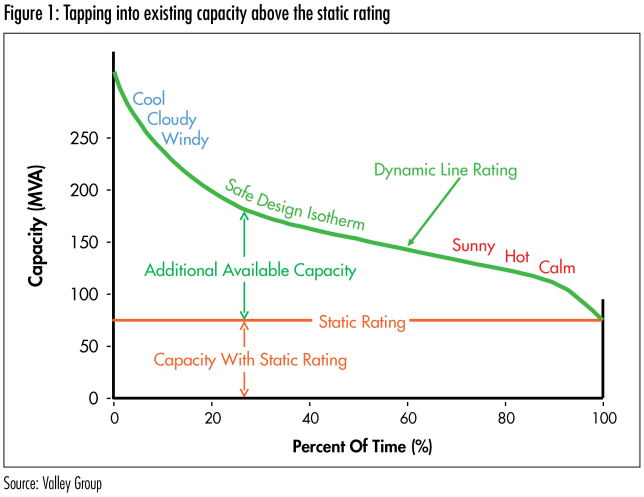


Figure 2-2: Static vs Dynamic Line Rating

Let $\mathcal{E}_D \subset \mathcal{E}$ denote the set of lines that are equipped with DLR devices. The complementary set $\mathcal{E}_S = \mathcal{E} \backslash \mathcal{E}_D$ denotes the set of lines that are not equipped with DLR

technology, and hence their rating will be fixed to the respective static line capacity values. Given that DLR deployments are done as part of government sponsored smart grid projects [44, 45], the set of lines $\mathcal{E}_D$ equipped with DLR technology is public knowledge. These lines will be the ones that are routinely prone to congestion and hence receive priority DLR implementation by the operator.

For a line $\{i,j\} \in \mathcal{E}_D$, we denote u_{ij}^d as the actual line rating computed by the DLR software using measurements collected from the Supervisory Control and Data Acquisition (SCADA) system.

$$u_{ij} = \begin{cases} u_{ij}^s & \text{if } \{i,j\} \in \mathcal{E}_S \\ u_{ij}^d & \text{if } \{i,j\} \in \mathcal{E}_D, \end{cases} \tag{2.9}$$

where

$$\forall\ \{i,j\} \in \mathcal{E}_D \quad u_{ij}^{min} \leqslant u_{ij}^d \leqslant u_{ij}^{max} \tag{2.10}$$

i.e. the DLRs can only take values between a certain range.

Thus the DC-optimal power flow problem faced by the SO can be posed as follows:

$$\min_{p,\theta} \quad C(p) \qquad \text{s.t. } (2.1) - (2.6), (2.7), (2.9). \tag{2.11}$$

We assume an *informed attacker*. Specifically, the attacker's knowledge includes the network topology, line susceptances, set of generators, and their corresponding generation limits, and the cost of generation. The attacker also knows the nominal demand d_j at each node j and the nominal generator output p_i for each $i \in \mathcal{G}$. In power systems terminology, with this knowledge, the attacker can solve for an DC ED solution which is an approximation of AC ED solution that the EMS implements on the power system. Note that our assumption on attacker's knowledge is not unrealistic given that all major ISOs publicly disclose historical generation and demand patterns and the locational marginal prices in day ahead and hourly power markets.

Since the SO knows the static line ratings and these are fixed in ED software implementations, we assume that the attacker cannot compromise them in ED implementation's memory. Any compromise to static line ratings can be overridden by simple built-in

checks in power flow implementations. Also, since the static ratings are typically calculated for constant (worst-case) weather conditions over an extended period of time (few months to years), we assume that the attacker knows their values. This assumption can be justified by the fact that the manufacturers of transmission line conductors supply static line ratings in their product specifications. Thus, under the aforementioned constraints, the set of lines $\mathcal{E}_D$ constitutes the attacker's constraint since the attacker only targets DLR ratings and not the static ones.

2.2.3 Attacker objective

Now, we present the constraints faced by the attacker so that the attack remains stealthy, and the SO's ED software admits the DLR ratings manipulated by the attacker. Then, we formulate the attack policy of the attacker as a bilevel optimization problem.

Under our attack model, the attacker accesses the actual DLR values u_{ij}^d for lines $\{i,j\} \in \mathcal{E}_D$ in ED's dynamic memory and replaces them with incorrect values u_{ij}^a. The attacker knows u_{ij}^d and computes u_{ij}^a in order to maximize the violation of line ratings by the resulting power flows. To avoid detection by in-built checks, each u_{ij}^a is constrained by minimum and maximum permissible limits of line ratings, denoted as u_{ij}^{min} and u_{ij}^{max}, respectively. These limits are also known by the attacker. For ease of presentation, we introduce an auxiliary variable $\widehat{u}_{ij}$ to denote the manipulated dynamic line rating for the line $\{i,j\} \in \mathcal{E}_D$. The attacker is subject to following constraints:

$$\forall \{i,j\} \in \mathcal{E}_D \quad \begin{cases} \widehat{u}_{ij} = u_{ij}^a \\ u_{ij}^{min} \leqslant \widehat{u}_{ij} \leqslant u_{ij}^{max}, \end{cases} \tag{2.12}$$

because, the attacker wants to maintain a level of stealthiness, so he does not choose an out-of-bound DLR value, that may set off an alarm.

If the DLR value of a line $\{i,j\} \in \mathcal{E}_D$ is manipulated by the attacker, then the EMS software will obey the following constraint for the power flow on the line:

$$\forall \{i,j\} \in \mathcal{E} \quad |f_{ij}| \leqslant \widehat{u}_{ij}. \tag{2.13}$$

We pose the problem of optimal attack generation – from the attacker's viewpoint – as the following bilevel optimization problem:

$$\max_{u^a} \quad U_{cap}(f; u^d) = \max_{\{i,j\}\in\mathcal{E}_D} 100 \left(\frac{|f_{ij}|}{u^d_{ij}} - 1 \right)_+ \tag{2.14a}$$

$$\min_{p,\theta} \quad C(p) \quad \text{s.t. } (2.1) - (2.6), (2.12), (2.13), \tag{2.14b}$$

where $a_+ := \max(a, 0)$. This problem is equivalent to a 2-stage sequential (Stackelberg) game, in which the attacker (leader) chooses his strategy assuming a best response from the defender (follower). Specifically, in the first stage, the attacker chooses the incorrect DLR ratings u^a (or equivalently $\widehat{u}_{ij}$) that are subsequently implemented in runtime by localizing and corrupting true DLR values in the nonlinear ED controller's memory. The attacker's objective is to maximize the maximum percentage capacity bound violation of the power flows f_{ij} on lines $\{i, j\} \in \mathcal{E}_D$ over the true DLR values u^d_{ij} after the defender responds optimally in the second stage. This objective can be expressed as $U_{cap}(f; u^d)$ in (2.14a). In the second stage, the defender chooses the generator outputs p and voltage phase angles θ that achieves min-cost solution to DC-ED, i.e., minimize the generation costs (2.2) subject to the constraints (2.1)-(2.6),(2.12),(2.13). The attacker ensures that under the manipulated DLR ratings $\widehat{u}_{ij}$ for lines $\{i, j\} \in \mathcal{E}_D$ and given static ratings u^s_{ij} for lines $\{i, j\} \in \mathcal{E}_S$, there exists a feasible flow allocation that minimizes the generation cost (2.2), otherwise the SO will be require to setting off an alarm causing the SO to initiate other actions such as load curtailment.

Note that the actual generation cost faced by the operator when incorrect u^a are used in the SO's nonlinear ED formulation will be different than the defender cost obtained in the stage 2 subgame. In fact, the nonlinear ED is likely to be infeasible in the sense that the power flows on certain lines can exceed the permissible line ratings.

The attack model can be summarized as follows. The physical system consists of the physical components, e.g., generators, transmission network, and the loads. Each of these components send data to the EMS via means of SCADA, which is part of the attacker knowledge. The generators submit the cost functions, the transmission network submits

the topology and the line ratings, and the loads submit the demand. The attacker uses this data to compute a DLR manipulation based on his attack policy, and then compromises the DLR values utilized by the EMS while solving the ED problem. Finally, the EMS implements the false ED solution by dispatching the new generation set-points to the individual generators.

Next, we present our computational approach to compute the optimal maximin attack.

2.3 Attack implementation on control center software

We implemented our proposed attack in real controller software packages. Figure 2-3 shows the stages of the implemented attack. Initially, we assume a controller executable file (vulnerable point) and sensitive data sources (e.g., inputs such as DLRs originating from an external source) are given. Next, through memory taint analysis, we narrow down our search space to identify the the memory regions where the sensitive parameters may reside in memory during the controller execution. Accordingly, all the memory regions affected by the target input are marked (tainted). The tainted areas are then searched for the values of interest (e.g., target DLRs), and candidates are shortlisted. To identify the correct candidate from the set of candidates, we generate structural memory pattern signatures around the correct candidates during the offline binary analysis phase. We use our past work [122] to extract binary-level data type and code, and data pointers and their interdependencies (discussed below). Given the reverse engineered logical memory layout, we create structural patterns of the memory regarding where the target parameters reside. Those patterns are then used to generate the exploit binary. During the attack phase the exploit searches the dynamic memory address space to locate the target parameters using the patterns. Finally, it changes the identified parameter values to the optimal attack values, as discussed in Sec. 2.2.

Every control algorithm implementation by controller software executables involve code and data. The code instructions encode the algorithm logic (e.g., iterative optimization loops), whereas the data stores the controller parameters such as the OPF constraints and DLRs. Modification of the code instructions are often infeasible due to $W \oplus X$ protections. However, the data regions should be (and are set as) writable, because the EMS

operators often update their values dynamically according to the most recent power system configuration.

Maintenance of control-sensitive variable values such as DLRs by the controller software provides an attack surface to modify them in memory space during the attack. Our investigations of EMS software binaries showed heavy use of data structures and class objects to store those values that are used directly by OPF. During the offline phase, we analyzed the EMS software binary to determine its memory's structural layout. We are interested in structural information such as the allocated class instances (objects), the class hierarchy, and the logical interdependencies between the instantiated objects within the memory, e.g., cross-object code and data pointers. We are not interested in exact object memory addresses, because the addresses will likely differ during the attack due to unpredictable (inputs and hence) dynamic execution paths. Instead, by capturing the logical interconnections among the instantiated memory-resident objects, we extracted invariants about their interdependencies that remain the same across different runs. The attacker later uses the invariants during the attack to locate (and corrupt) the DLR values.

Search for a specific DLR value during the attack results in several memory-resident candidates that are mostly (except one) false positives. To identify the correct candidate, our implementation uses the invariants, expressed as propositional logic predicates, that capture the logical memory structural patterns around the target DLR parameters. We use three kinds of memory patterns: address-relative intra-class type patterns, code pointer-instruction patterns, and data pointer-based patterns (Table 2.1).

Address-relative intra-class type patterns. The attack extracts execution-agnostic memory structural patterns around the target DLR values in memory. We concentrate on intra-class patterns that capture fixed offset relations among members of the same class as the target DLR parameter, and their types and/or values. If the DLR parameter is stored as a member of a class that also contains other variable(s), whose type is (are) easy to identify, we use that information as a local signature for the target parameter. In memory forensics, types such as character strings, pointers [78], and fixed-value member fields can be identified simply. We investigate the vicinity of the target parameter within the same object looking for addresses that store easy-to-identify data types. If one or

more of such samples are found, their type/value and corresponding offset from the target parameter address is used to produce the signature. The attack creates simple-to-check logical predicates for each candidate (e.g., "candidate_addr + $0x08$ stores $0x00000001$"). Our implementation aggregates the produced predicates into a single conjunctive logic signature.

Code pointer-instruction patterns. We leverage the code pointer relations within the memory regions to extract invariants (logical predicates) about the structural memory layout around the target DLR parameters. We extract such invariants given the reverse engineered class object pointers, and their logical interdependencies with the corresponding member and virtual functions. We use the fact that code segments (e.g., instructions of member and virtual functions) within the controller software binary are typically set as read-only with fixed content. Table 2.1 shows a sample code pointer-based predicate for the illustrated pattern. The signature checks whether the first four byte content of the target parameter's object's second virtual function is equal to the corresponding function prologue. As denoted, the signature does not depend on the absolute address values given the target parameter candidate's location. The attack can automatically generate the code pointer patterns for the object's individual member and virtual functions. Finally, the generated predicates are combined into a single conjunctive logical predicate to check against all the identified candidates within the EMS memory space attack time.

Data pointer-based patterns. The data pointer-based patterns do not often assume fixed data values in memory, and is purely based on memory structure and the relations between various objects. We perform a recursive pointer traversal among the recognized objects on the controller's memory space following its earlier forensics analyses of the allocated objects and the stored pointer values within them (member fields). The algorithm implements a depth-first search starting from individual recognized pointers within the memory space. For each pointer under the consideration, we determine if its destination is an memory-resident object. If so, the attack recursively traverses all the member pointer fields within the destination object. During its recursive search, our implementation generates the corresponding directed graph, where nodes represent allocated objects, and the outgoing edges indicate the member pointer fields within the source object. The generated

directed graph represents the inter-object dependencies within the memory space. Once the generation of the graph in completed, our implementation searches for cycles. Such cycles are very popular in widely used data structures such as linked lists (the rightmost entry on Table 2.1). The attack turns each cycle within the graph into a logical predicate that corresponds to a data pointer-based signature.

2.4 Empirical attack deployment results

To assess the proposed attack feasibility in practice, we implemented it against widely-used commercial and open-source industrial controller software packages. The implemented attack involves the following steps: *i)* during the offline phase, we reverse engineer the EMS software binary to locate DLR parameters within the controller and create the corresponding invariants that hold true regardless of their absolute memory addresses; *ii)* during the online phase (attack time), the exploit searches the controller memory for the known legitimate DLR values and collects the candidates; *iii)* the attack recognizes the only true candidate by applying the invariants on the collected set of candidates; and *iv)* our implementation modifies the value maliciously according to the optimal attack generation algorithms discussed in the previous section. We now explain the results for our empirical validation.

Reconnaissance of control center software

We validated the proposed attack on real-world widely-used industrial controller software packages. We first present the detailed results on PowerWorld, and later compare the attack's performance for other controllers (NEPLAN, PowerFactory, PowerTools, and SmartGridToolbox).

Figure 2-4a shows a generated code pointer-based memory signature in PowerWorld. The corresponding pattern predicate for runtime memory search was "*(*(candidate_addr - 0x54) - 0x24) == 0x5356578B", where 0x5356578B is the hex representation of the sub_1375A8C function's first four instruction bytes. The rating of every transmission line is stored in offset 0x24 of the corresponding TTRLine object. The information about the transmission lines of the power system is stored as a doubly linked list

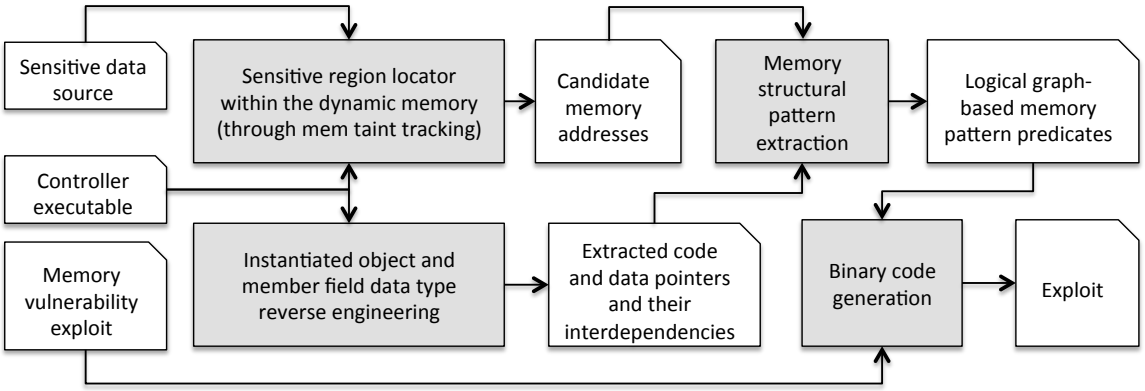


Figure 2-3: Flowchart for attack implementation.

Intra-Class Pattern (type)	Code Pointer Pattern (content)	Data Pointer Pattern (relation)

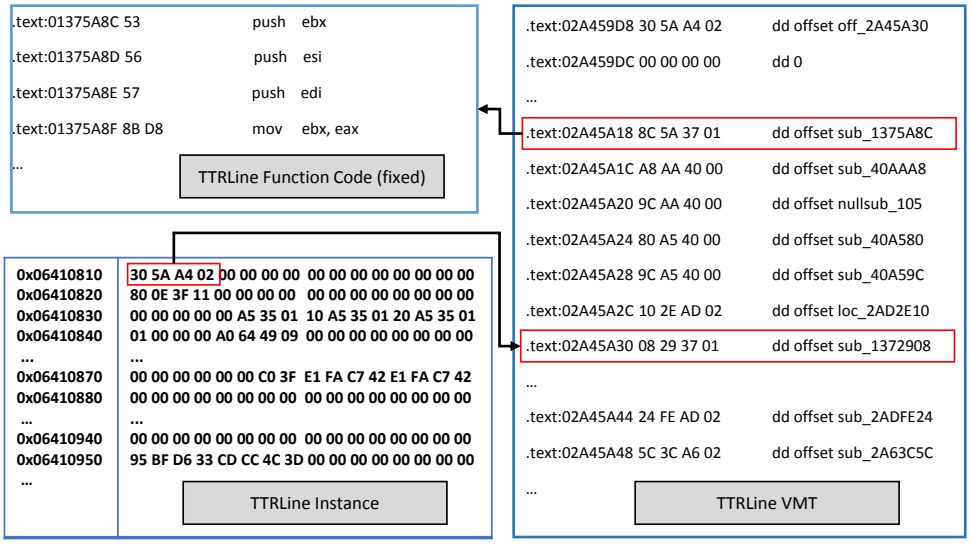
class A size(20):
+---
0 | {vfptr} // virtual fn table*
4 | line-rating // target parameter
8 | mem-var2
12 | mem-var3
16 | line-name // char* string
+---
12 bytes
	class B size(8):
	+---
	0 | {vfptr} // virtual fn table*
	4 | line-rating // target parameter
	+---
	B's vftable:
	0 | &A::A_virt1
	4 | &A::A_virt2
	53 | push ebx
	56 | push esi
	8B F2 | mov esi, edx
		class C size(16):
		0 | {vfptr}
		4 | linked_list_prev // previous node
		8 | linked_list_next // next node
		12 | lr // target parameter
		class C size(16):
		0 | {vfptr}
		4 | linked_list_prev // previous node
		8 | linked_list_next // next node
		12 | lr // target parameter

type(&line-rating + 0x0C) == string	*(*(&line-rating-0x04)+0x04) == 0x53568BF2	*(*(&lr - 0x08) + 0x04) == (&lr - 0x10)

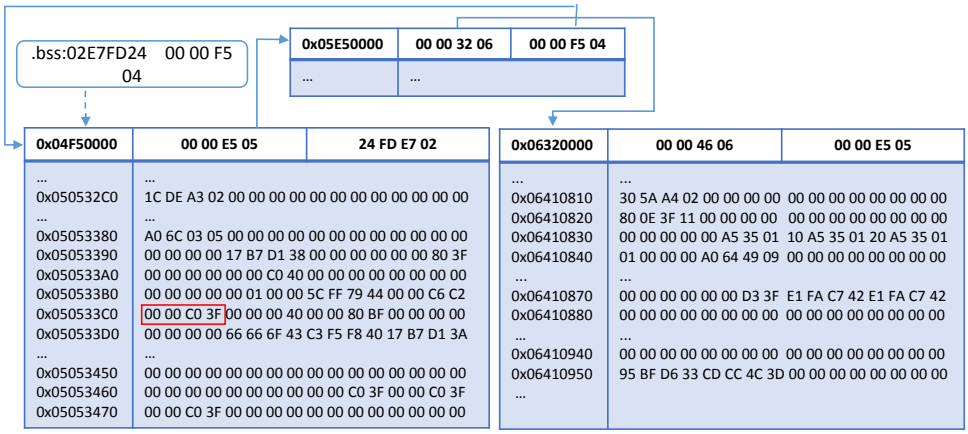
Table 2.1: Logical memory structure signatures for critical parameters.

Table 2.2: The target parameter value recognition accuracy.

Param. values	#Hits	#Relevant	#Recognized	Accuracy
0x3FC00000	143	3	3	100%
0x02A45A30	2038	4	4	100%
0x06410570	30	1	1	100%
0x06410810	30	1	1	100%
0x06410810	28	1	1	100%



(a) Code pointer-instruction pattern.



(b) Linked-list as data pointer-based pattern.

Figure 2-4: Code and data pointer-based structural memory patterns in PowerWorld used for graphical predicate generation.

of TTRLine objects in PowerWorld memory space. The attack used "*(*(candidate_addr - 0x24) + 0x04) == (candidate_addr - 0x24)" as the pattern predicate for line ratings. Let us call the linked list node that stores the target line rating A. The pattern predicate above essentially verifies the following linked list invariant: whether A's previous node's next pointer points to A. More complex patterns can be extracted if needed; however, our empirical studies on PowerWorld shows simple patterns always suffice to identify and isolate the exact candidate uniquely.

Figure 2-4b shows another PowerWorld data pointer pattern for line ratings. PowerWorld allocates linked list nodes (0x13FFF0 sizes each) allocated by VirtualAlloc for objects instances of different classes (e.g., TGen, TBus and TTRLine). Only three nodes are shown. If our objective is to look for line rating 0x3FC00000, its corresponding pattern predicate will encode the offset to get the node's initial member value 0x05E50000 that points to the next node shown (summarized) on the top of the figure. The second element of each node (0x04F50000 in the top node) points to the previous node. A relatively more complex second-degree predicate would be "*(*(*(*(candidate_addr - 0x1033C0)) + 0x04)+ 0x04) == candidate_addr - 0x1033C0", i.e., $A \rightarrow next \rightarrow next \rightarrow previous \rightarrow previous == A$, where A represents the data structure that stores the line rating 0x3FC00000.

The attack payload checks for patterns on the identified candidates before corrupting their values. The code searches for the specific value in memory, and modifies the identified candidate. Table 2.2 shows how many hits our implementation finds for individual target power system parameter values on PowerWorld memory space. The number empirically proves the infeasibility of memory corruption attacks without the use of signature predicates. The next column shows how well the signatures dismiss the irrelevant candidates and identify the true target values. Table 2.3 shows the forensics analysis accuracy for five different EMS software packages. Through the use of the code pointer signatures and its extracted knowledge about the class hierarchies, our implementation was able to correctly recognize the class types of all object instances within the EMS memory. The payload initializes the OPF algorithm in its corresponding thread. Once it changes the identified memory addresses, it restarts the control loop through the call to Cre-

Table 2.3: Memory layout (object) forensics accuracy. The instances were correctly marked with their types.

EMS Software	vfTable	Line	Bus	Gen.	Accuracy
PowerWorld	8527	3	3	2	100%
NEPLAN	6549	51	30	5	100%
PowerFactory	110	34	39	10	100%
Powertools	3	185	118	53	100%
SmartGridToolbox	194	79	57	4	100%

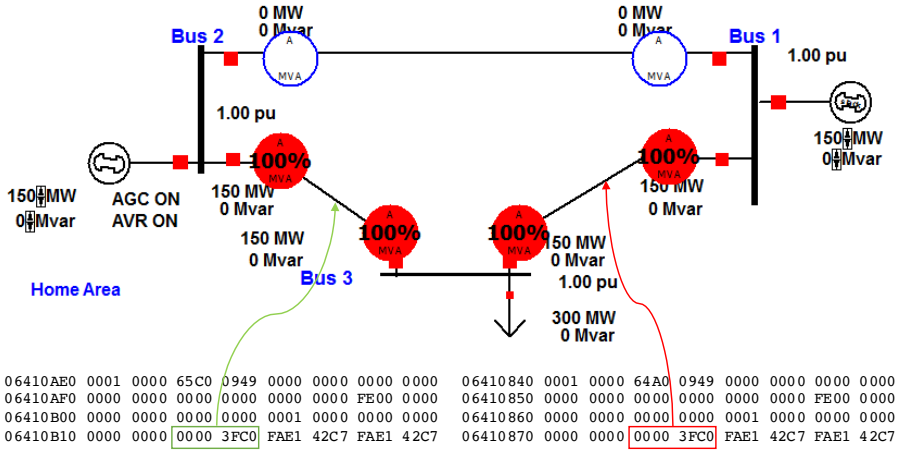
ateThread function within kernel32.dll that is loaded by almost all windows processes.

Attack demonstration

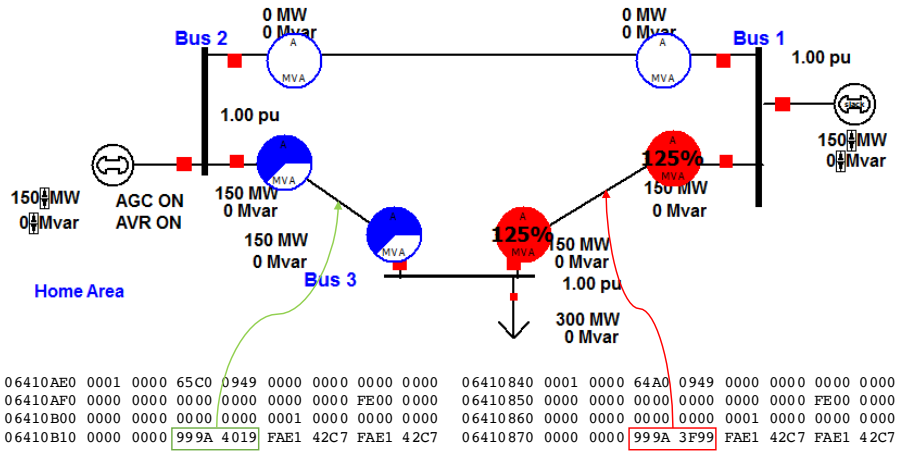
As a concrete example, we show how the state of underlying power system gets affected once the memory corruption is completed (Figure 2-5[2]). Before the corruption (Figure 2-5a), the EMS GUI visualizes the safe state of power system operation, where the transmission lines are mostly fully utilized; however, no line rating (capacity constraints) are violated. The optimal attack generation algorithm computes the adversary-optimal values for the line ratings, and chooses to *i)* modify the $B1 - B3$ transmission line to $120MW$ from $150MW$; and *ii)* modify the line rating for the $B2-B3$ transmission line to $240MW$ from $150MW$. While implementing the optimal attacker strategies that we obtain from the maximin solution, we need to translate the line rating values to higher values using basic power flow calculations. For example, for the implementation of optimal attack, we use $\widehat{u}_{13} = 120\ MVA$ and $\widehat{u}_{23} = 240\ MVA$. These values are higher than the values $\widehat{u}_{13} = 100$ and $\widehat{u}_{23} = 200$ calculated by the bilevel optimization.

This increase in optimal line rating manipulations is necessary to account for the fact that the AC OPF implementation is constrained by the line rating bounds on apparent power flows (with both real and reactive power components) while the optimal attack generation procedure calculates manipulated line rating assuming that only real power flows are subject to line ratings. As the consequence, the power system enters an unsafe state after the OPF control algorithm uses the corrupted line ratings and hence produces

[2]The pie charts on the transmission lines represent the used percentages of the line power flow capacities in that particular state.



(a) PowerWorld pre-attack power system state (safe).



(b) PowerWorld post-attack power system state (unsafe).

fbus	tbus	r	x	b	rateA	rateB	rateC	ratio	angle	status	angmin	angmax
1	3	0.0	0.05	0.0	150.0	9999.0	9999.0	0.0	0.0	1	-30.0	30.0
1	2	0.0	0.05	0.0	150.0	9999.0	9999.0	0.0	0.0	1	-30.0	30.0
2	3	0.0	0.05	0.0	150.0	9999.0	9999.0	0.0	0.0	1	-30.0	30.0

016B2AE0 0001 0000 0000 0000 2AC8 016B 0000 0000
016B2AF0 0000 0000 0000 3FF8 0000 0000 0000 0000
016B2B00 0000 0000 0000 3FF0 0000 0000 0000 0000
016B2B10 0000 0000 0000 0000 999A 9999 9999 3FA9
016B2B20 0000 0000 0000 0000 FFFF FFFF FFFF C033
016B2B30 0000 0000 0000 3FF0 0000 0000 0000 0000
016C0500 0003 0000 0000 0000 95B8 016B 0000 0000
016C0510 0000 0000 0000 3FF8 0000 0000 0000 0000
016C0520 0000 0000 0000 3FF0 0000 0000 0000 0000
016C0530 0000 0000 0000 0000 999A 9999 9999 3FA9
016C0540 0000 0000 0000 0000 FFFF FFFF FFFF C033
016C0550 0000 0000 0000 3FF0 0000 0000 0000 0000

(c) Powertools memory image of the sensitive parameters.

Figure 2-5: PowerWorld and Powertools controller software attack results as the result of targeted adversary-optimal line rating manipulation.

wrong control outputs to the power generators; see Figure 2-5b. Optimal and physics-aware corruption of the sensitive values through a controller attack allows the intruders to maximize the physical impact on the power system operations without having to compromise a large number of sensors as required in false data injection attacks. We also performed the same memory data corruption attack on Powertools [66] package. In this scenario, the attacker changed the line rating for two of the branches as shown in Figure 2-5c. Similar to the PowerWorld case, the exploit locates the sensitive parameters (line ratings) and modifies them during the program execution. As the result, the memory corruption impacted the power flow iterations of DC-OPF performed by the Powertools software that consumed the modified memory regions, and made it converge to a different wrong value. In terms of the attack implementation approach, the attacks against PowerWorld and powertools were identical.

2.5 Cyber-security implications

Our attack and similar domain-specific memory data corruption attacks can be mitigated through several potential solutions: *i)* Protection of sensitive data: fine-grained data isolation mechanisms such as hardware supported Intel SGX can be leveraged to store and process sensitive data such as power system parameters within protection enclave regions. This protects sensitive data against access requests by other irrelevant instructions in the same memory space. A more fine-grained version of such memory-based data protection can distinguish between data that are often fixed during the operation (e.g., power system topological information) vs. regularly updated data regions (e.g., sensor measurements) to facilitate lower-overhead protection such as read-only memory pages for the fixed data once they are loaded on memory initially. *ii)* Control command verification: controller output verification mechanisms such as an extended version of TSV [88] can be used to ensure the safety of the (maliciously) issued control commands by an infected control system software before they are allowed to reach the actuators. Monitoring of the control channel, however, does not ensure the correct functionality of the control system software. Instead it just ensures its outputs (even though corrupted) are within the safety margins of the physical plant. *iii)* Intrusion-tolerant replication: a more tradi-

tional approach is to use redundancy such as N-version programming by maintaining a redundant controller software that is different from the main one used. The replica controller can monitor the dynamic behavior of the physical plant (e.g., power system) as well as the main controller's output to the actuators. The replica can rerun the control algorithm to calculate and compare its calculated control outputs with those of the main controller. Hence, the main controller infection (misbehavior) can be identified if a mismatch is detected; *iv)* Algorithmic redundancy: Carefully designed algorithmic tools (e.g., attack-aware optimal dispatch) can provide safe operating regimes to limit the impact of successful attacks. Indeed, this is a topic of future research.

2.6 Online learning of transmission network dynamics

So far, we assumed that both the operator and the attacker had knowledge about the transmission network parameters. However, changing weather conditions as well as operator actions overall affect the network parameters such as line susceptances, net nodal generation inertia, damping coefficients etc. As a result, the attacker and even the operator may not have exact knowledge about such parameters. This information is necessary for operator tasks such as accurate state estimation, and determining optimal operator response. Also, the attacker may able to use this information for generating optimal attacks. Thus, a key question arises: *How can either player could go about achieving this information?* In this section, we describe an approach based online learning from sensor measurements.[3] First, we describe the approach used in [82] in which they assume that each network node has a Phasor Measurement Unit (PMU). PMUs are the state-of-the-art technology that enable real-time monitoring of the TN. Then, we describe the conditions under which the approach in [82] could be extended to the case when a subset of nodes do not have PMUs.

In [82], an online method to learn the dynamic state matrix using time-stamped PMU sensor data is described. First, a classical reduction is applied to the TN to obtain a network of aggregated generators, in which passive loads are eliminated by Kron reduction [47]. Second, a linear phase dynamical model is assumed in which a node $i \in \mathcal{N}$ of the network is characterized by its generator angle θ_i, non-zero inertia M_i, and damping coefficient D_i.

[3] This is joint work with Andrey Lokhov, Sidhant Misra, Marc Vuffray, and Nathan Lemons.

The temporal evolution of the networks is obtained using the standard swing equations:

$$M_i\ddot{\theta} + D_i(\dot{\theta} - \omega^0) = P_i^{(m)} - P_i^{(e)}, \tag{2.15}$$

where ω^0 denotes the synchronous frequency (60 Hz in the U.S.); $\dot{\theta}_i(\frac{\partial\theta_i}{\partial t})$ and $\dot{\theta}_i(\frac{\partial^2\theta_i}{\partial t^2})$ denote the angular speed and the rate of change of angular speed; $P_i^{(m)}$ is the net mechanical power input; and $P_i^{(e)}$ is the net electrical output.

The line flows are related to the net electrical output as follows:

$$P_i^{(e)} = \sum_{(i,j)j\in\mathcal{E}} f_{ij}, \tag{2.16}$$

where f_{ij} is approximated using DC power flows as $f_{ij} = \beta_{ij}(\theta_i - \theta_j)$. The resultant dynamical model based on the DC linearization is expressed as follows:

$$M_i\ddot{\theta} + D_i(\dot{\theta} - \omega^0) = -\sum_{(i,j)j\in\mathcal{E}} f_{ij} + \delta P_i, \tag{2.17}$$

where $\delta P_i = P_i^{(m)} - P_i^{(e)}$ represents the exogenous power deviations at the nodes, $\dot{\omega}$ denotes the relative generator rotor speed with respect to the standard synchronous speed $\omega^{(0)}$. Thus, the dynamical system for the whole system is written as:

$$\begin{bmatrix} \dot{\delta}_t \\ \dot{\omega}_t \end{bmatrix} = \begin{bmatrix} \mathbf{0}_{N\times N} & \mathbf{1}_{N\times N} \\ -M^{-1}L & -M^{-1}D \end{bmatrix} \begin{bmatrix} \delta_t \\ \omega_t \end{bmatrix} + \begin{bmatrix} \mathbf{0}_N \\ M^{-1}\delta P \end{bmatrix}, \tag{2.18}$$

where $\mathbf{0}_N$ denotes a N-length vector of all zeros, and $\mathbf{1}_{N\times N}$ denotes an identity matrix of size N. L is a susceptance-weighted Laplacian matrix defined as $L_{ij} = \beta_{ij}$ for $(i,j) \in \mathcal{E}$, $L_{ii} = \sum_{(i,k)\in\mathcal{E}} \beta_{ik}$, and $L_{ij} = 0$ otherwise. M and D represent the diagonal matrices with diagonal entries being M_i and D_i. This system can be compactly written as:

$$\dot{X}_t = A_d X_t + \xi_t. \tag{2.19}$$

It is assumed that the PMU sensor measurements (voltage angles) are accurate, which is

why we can write $\xi_t = \begin{bmatrix} \mathbf{0}_N \\ v_t \end{bmatrix}$.

Third, by applying Euler-Maruyama discretization to (2.19), one gets:

$$X_{t+1} = AX_t + B\xi_t, \tag{2.20}$$

where $A = (A_d \Delta t + \mathbf{1}_{2N\times 2N})$, $\xi_t \sim \text{Normal}(0, \mathbf{1}_{2N\times 2N})$, and B denotes the scale of fluctuations of ξ_t. Since it is a reasonable to assume that the deviations in net power consumption are spatially independent across the nodes, B is diagonal. Thus, $B_{ii} = M_i^{-1}\sigma_{P_i}\sqrt{\Delta t}\ \forall i \in [N+1, 2N]$ and $B_{ii} = 0\ \forall i \in [1, N]$.

Fourth, the maximum likelihood estimators for matrix A are derived. Suppose there are T discrete observations of the system $\{X_t\}_{t=1,\cdots,T}$, the cross-correlation matrices with and without displacement are:

$$\Sigma_1 = \frac{1}{T-1}\sum_{t=1}^{T-1} X_{t+1}{X_t}^\top \tag{2.21}$$

$$\Sigma_0 = \frac{1}{T-1}\sum_{t=1}^{T-1} X_t{X_t}^\top \tag{2.22}$$

Finally, the maximum-likelihood estimator for the dynamic matrix is obtained as follows:

$$\widehat{A} = \Sigma_1\Sigma_0^{-1} \tag{2.23}$$

Now, we describe how this approach maybe extended to the case of partial observability under certain restrictions. Our goal is to use the structural properties of the swing equations which may allow us to reconstruct the dynamic matrix even under partial observability.

First, we revisit the dynamical equations for the entire system:

$$\begin{bmatrix} \dot{\delta}_t \\ \dot{\omega}_t \end{bmatrix} = \begin{bmatrix} \mathbf{0}_{N\times N} & \mathbf{1}_{N\times N} \\ -M^{-1}L & -M^{-1}D \end{bmatrix} \begin{bmatrix} \delta_t \\ \omega_t \end{bmatrix} + \begin{bmatrix} \mathbf{0}_{N\times N} & \mathbf{0}_{N\times N} \\ \mathbf{0}_{N\times N} & M^{-1} \end{bmatrix} \begin{bmatrix} \mathbf{0}_N \\ v_t \end{bmatrix}. \tag{2.24}$$

Next, we partition the nodes state into observable nodes (with PMUs) and hidden

nodes (without PMUs), denoted $\mathcal{O}$ and $\mathcal{H}$, respectively. Let $O := |\mathcal{O}|$ and $H := |\mathcal{H}|$. Then, we get the following equation:

$$\left[\begin{array}{c} \dot{\delta}_t^{\mathcal{O}} \\ \dot{\omega}_t^{\mathcal{O}} \\ \hline \dot{\delta}_t^{\mathcal{H}} \\ \dot{\omega}_t^{h} \end{array}\right] = \left[\begin{array}{c|c} A_{d,\mathcal{O}\mathcal{O}} & A_{d,\mathcal{O}\mathcal{H}} \\ \hline A_{d,\mathcal{H}\mathcal{O}} & A_{d,\mathcal{H}\mathcal{H}} \end{array}\right] \left[\begin{array}{c} \delta_t^{\mathcal{O}} \\ \omega_t^{\mathcal{O}} \\ \hline \delta_t^{\mathcal{H}} \\ \omega_t^{\mathcal{H}} \end{array}\right] + \left[\begin{array}{c|c} B_{\mathcal{O}\mathcal{O}} & \mathbf{0}_{O\times H} \\ \hline \mathbf{0}_{H\times O} & B_{\mathcal{H}\mathcal{H}} \end{array}\right] \left[\begin{array}{c} u_t \\ \hline w_t \end{array}\right], \tag{2.25}$$

where

$$A_{d,\mathcal{O}\mathcal{O}} = \begin{bmatrix} \mathbf{0}_{O\times O} & \mathbf{1}_{O\times O} \\ -(M^{-1}L)_{\mathcal{O}\mathcal{O}} & -(M^{-1}D)_{\mathcal{O}\mathcal{O}} \end{bmatrix}, \quad A_{d,\mathcal{O}\mathcal{H}} = \begin{bmatrix} \mathbf{0}_{O\times H} & \mathbf{0}_{O\times H} \\ -(M^{-1}L)_{\mathcal{O}\mathcal{H}} & -\mathbf{0}_{O\times H} \end{bmatrix},$$

$$A_{d,\mathcal{H}\mathcal{O}} = \begin{bmatrix} \mathbf{0}_{H\times O} & \mathbf{0}_{H\times O} \\ -(M^{-1}L)_{\mathcal{H}\mathcal{O}} & -\mathbf{0}_{H\times O} \end{bmatrix}, \quad A_{d,\mathcal{H}\mathcal{H}} = \begin{bmatrix} \mathbf{0}_{H\times H} & \mathbf{1}_{H\times H} \\ -(M^{-1}L)_{\mathcal{H}\mathcal{H}} & -(M^{-1}D)_{\mathcal{H}\mathcal{H}} \end{bmatrix},$$

$$B_{\mathcal{O}\mathcal{O}} = \begin{bmatrix} \mathbf{0}_{O\times O} & \mathbf{0}_{O\times O} \\ \mathbf{0}_{O\times O} & -M^{-1}{}_{\mathcal{O}\mathcal{O}} \end{bmatrix}, \quad B_{\mathcal{H}\mathcal{H}} = \begin{bmatrix} \mathbf{0}_{H\times H} & \mathbf{0}_{H\times H} \\ \mathbf{0}_{H\times H} & -M^{-1}{}_{\mathcal{H}\mathcal{H}} \end{bmatrix},$$

$$u_t = \begin{bmatrix} \mathbf{0}_O \\ v_t^{\mathcal{O}} \end{bmatrix} \quad v_t = \begin{bmatrix} \mathbf{0}_H \\ v_t^{\mathcal{H}} \end{bmatrix}.$$

Note that we take advantage of the fact that $\mathbf{1}_{N\times N}$ and $M^{-1}D$ are diagonal matrices with their off-diagonal elements being zero. For example, $M^{-1}D_{\mathcal{O}\mathcal{H}}$ is a zero matrix.

After applying Euler-Maruyama discretization, we get

$$\left[\begin{array}{c} \delta_{t+1}^{\mathcal{O}} \\ \omega_{t+1}^{\mathcal{O}} \\ \delta_{t+1}^{\mathcal{H}} \\ \omega_{t+1}^{\mathcal{H}} \end{array}\right] = \left[\begin{array}{c|c} \mathbf{1}_{2O\times 2O} + A_{d,\mathcal{O}\mathcal{O}}\Delta t & A_{d,\mathcal{O}\mathcal{H}}\Delta t \\ \hline A_{d,\mathcal{H}\mathcal{O}}\Delta t & \mathbf{1}_{2H\times 2H} + A_{d,\mathcal{H}\mathcal{H}}\Delta t \end{array}\right] \left[\begin{array}{c} \delta_t^{o} \\ \omega_t^{o} \\ \delta_t^{h} \\ \omega_t^{h} \end{array}\right] + \begin{bmatrix} G & 0 \\ 0 & J \end{bmatrix} \begin{bmatrix} u_t \\ w_t \end{bmatrix}, \tag{2.26}$$

where $G = B_{\mathcal{O}\mathcal{O}}\Delta t$ and $J = B_{\mathcal{H}\mathcal{H}}\Delta t$.

This can be re-written as

$$\begin{bmatrix} y_{t+1} \\ z_{t+1} \end{bmatrix} = \begin{bmatrix} A_{\mathcal{O}\mathcal{O}} & A_{\mathcal{O}\mathcal{H}} \\ A_{\mathcal{H}\mathcal{O}} & A_{\mathcal{H}\mathcal{H}} \end{bmatrix} \begin{bmatrix} y_t \\ z_t \end{bmatrix} + \begin{bmatrix} G & 0 \\ 0 & J \end{bmatrix} \begin{bmatrix} u_t \\ w_t \end{bmatrix}, \tag{2.27}$$

where $y_t = \begin{bmatrix} \delta_t^{\mathcal{O}} \\ \omega_t^{\mathcal{O}} \end{bmatrix}$ and $z_t = \begin{bmatrix} \delta_t^{\mathcal{H}} \\ \omega_t^{\mathcal{H}} \end{bmatrix}$ denote the observable and unobservable variables.

Assume that $E^k = 0$ for some $k \in \mathbb{Z}_+$. This assumption states that the contribution of the hidden nodes to the overall evolution of the network state becomes negligible as time progresses. Then, using this assumption and by expanding (2.27), we get

$$y_{t+1} = A_{\mathcal{O}\mathcal{O}} y_t + \sum_{m=0}^{k-1} A_{\mathcal{O}\mathcal{H}} A_{\mathcal{H}\mathcal{H}}^m A_{\mathcal{H}\mathcal{O}} y_{t-m-1} + G u_t + \sum_{m=0}^{k-1} A_{\mathcal{O}\mathcal{H}} A_{\mathcal{H}\mathcal{H}}^m J w_{t-m-1}. \tag{2.28}$$

This can be equivalently written as:

$$y_{t+1} = \begin{bmatrix} A_{\mathcal{O}\mathcal{O}}{}^\top \\ (A_{\mathcal{O}\mathcal{H}} A_{\mathcal{H}\mathcal{O}})^\top \\ \vdots \\ (A_{\mathcal{O}\mathcal{H}} A_{\mathcal{H}\mathcal{H}}^{k-1} A_{\mathcal{H}\mathcal{O}})^\top \end{bmatrix}^\top \begin{bmatrix} y_t \\ y_{t-1} \\ \vdots \\ y_{t-k} \end{bmatrix} + \begin{bmatrix} G^\top \\ (A_{\mathcal{O}\mathcal{H}} J)^\top \\ \vdots \\ (A_{\mathcal{O}\mathcal{H}} A_{\mathcal{H}\mathcal{H}}^{k-1} J)^\top \end{bmatrix}^\top \begin{bmatrix} u_t \\ w_{t-1} \\ \vdots \\ w_{t-k} \end{bmatrix}. \tag{2.29}$$

Let $Y_t = \begin{bmatrix} y_{t+k} \\ y_{t+k-1} \\ \vdots \\ y_t \end{bmatrix}$, $X = \begin{bmatrix} A_{\mathcal{O}\mathcal{O}}{}^\top \\ A_{\mathcal{O}\mathcal{H}} A_{\mathcal{H}\mathcal{H}}^0 A_{\mathcal{H}\mathcal{O}}{}^\top \\ \vdots \\ A_{\mathcal{O}\mathcal{H}} A_{\mathcal{H}\mathcal{H}}^{k-1} A_{\mathcal{H}\mathcal{O}}{}^\top \end{bmatrix}$ and $\eta_t = \begin{bmatrix} G^\top \\ A_{\mathcal{O}\mathcal{H}} A_{\mathcal{H}\mathcal{H}}^0 J^\top \\ \vdots \\ A_{\mathcal{O}\mathcal{H}} A_{\mathcal{H}\mathcal{H}}^{k-1} J^\top \end{bmatrix}^\top \begin{bmatrix} u_t \\ w_{t-1} \\ \vdots \\ w_{t-k} \end{bmatrix}$. Then, by substitution of Y_t, X and η_t

$$y_{t+k+1}{}^\top = Y_t{}^\top X + \eta_{t+k}{}^\top. \tag{2.30}$$

If we individually left-multiply (2.30) with y_{t+k+1}, and sum it over from $t = 1$ to $t = T-1$, we get,

$$\Sigma_0 = \begin{bmatrix} \Sigma_1{}^\top & \Sigma_2{}^\top & \cdots & \Sigma_{k+1}{}^\top \end{bmatrix} X, \tag{2.31}$$

where $\Sigma_k = \frac{1}{T-1} \sum_{t=1}^{T-1} y_{t+k} y_t{}^\top$ is the generalization of the cross-correlation matrix with displacement in (2.21) where the observations are limited to the PMU measurements from only observable nodes. Note that, since y_{t+k+1} has zero correlation with η_t, the sum over several time steps will lead to the contribution of the noise vector terms to zero.

Similarly, if we left-multiply (2.30) with $y_{t+k+2}, \cdots, y_{t+2k}$, and sum it over from $t = 1$ to $t = T - 1$, we get,

$$\begin{bmatrix} \Sigma_0 \\ \Sigma_1 \\ \vdots \\ \Sigma_k \end{bmatrix} = \begin{bmatrix} {\Sigma_1}^\top & {\Sigma_2}^\top & \cdots & {\Sigma_{k+1}}^\top \\ {\Sigma_2}^\top & {\Sigma_3}^\top & \cdots & {\Sigma_{k+2}}^\top \\ \vdots & \vdots & \ddots & \vdots \\ {\Sigma_{k+1}}^\top & {\Sigma_{k+2}}^\top & \cdots & {\Sigma_{2k+1}}^\top \end{bmatrix} X. \tag{2.32}$$

Here, we assume the system to be stable which allows it to reach an equilibrium. That is, $\Sigma_k = \frac{1}{T-1}\sum_{t=1}^{T-1} y_{t+k} = \frac{1}{T-1}\sum_{t=l}^{l+T-1} y_{t+k}$ for all $l \in \mathbb{Z}_+$. Equation (2.32) allows us to straightforwardly compute $A_{\mathcal{OO}}$ by applying simple Linear Algebra. However, computation of $A_{\mathcal{OH}}$, $A_{\mathcal{HO}}$ and $A_{\mathcal{HH}}$ is non-trivial as they only occur in non-linear terms. However, we can compute $A_{\mathcal{OH}} A_{\mathcal{HH}}^m A_{\mathcal{HO}}$ for $m = 0, \cdots, k-1$.

We present the next set of results with the purpose of recovering the individual matrices $A_{\mathcal{OH}}$, $A_{\mathcal{HO}}$ and $A_{\mathcal{HH}}$ given their product terms $A_{\mathcal{OH}} A_{\mathcal{HH}}^m A_{\mathcal{HO}}$ for $m = 0, \cdots, k-1$. Consider the following condition, which we assume for the rest of the section.

Condition 1. *1. Each visible node is connected to at most one hidden node.*

2. A hidden node is connected to exactly one visible node.

Let $\mathcal{U} \subseteq \mathcal{O}$ be the set of observable nodes such that each one of them is connected exactly one hidden node. The Propositions 1 and 2 provides us information about the structure of matrices that constitute the dynamic matrix A.

Proposition 1. *Under Condition 1, the following statements are true:*

1. $(M^{-1}L)_{\mathcal{HH}}$ *is a diagonal matrix.*
2. $(M^{-1}L)_{\mathcal{OH}}$ *has exactly 1 non-zero entry in each column, and exactly 1 non-zero entry in each row corresponding to node* $o \in \mathcal{U}$.
3. $(M^{-1}L)_{\mathcal{HO}}$ *has exactly 1 non-zero entry in each row, and exactly 1 non-zero entry in each column corresponding to node* $o \in \mathcal{U}$.

Proof of Proposition 1 is trivial.

Proposition 2. *Under Condition 1, for $i \in \mathbb{Z}_+$ and $i \geqslant 1$, $A^i_{\mathcal{H}\mathcal{H}} \in \mathbb{R}^{2H\times 2H}$ such that $A^i_{\mathcal{H}\mathcal{H}} = \begin{bmatrix} \Lambda_{i1} & \Lambda_{i2} \\ \Lambda_{i3} & \Lambda_{i4} \end{bmatrix}$ where $\Lambda_{i1}, \Lambda_{i2}, \Lambda_{i3}, \Lambda_{i4}$ are diagonal matrices.*

Proof. We can prove this using induction. $A^1_{\mathcal{H}\mathcal{H}} = \begin{bmatrix} \mathbf{1}_{H\times H} & T\mathbf{1}_{H\times H} \\ -T(M^{-1}L)_{\mathcal{H}\mathcal{H}} & \mathbf{1}_{H\times H} - T(M^{-1}D)_{\mathcal{H}\mathcal{H}} \end{bmatrix}$. Using Proposition 1, the base case is satisfied. Now, the inductive hypothesis is that $A^{i-1}_{\mathcal{H}\mathcal{H}} = \begin{bmatrix} \Lambda_{i-1,1} & \Lambda_{i-1,2} \\ \Lambda_{i-1,3} & \Lambda_{i-1,4} \end{bmatrix}$ where $\Lambda_{i-1,1}, \Lambda_{i-1,2}, \Lambda_{i-1,3}, \Lambda_{i-1,4} \in \mathbb{R}^N$ are diagonal matrices. Then, $A^i_{\mathcal{H}\mathcal{H}} = A^{i-1}_{\mathcal{H}\mathcal{H}} \times E = \begin{bmatrix} \Lambda_{i-1,1} & \Lambda_{i-1,2} \\ \Lambda_{i-1,3} & \Lambda_{i-1,4} \end{bmatrix} \times \begin{bmatrix} \Lambda_{1,1} & \Lambda_{1,2} \\ \Lambda_{1,3} & \Lambda_{1,4} \end{bmatrix}$. The proof completes by noting that product of two diagonal matrices is a diagonal matrix and sum of two diagonal matrices is also a diagonal matrix. □

Based on Proposition 2, we can obtain simple non-linear expressions for the terms in $A_{\mathcal{O}\mathcal{H}}A_{\mathcal{H}\mathcal{H}}A_{\mathcal{H}\mathcal{O}}$, $A_{\mathcal{O}\mathcal{H}}A^2_{\mathcal{H}\mathcal{H}}A_{\mathcal{H}\mathcal{O}}$ and $A_{\mathcal{O}\mathcal{H}}A^3_{\mathcal{H}\mathcal{H}}A_{\mathcal{H}\mathcal{O}}$ based on the entries of the original dynamic matrix A. Therefore, we conjecture that under Condition 1, if $A_{\mathcal{O}\mathcal{H}}A_{\mathcal{H}\mathcal{H}}A_{\mathcal{H}\mathcal{O}}$, $A_{\mathcal{O}\mathcal{H}}A^2_{\mathcal{H}\mathcal{H}}A_{\mathcal{H}\mathcal{O}}$ and $A_{\mathcal{O}\mathcal{H}}A^3_{\mathcal{H}\mathcal{H}}A_{\mathcal{H}\mathcal{O}}$ are known, then we can reconstruct $A_{\mathcal{O}\mathcal{H}}$, $A_{\mathcal{H}\mathcal{O}}$, and $A_{\mathcal{H}\mathcal{H}}$ matrices using non-linear regression. We provide a sketch of the procedure for computing these matrices. Firstly, for $m \in \mathbb{Z}_+$, $A_{\mathcal{O}\mathcal{H}}A^m_{\mathcal{H}\mathcal{H}}A_{\mathcal{H}\mathcal{O}} \in \mathbb{R}^{2O\times 2O}$. Secondly, $(A_{\mathcal{O}\mathcal{H}}A^m_{\mathcal{H}\mathcal{H}}A_{\mathcal{H}\mathcal{O}})_{O+o,h} = A_{\mathcal{O}\mathcal{H}O+o,h}A^m_{\mathcal{H}\mathcal{H}H+h,h}A_{\mathcal{H}\mathcal{O}H+h} \forall\ h \in \mathcal{H}, (o,h) \in \mathcal{E}$. Given that there are $3\,|\mathcal{U}|$ variables and $3\,|\mathcal{U}|$ constraints, we can write a non-linear regression model to estimate the parameters of dynamic matrix A. A computational study of this approach is part of ongoing work and will be reported in a later publication.

Concluding remarks: In this chapter, we studied an end-to-end framework for attack generation and implementation on an Energy Management System software. First, we assumed that both operator and the attacker possess knowledge of the parameters of an electricity transmission network. We showed how an attacker can perform offline analysis of an EMS software, and leverage its internal properties along with the knowledge of the TN parameters to generate optimal values for manipulation of control-sensitive parameters in the EMS. Then, we showed how that attack can be implemented during runtime by injecting the manipulated parameters in the dynamic memory of a compromised

EMS process. Finally, we showed how both attacker as well as the operator can estimate the power transmission dynamics by online learning of measurement data from Phasor Measurement Units even under certain restrictive conditions of partial observability.

Chapter 3

Vulnerability Assessment of Smart Distribution Networks

In the previous chapter, we presented an end-to-end framework for optimal attack generation and implementation in transmission network energy management system software. We considered an operator model in which the operator implements economic dispatch by unwittingly using the system parameters manipulated by the attacker.

In this chapter, we consider the problem of optimal attack generation in a radial DN with an "infinite" substation bus and a high penetration of Distributed Energy Resources (DERs), in which the operator can optimally respond to attacker actions. The disruption model consists of DER node compromises, whereas the operator response comprises of load control and response by non-compromised DERs. We also consider an optimal security problem in which the operator can proactively secure a subset of DER nodes subject to budget constraints to minimize the maximin loss caused by the attacker's disruption and operator's response.

3.1 Network model with "infinite" substation bus

Distribution network model

We summarize the standard network model of radial electric distribution systems [41, 108, 130]. Consider a tree network of nodes and distribution lines $\mathcal{G} = (\mathcal{N} \cup \{0\}, \mathcal{E})$,

where $\mathcal{N}$ denotes the set of all nodes except the substation (labeled as node 0), and let $N := |\mathcal{N}|$. Let $V_i \in \mathrm{W}$ denote the complex voltage at node i, and $\nu_i := |V_i|^2$ denote the square of voltage magnitude. We assume that the magnitude of substation voltage $|V_0|$ is constant. Let $I_j \in \mathrm{W}$ denote the current flowing from node i to node j on line $(i,j) \in \mathcal{E}$, and $\ell_j := |I_j|^2$ the square of the magnitude of the current. A distribution line $(i,j) \in \mathcal{E}$ has a complex impedance $z_j = r_j + \mathbf{j}x_j$, where $r_j > 0$ and $x_j > 0$ denote the resistance and inductance of the line (i,j), respectively, and $\mathbf{j} = \sqrt{-1}$.

The voltage regulation requirements of the DN under *nominal* no attack conditions govern that:

$$\forall \quad i \in \mathcal{N}, \quad \underline{\nu}_i \leqslant \nu_i \leqslant \overline{\nu}_i, \tag{3.1}$$

where $\underline{\nu}_i = |\underline{V}_i|^2$ and $\overline{\nu}_i = \left|\overline{V}_i\right|^2$ are the *soft* lower and upper bounds for maintaining voltage quality at node i. Additionally, voltage magnitudes under *all* conditions satisfy:

$$\forall \quad i \in \mathcal{N}, \quad \underline{\mu} \leqslant \nu_i \leqslant \overline{\mu}, \tag{3.2}$$

where $\underline{\mu}$ and $\overline{\mu}$ are the *hard* voltage safety bounds for any nodal voltage, and $0 < \underline{\mu} < \min_{i\in\mathcal{N}} \underline{\nu}_i \leqslant \max_{i\in\mathcal{N}} \overline{\nu}_i < \overline{\mu}$.

Load model

We consider constant power loads [52].[1] Let $sc_i := pc_i + \mathbf{j}qc_i$ denote the power consumed by a load at node i, where pc_i and qc_i are the real and reactive components. Let $\mathrm{sc}_i^{\mathrm{nom}} := \mathrm{pc}_i^{\mathrm{nom}} + \mathbf{j}\mathrm{qc}_i^{\mathrm{nom}}$ denote the *nominal* power demanded by a node i, where $\mathrm{pc}_i^{\mathrm{nom}}$ and $\mathrm{qc}_i^{\mathrm{nom}}$ are the real and reactive components of $\mathrm{sc}_i^{\mathrm{nom}}$. Under our assumptions, for all $i \in \mathcal{N}$, $pc_i \leqslant \mathrm{pc}_i^{\mathrm{nom}}$ and $qc_i \leqslant \mathrm{qc}_i^{\mathrm{nom}}$, i.e., the actual power consumed at each node is upper bounded by the nominal demand:

$$\forall \quad i \in \mathcal{N}, \quad sc_i \leqslant \mathrm{sc}_i^{\mathrm{nom}}. \tag{3.3}$$

[1] We do not consider frequency dependent loads as our analysis is limited to attacks that do not cause disturbances in system frequency; see Sec. 3.2 for our justification of constant system frequency assumption.

DER model

[2] Let $sg_i := pg_i + \mathbf{j}qg_i$ denote the power generated by the DER connected to node i, where pg_i and qg_i denote the active and reactive power, respectively. Following [53], [130], sg_i is bounded by the apparent power capability of the inverter, which is a given constant $\overline{\mathrm{sp}}_i$. We denote the DER set-point by $\mathrm{sp}_i = \mathbf{Re}(\mathrm{sp}_i) + \mathbf{jIm}(\mathrm{sp}_i)$, where $\mathbf{Re}(\mathrm{sp}_i)$ and $\mathbf{Im}(\mathrm{sp}_i)$ are the real and reactive components. The power generated at each node is constrained as follows:

$$\forall \quad i \in \mathcal{N}, \quad sg_i \leqslant \mathrm{sp}_i \in \mathcal{S}_i, \tag{3.4}$$

where $\mathcal{S}_i := \{\mathrm{sp}_i \in \mathrm{W} \quad | \quad \mathbf{Re}(\mathrm{sp}_i) \geqslant 0 \text{ and } |\mathrm{sp}_i| \leqslant \overline{\mathrm{sp}}_i\}$. $\mathcal{S} := \prod_{i\in\mathcal{N}} \mathcal{S}_i$ denotes the set of configurable set-points.

We denote the net power consumed at node i by $s_i := sc_i - sg_i$. A DN can be fully specified by the tuple $\langle \mathcal{G}, |V_0|, z, \mathrm{sc}^{\mathrm{nom}}, \overline{\mathrm{sp}} \rangle$, where $z, \mathrm{sc}^{\mathrm{nom}}, \overline{\mathrm{sp}}$ are row vectors of appropriate dimensions, and are assumed to be constant.

Power flow equations

The 3-phase balanced nonlinear power flow (NPF) on line $(i,j) \in \mathcal{E}$ is given by [41]:

$$S_j = \textstyle\sum_{k:(j,k)\in\mathcal{E}} S_k + sc_j - sg_j + z_j \ell_j \tag{3.5a}$$

$$\nu_j = \nu_i - 2\mathbf{Re}(\bar{z}_j S_j) + |z_j|^2 \ell_j \tag{3.5b}$$

$$\ell_j = \frac{|S_j|^2}{\nu_i}, \tag{3.5c}$$

where $S_j = P_j + \mathbf{j}Q_j$ denotes the complex power flowing from node i to node j on line $(i,j) \in \mathcal{E}$, and $\bar{z}$ is the complex conjugate of z; (3.5a) is the power conservation equation; (3.5b) relates the voltage drop and the power flows; and (3.5c) is the current-voltage-power relationship. For the NPF model (3.5), we define a state as follows:

$$\mathrm{x} := \Big[\nu, \ell, sc, sg, S\Big],$$

[2] We use the term DER to denote the complete DER-inverter assembly attached to a node of DN.

where $\mathrm{x} \in \mathbb{R}_{+}^{2N} \times \mathrm{W}^{3N}$, and ν, ℓ, sc, sg, and S are row vectors of appropriate dimensions. Let $\mathcal{F}$ denote the set of all states x that satisfy (3.2), (3.3), (3.4) and the NPF model (3.5), and define the set of all states with *no reverse power flows* (see Sec. 3.2 for additional assumptions) as follows:

$$\mathcal{X} := \{\mathrm{x} \in \mathcal{F} | S \geqslant 0\}.$$

The linear power flow (LPF) approximation of (3.5) is:

$$\widehat{S}_j = \textstyle\sum_{k:(j,k)\in\mathcal{E}} \widehat{S}_k + \widehat{sc}_j - \widehat{sg}_j \tag{3.6a}$$

$$\widehat{\nu}_j = \widehat{\nu}_i - 2\mathbf{Re}(\bar{z}_j \widehat{S}_j) \tag{3.6b}$$

$$\widehat{\ell}_j = \frac{\left|\widehat{S}_j\right|^2}{\widehat{\nu}_i}, \tag{3.6c}$$

where $\hat{\mathrm{x}} := [\widehat{\nu}, \widehat{\ell}, \widehat{sc}, \widehat{sg}, \widehat{S}]$ is a state of the LPF model, and analogous to the NPF model, define the set of LPF states $\hat{\mathrm{x}}$ with no reverse power flows as $\widehat{\mathcal{X}}$.

Notation and definitions

All vectors are row vectors, unless otherwise stated. For two vectors c and d, $c \odot d$ denotes their Hadamard product.

Let $K_j := \dfrac{r_j}{x_j}$ be the resistance-to-reactance (**r**/**x**) ratio for line $(i,j) \in \mathcal{E}$, and let $\underline{K}$ and $\overline{K}$ denote the minimum and maximum of the K_js over all $(i,j) \in \mathcal{E}$. We say that DERs at nodes j and k are homogeneous with respect to each other if their set-point configurations as well as their apparent power capabilities are identical, i.e., $\mathrm{sp}_j = \mathrm{sp}_k$ and $\overline{\mathrm{sp}}_j = \overline{\mathrm{sp}}_k$. Similarly, two loads at nodes j and k are homogeneous if $\mathrm{sc}_j^{\mathrm{nom}} = \mathrm{sc}_k^{\mathrm{nom}}$.

For any given node $i \in \mathcal{N}$, let $\mathcal{P}_i$ be the path from the root node to node i. Thus, $\mathcal{P}_i$ is an ordered set of nodes starting from the root node and ending at node i, excluding the root node; see Figure 3-1. We say that node j is an *ancestor* of node k ($j \prec k$), or equivalently, k is a successor of j *iff* $\mathcal{P}_j \subset \mathcal{P}_k$. We define the *relative ordering* $\preceq_i$, with respect to a "pivot" node i as follows:

- j *precedes* k ($j \preceq_i k$) *iff* $\mathcal{P}_i \cap \mathcal{P}_j \subseteq \mathcal{P}_i \cap \mathcal{P}_k$.

- j *strictly precedes* k ($j \prec_i k$) *iff* $\mathcal{P}_i \cap \mathcal{P}_j \subset \mathcal{P}_i \cap \mathcal{P}_k$.

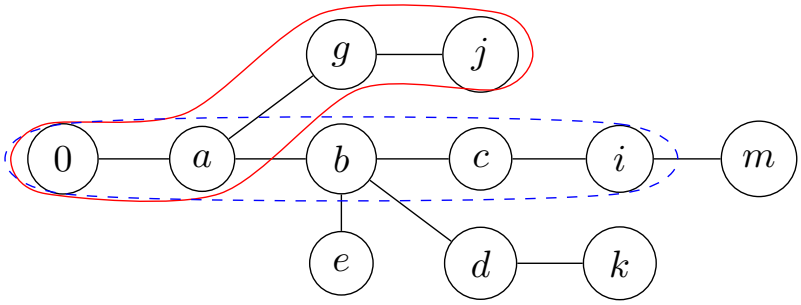


Figure 3-1: Precedence description of the nodes for a tree network. Here, $j \prec_i k$, $e =_i k$, $b \prec k$, $\mathcal{P}_j = \{a, g, j\}$, $\mathcal{P}_i \cap \mathcal{P}_j = \{a\}$.

- j is at the *same precedence level* as k ($j =_i k$) *iff*
  $\mathcal{P}_i \cap \mathcal{P}_j = \mathcal{P}_i \cap \mathcal{P}_k$.

We define the common path impedance between any two nodes $i, j \in \mathcal{N}$ as the sum of impedances of the lines in the intersection of paths $\mathcal{P}_i$ and $\mathcal{P}_j$, i.e., $Z_{ij} := \sum_{k \in \mathcal{P}_i \cap \mathcal{P}_j} z_k$, and denote the resistive (real) and inductive (imaginary) components of Z_{ij} by R_{ij} and X_{ij}, respectively.

Finally, we define some useful terminology for the tree network $\mathcal{G}$. Let H denote the height of $\mathcal{G}$, and let $\mathcal{N}_h$ denote the set of nodes on level h for $h = 1, 2, \cdots, H$. For any node $i \in \mathcal{N}$, h_i denotes the level of node i; $\mathcal{N}_i^c$ the set of children nodes of node i; Λ_i the set of nodes in the subtree rooted at node i; Λ_i^j the set of nodes in the subtree rooted at node i until level h_j, where $j \in \Lambda_i$; $\mathcal{N}_L$ the set of leaf nodes, i.e., $\mathcal{N}_L := \{j \in \mathcal{N} \mid \nexists\, k \in \mathcal{N} \text{ s.t. } (j, k) \in \mathcal{E}\}$.

3.2 Defender-Attacker-Defender game

We consider a 3-stage sequential game between a defender (network operator) and an attacker (external threat agent).

- **Stage 1:** The defender chooses a security strategy
  $u \in \mathcal{U}_B$ to secure a subset of DERs;

- **Stage 2:** The attacker chooses from the set of DERs that were not secured by the defender in Stage 1, and manipulates their set-points according to a strategy
  $\psi := \left[\mathrm{sp}^{\mathrm{a}}, \delta\right] \in \Psi_{\mathrm{k}}(u)$;

- **Stage 3:** The defender responds by choosing the set-points of the uncompromised DERs and, if possible, impose load control at one or more nodes according to a strategy $\phi := \left[\mathrm{sp}^{\mathrm{d}}, \gamma\right] \in \Phi(u, \psi)$.

The [DAD] game is a sequential game of perfect information, i.e. each player is perfectly informed about the actions that have been chosen by the previous players. The equilibrium concept is the classical Stackelberg equilibrium.

In this game, $\mathcal{U}_B$ and $\Phi(u, \psi)$ denote the set of defender actions in Stage 1 and 3, respectively; and $\Psi_{\mathrm{k}}(u)$ denotes the set of attacker strategies in Stage 2. Formally, the defender-attacker-defender [DAD] game is as follows:

$$[\mathrm{DAD}]\ \mathcal{L} := \min_{u \in \mathcal{U}_B}\ \max_{\psi \in \Psi_{\mathrm{k}}}\ \min_{\phi \in \Phi}\ \mathrm{L}(\mathrm{x}(u, \psi, \phi)) \tag{3.7}$$

$$\begin{aligned}
\text{s.t.} \quad & \mathrm{x}(u, \psi, \phi) \ \in \mathcal{X} && \text{(3.8a)}\\
& sc(u, \psi, \phi) \ = \gamma \odot \mathrm{sc}^{\mathrm{nom}} && \text{(3.8b)}\\
& sg(u, \psi, \phi) = u \odot \mathrm{sp}^{\mathrm{d}} + (\mathbf{1}_N - u) \\
& \qquad\qquad \odot \left[\delta \odot \mathrm{sp}^{\mathrm{a}} + (\mathbf{1}_N - \delta) \odot \mathrm{sp}^{\mathrm{d}}\right], && \text{(3.8c)}
\end{aligned}$$

where (3.8b) specifies that the *actual power consumed* at node i is equal to the power demand scaled by the corresponding load control parameter $\gamma_i \in [\underline{\gamma}_i, 1]$ chosen by the defender.

The constraint (3.8c) models the net effect of defender choice u_i in Stage 1, the attacker choice $(\mathrm{sp}^{\mathrm{a}}_i, \delta_i)$ in Stage 2, and the defender choice $\mathrm{sp}^{\mathrm{d}}_i$ in Stage 3 on the *actual power generated* at node i. Thus, (3.8c) is the *adversary model* of [DAD] game: the DER i is compromised *if and only if* it was not secured by the defender ($u_i = 0$) *and* was targeted by the attacker ($\delta_i = 1$). Specifically, if i is compromised, $\mathrm{sp}_i = \mathrm{sp}^{\mathrm{a}}_i$, where $\mathrm{sp}^{\mathrm{a}}_i = \mathbf{Re}(\mathrm{sp}^{\mathrm{a}}_i) + \mathbf{jIm}(\mathrm{sp}^{\mathrm{a}}_i)$ is the false set-point chosen by the attacker. The set-points of non-compromised DERs are governed by the defender, i.e., if DER i is not compromised $\mathrm{sp}_i = \mathrm{sp}^{\mathrm{d}}_i$.

Note that the physical restriction (3.4) applies to all DER nodes, including the com-

promised ones. If the attacker's set-point violates this constraint, it will not be admitted by the inverter as a valid set-point. Such an attack will not affect the attack model (3.8c), and consequently it will not change the actual power generated by the DER. Also, our adversary model assumes that the DERs' power output, sg, quickly attain the set-points specified by (3.8c). Thus we do not consider dynamic set-point tracking. [3]

During the nominal operating conditions, the network operator minimizes the line losses due to power flow on the distribution lines ($\mathrm{L_{LL}}$). Typical OPF formulations mainly account for this cost. However, this objective function is not representative of the loss incurred by operator (defender) during the aforementioned attack on the DN. We define loss function in [DAD] as follows:

$$\mathrm{L}(\mathrm{x}(u, \psi, \phi)) \coloneqq \mathrm{L_{VR}}(\mathrm{x}) + \mathrm{L_{LC}}(\mathrm{x}) + \mathrm{L_{LL}}(\mathrm{x}), \tag{3.9}$$

where $\mathrm{L_{VR}}(\mathrm{x})$ and $\mathrm{L_{LC}}(\mathrm{x})$ model the *monetary cost* to the defender due to the loss in voltage regulation and the cost of load curtailment/shedding (i.e., loss due to partially satisfied demand), respectively. The term denotes $\mathrm{L_{LL}}$ the total line losses. These costs are defined as follows:

$$\mathrm{L_{VR}}(\mathrm{x}) \coloneqq \left\| W \odot (\underline{\nu} - \nu)_+ \right\|_\infty \tag{3.10a}$$

$$\mathrm{L_{LC}}(\mathrm{x}) \coloneqq \left\| C \odot (1 - \gamma) \odot \mathrm{pc}^{\mathrm{nom}} \right\|_1 \tag{3.10b}$$

$$\mathrm{L_{LL}}(\mathrm{x}) \coloneqq \left\| r \odot \ell \right\|_1, \tag{3.10c}$$

where $W, C \in \mathbb{R}^N_+$. The weight W_i is the cost of unit voltage bound violation and C_i is the cost of shedding unit load (or demand dissatisfaction) at node i, and r denotes the vector of resistances. Note that $\mathrm{L_{VR}}$ is the maximum of the weighted non-negative difference between the lower bound $\underline{\nu}_i$ and nodal voltage square ν_i. We expect that during the attack, the defender's primary concern will be to satisfy the voltage regulation requirements, and minimize the inconvenience to the customers due to load curtailment. Thus, we assume

[3] Note that, under this adversary model, the impact of DER compromise is different than the impact of a natural event, e.g. cloud cover, during which $pg = \mathbf{0}$. The reactive power contribution may be non-negative during a natural event; however, as we show in Sec. 3.3, a compromised DER contributes reactive power equal to the negative of apparent power capability.

that the weights W_i and C_i are chosen such that $\mathrm{L_{LL}}$ is relatively small compared to $\mathrm{L_{VR}}$ and $\mathrm{L_{LC}}$.

Note that we added the $\mathrm{L_{LL}(x)}$ term in (3.9) primarily to ensure that the loss function $\mathrm{L(x)}$ remains strictly convex function of the net demand $s = sc - sg$. The strict convexity allows us to have a unique solution for the inner problem for fixed attacker's actions. In our computational study in Sec. 3.5, we choose the weights W and C such that the line loss is negligible compared to $\mathrm{L_{VR}}$ and $\mathrm{L_{LC}}$.

However, more generally, the loss function $\mathrm{L(x)}$ should reflect the monetary costs incurred by the defender in maintaining the supply-demand balance and in restoring the safe operating conditions after the attack. Such a general model will contain following terms: (a) the cost of supplying additional power from the substation node to match the difference between actual power consumed by the loads and the effective DER generation ($\mathrm{L_S(x)}$); (b) the cost due to the loss of voltage regulation ($\mathrm{L_{VR}(x)}$); (c) the cost of curtailing or shedding certain loads ($\mathrm{L_{LC}(x)}$); (d) the cost of reactive power (VAR) control and the cost of energy spillage for the uncompromised DERs ($\mathrm{L_{AC}(x)}$); and (e) the costs of equipment damage due to the attack ($\mathrm{L_D(x)}$).

For the sake of simplicity, we do not consider $\mathrm{L_{AC}(x)}$ and $\mathrm{L_D(x)}$ in our formulation. The choice of ignoring $\mathrm{L_{AC}(x)}$ can be justified if we assume that the DER owners participate in VAR control, perhaps in return of a pre-specified compensation by the operator/defender. Alternatively, the DERs may be required to contribute reactive power during contingency scenarios (i.e., supply-demand mismatch during the attack). The main difficulty in modeling $\mathrm{L_D(x)}$ is that it requires relating the state vector to the probability of equipment failures. Since our focus is on security assessment of DNs, as opposed to network reinforcement using investment in physical protection devices, we ignore this cost in our analysis. Finally, we also ignore the contribution of $\mathrm{L_S(x)}$ to the loss function, as it is likely to be dominated by $\mathrm{L_{VR}}$ and $\mathrm{L_{LC}}$.

Stage 1 [Security Investment]

The set of defender actions is:

$$\mathcal{U}_B := \{u \in \{0,1\}^{\mathcal{N}} \mid \|u\|_0 \leqslant B\},$$

where $B \leqslant |\mathcal{N}|$ denotes a security budget. Since, securing control-center's communication to every DER node in a geographically diverse DN might be costly/impractical, we impose that the maximum number of nodes the defender can secure is B. A defender's choice $u \in \mathcal{U}_B$ implies that a DER at node i is secure if $u_i = 1$ (i.e. DER at node i cannot be compromised), and vulnerable to attack if $u_i = 0$. Let $\mathcal{N}_s(u) := \{i \in \mathcal{N} | u_i = 1\}$ and $\mathcal{N}_v(u) := \mathcal{N} \backslash \mathcal{N}_s(u)$ denote the set of secure and vulnerable nodes, for a given u. [4]

There are several factors which limit the defender's ability to ensure full security of DERs. First, to ensure the security of control software and network communications that support DER operations, we need cost-effective and interoperable security solutions that can be widely adopted by different entities (e.g., DER manufacturers, service providers, and owners). Secondly, the DNs are likely to inherit some of the vulnerabilities of COTS IT devices that may directly or indirectly affect DER operations. Third, the defenders (operators) need to justify the business case to deploy security solutions. Existing work on security investments in such networked environments, indicates that the operators tend to underestimate security risks [8]. Consequently, in the absence of proper regulatory impositions, they tend to underinvest in well-known security solutions. In our model, we capture the limitations imposed by these factors by introducing a security budget B which restricts the maximum number of nodes the defender can secure in Stage 1.

Stage 2 [Attack]

Let $\Psi_{\mathrm{k}}(u) := \mathcal{S}(u) \times \mathcal{D}_{\mathrm{k}}(u)$ denotes the set of attacker actions for a defender's choice u, where

$$\mathcal{S}(u) := \textstyle\prod_{i \in \mathcal{N}_v(u)} \mathcal{S}_i \times \prod_{j \in \mathcal{N}_s(u)} \{0 + 0\mathbf{j}\}$$
$$\mathcal{D}_{\mathrm{k}}(u) := \{\delta \in \{0,1\}^{\mathcal{N}} \mid \delta \leqslant \mathbf{1}_N - u,\ \|\delta\|_0 \leqslant \mathrm{k}\},$$

[4] Note that by a "secure" node, we mean that the DER at that node is not prone to compromise by the attacker. From a practical viewpoint, the defender can secure a DER node by investing in node security solutions such as intrusion prevention systems (IPS) [34]. These security solutions are complementary to the device hardening technologies that can secure the DER-inverter assembly. Our focus is on security against a threat agent interested in simultaneously compromising multiple DERs. Thus, we restrict our attention to node security solutions.

and $\mathrm{k} \leqslant |\mathcal{N}_v|$ is the maximum number of DERs that the attacker can compromise. This limit accounts for the attacker's resource constraints (and/or restrict his influence based on his knowledge of DER vulnerabilities). The attacker *simultaneously* compromises a subset of vulnerable DER nodes by introducing incorrect set-points (see the adversary model (3.8c)), and increase the loss L (see (3.9)). The attacker's choice is denoted by $\psi := \left[\mathrm{sp}^{\mathrm{a}}, \delta\right] \in \Psi_{\mathrm{k}}(u)$, where sp^{a} denotes the vector of incorrect set-points chosen by the attacker, and $\delta \in \mathcal{D}_{\mathrm{k}}$ denotes the attack vector that indicates the subset of DERs compromised. A DER at node i is compromised if $\delta_i = 1$, and not compromised if $\delta_i = 0$.

We assume that the attacker has full information about the DN, i.e., she knows $\langle \mathcal{G}, |V_0|, z, \mathrm{sc}^{\mathrm{nom}}, \mathrm{sp} \rangle$ and maximum fraction of controllable load at each node. The attacker also knows the set of DERs secured by the defender in Stage 1 of the game, voltage regulation bounds, and defender's cost parameters (i.e. the weight W_i for voltage bound violation and the cost of unit load shedding C_i for each node i). By assuming such an *informed attacker*, we are able to focus on how the attacker uses the knowledge of the physical system toward achieving her objective. Thus, we take a conservative approach and do not explicitly consider particular mechanisms of how a security vulnerability might be exploited by the attacker. Admittedly, our attack model may be unrealistic in some scenarios; however, it allows us to identify the critical DER nodes, and characterize optimal security investment and defender response; see Sec. 3.5.

Next, we justify the attacker's resource constraint k. First, the DERs are likely to be heterogeneous in their capacity, design, and manufacturer type. The attacker may not have the specific knowledge to exploit vulnerabilities in all DER systems deployed on a DN. Secondly, in practice, the process of DER integration is gradual and so is the progress on implementing security solutions in the control processes that support DER operations. The attacker's capability to compromise DERs depends on how the available threat channels vary which such a technological change. Third, the security of DNs is likely to be affected by the security practices adopted by owners of DERs. For example, the attacker's capability will be limited if the DER operations are secured by a regulated distribution utility who faces compliance checks or mandatory disclosure of known incidents. In contrast, he is more likely to gain a backdoor entry if the DN has substantial participation

from a variety of third party DER owners who may not follow prudent security practices. In our analysis, we model the attacker's capability by introducing a parameter k, which is the maximum number of DERs that the attacker can compromise.

Stage 3 [Defender Response]

Let $\underline{\gamma}_i \geqslant 0$ denote the maximum permissible fraction of load control at node i, and define the set of Stage 3 defender actions:

$$\Phi(u, \psi) \coloneqq \mathcal{S} \times \Gamma,$$

where $\Gamma \coloneqq \prod_{i \in \mathcal{N}} [\underline{\gamma}_i, 1]$. The defender chooses new set-points sp^{d} of non-compromised DERs, and load control parameters γ_i to reduce the loss L. The defender action is modeled as a vector $\phi \coloneqq \left[\mathrm{sp}^{\mathrm{d}}, \gamma\right] \in \Phi(u, \psi)$, where sp^{d} (resp. γ) denotes the vector of $\mathrm{sp}_i^{\mathrm{d}}$ (resp. γ_i).

We make the standard assumption that the defender knows the nominal demand (i.e., the demand in pre-attack conditions) using measurements collected from the DN nodes. We also assume that the defender can distinguish between compromised and non-compromised DERs. In heavy loading conditions, the defender expects the output of a non-compromised DER to lie in the first quadrant (see Figure 3-3 in Sec. 3.3), i.e. it contributes positive active and reactive power to the DN. A simple technique to detect compromised DERs is whether the inverter output lies in the fourth quadrant.

Assumptions about the DN model

In general, [DAD] is a non-convex, non-linear, tri-level optimization problem with mixed-integer decision variables. Hence, it is a computationally hard problem. Our goals are:

(i) to provide structural insights about the optimal attacker and defender strategies of the [DAD] game;

(ii) to approximate the non-linear (hard) problem by formulating computationally tractable variants based on linear power flow models.

To address these goals we make the following assumptions:

$(\mathbf{A0})_1$ **Voltage quality:** In no attack (nominal) conditions, both $\mathcal{X}$ and $\widehat{\mathcal{X}}$ satisfy the voltage quality bounds (3.1).

$(\mathbf{A0})_2$ **Safety:** Safety bounds (3.2) are always satisfied, i.e., $\forall\ (u,\psi,\phi) \in \mathcal{U}_B \times \Psi \times \Phi$, $\forall\ \mathrm{x}(u,\psi,\phi) \in \mathcal{X}$, $\underline{\mu}\mathbf{1}_N \leqslant \nu \leqslant \overline{\mu}\mathbf{1}_N$.

$(\mathbf{A0})_3$ **No reverse power flows:** Power flows from node 0 towards the downstream nodes, i.e., $\widehat{S} \geqslant 0$. This implies that $\forall\ \hat{\mathrm{x}} \in \widehat{\mathcal{X}},\ \hat{\nu} \leqslant \nu_0\mathbf{1}_N$; similarly, for NPF model.

$(\mathbf{A0})_4$ **Small impedance:** All power flows are in the per unit (*p.u.*) system, i.e., $\nu_0 = 1$ and $\forall\ (i,j) \in \mathcal{E},\ |S_j| < 1$. Furthermore, the resistances and reactances are small, i.e.,

$$\forall\ (i,j) \in \mathcal{E}, r_j \leqslant \frac{\underline{\mu}^2}{4\underline{\mu}+8} < 1,\ x_j \leqslant \frac{\underline{\mu}^2}{4\underline{\mu}+8} < 1,$$

and the common path resistances and reactances are also smaller than 1, i.e., $R_{ii} \leqslant 1$ and $X_{ii} \leqslant 1\ \forall\ i \in \mathcal{N}$.

$(\mathbf{A0})_5$ **Small line losses:** The line losses are very small compared to power flows, i.e., $\forall\ \mathrm{x} \in \mathcal{X},\ z \odot \ell \leqslant \epsilon_0 S$, where ϵ_0 is a small positive number. [5]

$(\mathbf{A0})_1$-$(\mathbf{A0})_2$ are standard assumptions. $(\mathbf{A0})_3$ assumes that the DER penetration level is such that the net demand is always positive. In real-world DNs, both r_js and x_js are typically around 0.01 $(\mathbf{A0})_4$. Also, residential load power factors ($pc_j/|sc_j|$) are in range of 0.88-0.95. For these values, one can show that $\epsilon_0 \approx 0.05$ $(\mathbf{A0})_5$. We will denote $(\mathbf{A0})_1$-$(\mathbf{A0})_5$ by **(A0)** .

In addition to the aforementioned assumption, we also assume that *(a)* the node 0 is an infinite bus; *(b)* the voltage ν_0 is constant, and *(c)* the system frequency is constant.

These assumptions are standard in the steady state power flow analyses, and can be justified as follows: Our focus is on the security assessment of DNs that have substation nodes with high enough ramp rates in supplying $\sim 50\ MW$ power (typical for medium-voltage (MV) substations). That is, any supply-demand imbalance of the order of $50\ MW$ can be cleared relatively quickly by the substation; hence the infinite substation bus assumption.

[5] Equivalently, ϵ_0 is an upper bound on the maximum ratio of the magnitudes of line losses and the power flows, i.e., $\epsilon_0 = \max_{(i,j)\in\mathcal{E}, P_j\neq 0, Q_j\neq 0} \max\left(r_j\ell_j/P_j, x_j\ell_j/Q_j\right)$. Thus, ϵ_0 can be determined by setting the values of loads to the corresponding nominal demands, and then computing the line losses and power flows for nominal conditions.

The assumption *(b)* is typical in OPF formulations and we make it for the sake of mathematical convenience. Indeed, as a consequence of attack, there will be a net reduction in the substation voltage relative to the pre-attack value ν_0. This effect is due to a higher net demand after the Stage 3 of the game. To meet this additional demand, higher currents will flow through the distribution lines, resulting in even higher drops in the nodal voltages than what we obtained using the computational approach detailed in Sec. 3.3. Thus, our estimate of the optimal loss is actually a lower bound on the true value of optimal loss that the defender would face when the substation voltage drops after the attack.

To justify assumption *(c)*, we argue that even large-scale penetration of DERs is not likely to achieve a generation capacity beyond $50\ MW$ from a single DN. Even in the worst case, i.e. when all the DERs are simultaneously disconnected, their impact on the system frequency will be negligible.

Next, we choose ϵ as follows

$$\epsilon := (1-\epsilon_0)^{-H} - 1, \tag{3.11}$$

where H is the height of the tree DN and ϵ_0 is chosen as above. Now, consider another linear power flow model (which we call the ϵ-LPF model):

$$\breve{S}_j = \textstyle\sum_{k:(j,k)\in\mathcal{E}} \breve{S}_k + (1+\epsilon)(\breve{sc}_j - \breve{sg}_j) \tag{3.12a}$$

$$\breve{\nu}_j = \breve{\nu}_i - 2\mathbf{Re}(\bar{z}_j \breve{S}_j) \tag{3.12b}$$

$$\breve{\ell}_j = \frac{\left|\breve{S}_j\right|^2}{\breve{\nu}_i}, \tag{3.12c}$$

and $\breve{\mathrm{x}} := \left[\breve{\nu}, \breve{\ell}, \breve{sc}, \breve{sg}, \breve{S}\right]$ is a state of ϵ-LPF model, and $\breve{\mathcal{X}}$ is the set of all states $\breve{\mathrm{x}}$ with no reverse power flows. (Note that for $\epsilon = 0$, (3.12) becomes (3.6).)

We also note that both LPF and ϵ-LPF models ignore the line losses term $z_j\ell_j$ in the power balance equation (5a), and the term $|z_j|^2\,\ell_j$ in the voltage drop equation (5b). The power flows obtained by ignoring these terms approximate the non-linear power flow (NPF) model calculations under the assumption $(\mathbf{A0})_3$, i.e., the line impedances are very

small $|z_j| \ll 1$. Under the assumption $(\mathbf{A0})_2$, i.e. no reverse power flows, the LPF provides a lower bound on the line power flows, and an upper bound on the nodal voltages of the standard DistFlow model [52],[53]. The main use of ϵ-LPF model is that it provides an *upper bound* on the line power flows and a lower bound on the nodal voltages; see Proposition 3 in Sec. 3.3.

We will consider two variants of the [DAD] game (3.44)-(3.45):

$$[\widehat{\text{DAD}}]\ \widehat{\mathcal{L}} := \min_{u\in\mathcal{U}_B}\ \max_{\psi\in\Psi_{\text{k}}}\ \min_{\phi\in\Phi}\ \widehat{\text{L}}(\hat{\text{x}}(u,\psi,\phi))$$

$$\text{s.t.}\quad \hat{\text{x}}(u,\psi,\phi)\in\widehat{\mathcal{X}},\ (3.8b),\ (3.8c),$$

and

$$[\widetilde{\text{DAD}}]\ \breve{\mathcal{L}} := \min_{u\in\mathcal{U}_B}\ \max_{\psi\in\Psi_{\text{k}}}\ \min_{\phi\in\Phi}\ \breve{\text{L}}(\breve{\text{x}}(u,\psi,\phi))$$

$$\text{s.t.}\quad \breve{\text{x}}(u,\psi,\phi)\in\breve{\mathcal{X}},\ (3.8b),\ (3.8c),$$

where $\widehat{\text{L}}(\hat{\text{x}}) := \text{L}_{\text{VR}}(\hat{\text{x}}) + \text{L}_{\text{LC}}(\hat{\text{x}})$, and $\breve{\text{L}}(\breve{\text{x}}) := \text{L}_{\text{VR}}(\breve{\text{x}}) + \text{L}_{\text{LC}}(\breve{\text{x}})$ are the loss functions for $[\widehat{\text{DAD}}]$ and $[\widetilde{\text{DAD}}]$, respectively. Note that the loss functions $\widehat{\text{L}}$ and $\breve{\text{L}}$ do not have the line losses term. The optimal loss L of $[\widehat{\text{DAD}}]$ and $[\widetilde{\text{DAD}}]$ are denoted by $\widehat{\mathcal{L}}$ and $\breve{\mathcal{L}}$, respectively. Our results in §3.6-3.5 show that **(a)** $[\widehat{\text{DAD}}]$ (resp. $[\widetilde{\text{DAD}}]$) help provide under (resp. over) approximation of [DAD]; and **(b)** the derivation of structural properties of optimal strategies in both $[\widehat{\text{DAD}}]$ and $[\widetilde{\text{DAD}}]$ is analogous to one another.

We will, henceforth, abuse the notation, and use Ψ and Φ to denote $\Psi_{\text{k}}(u)$ and $\Phi(u,\psi)$, respectively. For a summary of notations, see Table 3.1.

$\mathbf{j}$	$\mathbf{j} = \sqrt{-1}$ complex square root of -1		
	Network parameters		
$\mathcal{N}$	set of nodes		
$\mathcal{E}$	set of edges		
$\mathcal{G}$	tree topology $\mathcal{G} = (\mathcal{N}, \mathcal{E})$		
r_j	resistance of line $(i,j) \in \mathcal{E}$		
x_j	reactance of line $(i,j) \in \mathcal{E}$		
z_j	impedance $z_j = r_j + \mathbf{j}x_j$ of line $(i,j) \in \mathcal{E}$		
H	height of the tree		
$\mathcal{N}_h$	set of nodes on level $h \in 1, 2, \cdots, H$		
h_i	level of node i		
$\mathcal{N}_i^{\mathrm{c}}$	set of children nodes of node i		
Λ_i	subtree rooted at node $i \in \mathcal{N}$		
Λ_i^j	subtree rooted at node $i \in \mathcal{N}$ until level h_j for $j \in \Lambda_i$		
$\mathcal{P}_i$	path from the root node to node i		
Z_{ij}	$Z_{ij} := \sum_{k \in \mathcal{P}_i \cap \mathcal{P}_j} z_k$ common path impedances between nodes i and j		
	Power flow notations		
NPF	Nodal quantities of node $i \in \mathcal{N}$	LPF	ϵ-LPF
$\mathrm{sc}_i^{\mathrm{nom}}$	complex power demand at node i	$-$	$-$
sc_i	complex power consumed at node i	$\widehat{sc}_i$	$\breve{sc}_i$
sg_i	complex power generated at node i	$\widehat{sg}_i$	$\breve{sg}_i$
sp_i	complex power set-point of DER i	$\widehat{\mathrm{sp}}_i$	$\breve{\mathrm{sp}}_i$
V_i	complex voltage at node i	$\widehat{V}_i$	$\breve{V}_i$
ν_i	square of voltage magnitude at node i	$\widehat{\nu}_i$	$\breve{\nu}_i$
$\underline{\nu}_i, \overline{\nu}_i$	*soft* lower and upper bounds on square of voltage magnitude at node i		
NPF	Edge quantities of edge $(i,j) \in \mathcal{E}$	LPF	ϵ-LPF
S_j	complex power flowing on line (i,j)	$\widehat{S}_i$	$\breve{S}_i$
I_j	complex current flowing on line (i,j)	$\widehat{I}_i$	$\breve{I}_i$
ℓ_j	square of magnitude of current I_j	$\widehat{\ell}_i$	$\breve{\ell}_i$
x	$\mathrm{x} = (\nu, \ell, sc, sg, S)$ - state vector	$\widehat{\mathrm{x}}$	$\breve{\mathrm{x}}$
	Attacker model		
δ_i	$\delta_i = 1$ if DER i is compromised	$-$	$-$
$\mathrm{sp}_i^{\mathrm{a}}$	attacker set-point of DER i	$\widehat{\mathrm{sp}}_i^{\mathrm{a}}$	$\breve{\mathrm{sp}}_i^{\mathrm{a}}$
ψ	$\psi := (\mathrm{sp}^{\mathrm{a}}, \delta)$ attacker strategy	$\widehat{\psi}$	$\breve{\psi}$
	Defender model		
$\underline{\gamma}_i$	max. allowed fraction of load control	$-$	$-$
γ_i	fraction of load control at load i	$\widehat{\gamma}_i$	$\breve{\gamma}_i$
$\mathrm{sp}_i^{\mathrm{d}}$	defender set-point of DER i	$\widehat{\mathrm{sp}}_i^{\mathrm{d}}$	$\breve{\mathrm{sp}}_i^{\mathrm{d}}$
ϕ	$\phi := (\mathrm{sp}^{\mathrm{d}}, \gamma)$ defender strategy	$\widehat{\phi}$	$\breve{\phi}$

Table 3.1: Table of Notations.

3.3 Bilevel optimization problem

In this section, we consider the sub-game (Stages 2 and 3) induced by a fixed defender security strategy u in Stage 1:

$$[\mathrm{AD}] \quad \mathcal{L}^u := \max_{\psi\in\Psi} \min_{\phi\in\Phi} \mathrm{L}(\mathrm{x}(u,\psi,\phi)) \quad \text{s.t.} \quad (3.45)$$

Analogous to the variants of $[\mathrm{DAD}]$, $[\widehat{\mathrm{DAD}}]$ and $[\widetilde{\mathrm{DAD}}]$, we define two variants of the sub-game $[\mathrm{AD}]$: $[\widehat{\mathrm{AD}}]$ (resp. $[\widetilde{\mathrm{AD}}]$) with $\widehat{\mathcal{X}}$ (resp. $\breve{\mathcal{X}}$) in (3.45a). The optimal losses of $[\widehat{\mathrm{AD}}]$ and $[\widetilde{\mathrm{AD}}]$ are denoted by $\widehat{\mathcal{L}}^u$ and $\breve{\mathcal{L}}^u$), respectively.

For simplicity and *without loss of generality*, we focus on case for $u = \mathbf{0}$; i.e., no node is secured by the defender in Stage 1. With further abuse of notation, for a strategy profile $(\mathbf{0},\psi,\phi)$, we denote $\mathrm{x}(\mathbf{0},\psi,\phi)$ by $\mathrm{x}(\psi,\phi)$ as the solution of NPF model. Similarly, redefine $\widehat{\mathrm{x}}(\psi,\phi)$ and $\breve{\mathrm{x}}(\psi,\phi)$. We also drop the superscript u from $\mathcal{L}^u$, $\widehat{\mathcal{L}}^u$ and $\breve{\mathcal{L}}^u$.

Following the computational approach in the literature to solve (bilevel) interdiction problems [102], [72], we define the master-problem $[\mathrm{AD}]^{\mathrm{a}}$ (resp. sub-problem $[\mathrm{AD}]^{\mathrm{d}}$) for fixed $\phi \in \Phi$ (resp. fixed $\psi \in \Psi$):

$$\begin{aligned}
[\mathrm{AD}]^{\mathrm{a}} \quad & \psi^\star(\phi) \quad \in \operatorname{argmax}_{\psi\in\Psi} \quad \mathrm{L}(\mathrm{x}(\psi,\phi)) \quad \text{s.t.} \quad (3.45),\\
[\mathrm{AD}]^{\mathrm{d}} \quad & \phi^\star(\psi) \quad \in \operatorname{argmin}_{\phi\in\Phi} \quad \mathrm{L}(\mathrm{x}(\psi,\phi)) \quad \text{s.t.} \quad (3.45).
\end{aligned}$$

Similarly, define master- and sub- problems $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$ and $[\widehat{\mathrm{AD}}]^{\mathrm{d}}$ (resp. $[\widetilde{\mathrm{AD}}]^{\mathrm{a}}$ and $[\widetilde{\mathrm{AD}}]^{\mathrm{d}}$) for the variants $[\widehat{\mathrm{AD}}]$ (resp. $[\widetilde{\mathrm{AD}}]$).

Sec. 3.3 focuses on bounding the optimal loss for $[\mathrm{AD}]$ with the losses in $[\widehat{\mathrm{AD}}]$ and $[\widetilde{\mathrm{AD}}]$. The master- and sub- problems are addressed in Sec. 3.3 and Sec. 3.3, respectively. This leads to a computationally efficient iterative approach in Sec. 3.4 to solve the sub-games $[\mathrm{AD}]$, $[\widehat{\mathrm{AD}}]$, $[\widetilde{\mathrm{AD}}]$. Figure 3-2 provides an outline of results in this section.

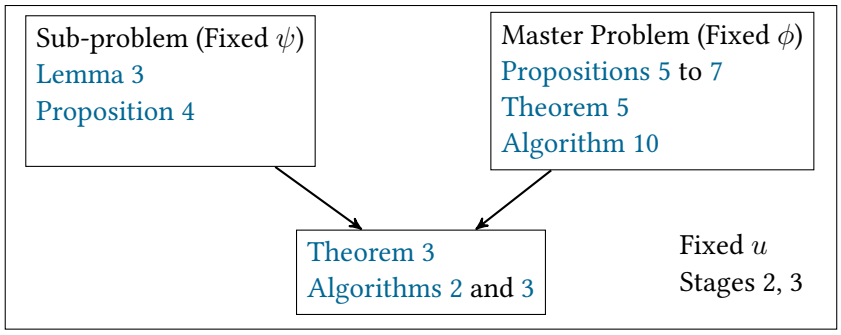


Figure 3-2: Outline of technical results in Sec. 3.6.

Upper and Lower Bounds on $\mathcal{L}$

Theorem 1. *Let* $(\psi^\star, \phi^\star)$, $(\widehat{\psi}^\star, \widehat{\phi}^\star)$ *and* $(\breve{\psi}^\star, \breve{\phi}^\star)$ *be optimal solutions to* [AD], $[\widehat{\text{AD}}]$ *and* $[\widetilde{\text{AD}}]$, *respectively; and denote the optimal losses by* $\mathcal{L}$, $\widehat{\mathcal{L}}$, $\breve{\mathcal{L}}$, *respectively. Then,*

$$\widehat{\mathcal{L}} \leqslant \mathcal{L} \leqslant \breve{\mathcal{L}} + \frac{\underline{\mu} N}{2\underline{\mu} + 4}. \tag{3.15}$$

To prove Theorem 1, we first state Lemmas 1 and 2, and Proposition 3 that relates $\mathrm{x}(\psi, \phi)$, $\widehat{\mathrm{x}}(\psi, \phi)$, and $\breve{\mathrm{x}}(\psi, \phi)$:

Lemma 1. *Consider a fixed* $(\psi, \phi) \in \Psi \times \Phi$. *The following holds:* $sc = \widehat{sc} = \breve{sc}$, $sg = \widehat{sg} = \breve{sg}$, *and*

$$\breve{S} = (1 + \epsilon)\widehat{S} \tag{3.16a}$$

$$\breve{\nu} - \nu_0 \mathbf{1}_N = (1 + \epsilon)(\widehat{\nu} - \nu_0 \mathbf{1}_N) \tag{3.16b}$$

$$\forall\ (i, j) \in \mathcal{E} \begin{cases} S_j = \sum_{k \in \Lambda_j} s_k + z_k \ell_k & \text{(3.17a)} \\ \widehat{S}_j = \sum_{k \in \Lambda_j} s_k & \text{(3.17b)} \end{cases}$$

$$\forall\ j \in \mathcal{N} \begin{cases} \widehat{\nu}_j = \nu_0 - 2 \sum_{k \in \mathcal{N}} \mathbf{Re}(\bar{Z}_{jk} s_k) & \text{(3.18a)} \\ \breve{\nu}_j = \nu_0 - 2(1 + \epsilon) \sum_{k \in \mathcal{N}} \mathbf{Re}(\bar{Z}_{jk} s_k) & \text{(3.18b)} \\ \widehat{\nu}_j = \nu_0 - 2 \sum_{k \in \mathcal{P}_j} \mathbf{Re}(\bar{z}_k \widehat{S}_k) & \text{(3.18c)} \\ \breve{\nu}_j = \nu_0 - 2 \sum_{k \in \mathcal{P}_j} \mathbf{Re}(\bar{z}_k \breve{S}_k). & \text{(3.18d)} \end{cases}$$

Lemma 2. *For a fixed* $(\psi, \phi) \in \Psi \times \Phi$,

$$\forall \quad (i,j) \in \mathcal{E}, \quad S_j \leqslant \frac{\widehat{S}_j}{(1-\epsilon_0)^{H-|\mathcal{P}_j|+1}}. \tag{3.19}$$

Proposition 3. *For a fixed strategy profile* $(\psi, \phi) \in \Psi \times \Phi$,

$$\widehat{S} \leqslant S \leqslant \breve{S}, \quad \widehat{\nu} \geqslant \nu \geqslant \breve{\nu}, \quad \widehat{\ell} \leqslant \ell \leqslant \breve{\ell}.$$

Hence,

$$\left.\begin{aligned} &\mathrm{L}_{VR}(\widehat{\mathrm{x}}) \leqslant \mathrm{L}_{VR}(\mathrm{x}) \leqslant \mathrm{L}_{VR}(\breve{\mathrm{x}}) \\ &\mathrm{L}_{\mathrm{LC}}(\widehat{\mathrm{x}}) = \mathrm{L}_{\mathrm{LC}}(\mathrm{x}) = \mathrm{L}_{\mathrm{LC}}(\breve{\mathrm{x}}) \\ &\mathrm{L}_{LL}(\widehat{\mathrm{x}}) \leqslant \mathrm{L}_{LL}(\widehat{\mathrm{x}}) \leqslant \mathrm{L}_{LL}(\breve{\mathrm{x}}) \end{aligned}\right\} \implies \mathrm{L}(\widehat{\mathrm{x}}) \leqslant \mathrm{L}(\mathrm{x}) \leqslant \mathrm{L}(\breve{\mathrm{x}}). \tag{3.20}$$

Proposition 3 implies that any attack ψ that increases $\widehat{\mathcal{L}}$ in $[\widehat{\mathrm{AD}}]$ (relative to the no attack case), also increases $\mathcal{L}$ in $[\mathrm{AD}]$ and $\breve{\mathcal{L}}$ in $[\widetilde{\mathrm{AD}}]$, respectively. The converse need not be true, i.e., an attack that increases $\mathcal{L}$ in $[\mathrm{AD}]$ (resp. $\breve{\mathcal{L}}$ in $[\widetilde{\mathrm{AD}}]$) need not increase $\widehat{\mathcal{L}}$ in $[\widehat{\mathrm{AD}}]$ (resp. $\mathcal{L}$ in $[\mathrm{AD}]$). Similarly, any defender response ϕ that reduces $\breve{\mathcal{L}}$ (resp. $\mathcal{L}$), also reduces $\mathcal{L}$ (resp. $\widehat{\mathcal{L}}$). Again, the converse statements do not apply here.

*Proof of **Theorem 1**.* For any $\mathrm{x} \in \mathcal{X}$,

$$\mathrm{L}_{\mathrm{LL}}(\mathrm{x}) \overset{(3.5c)}{=} \sum_{(i,j)\in\mathcal{E}} \frac{r_j(P_j^2+Q_j^2)}{\nu_i} \overset{\textbf{(A0)}_2,\textbf{(A0)}_4}{\leqslant} \frac{2}{\underline{\mu}} \sum_{(i,j)\in\mathcal{E}} r_j \overset{\textbf{(A0)}_4}{\leqslant} \frac{\underline{\mu} N}{2\underline{\mu}+4}. \tag{3.21}$$

Hence,

$$\begin{aligned} \breve{\mathcal{L}} &= \breve{\mathrm{L}}(\breve{\mathrm{x}}(\breve{\psi}^\star, \breve{\phi}^\star(\breve{\psi}^\star))) \\ &\geqslant \breve{\mathrm{L}}(\breve{\mathrm{x}}(\psi^\star, \breve{\phi}^\star(\psi^\star))) && \text{(by optimality of } \breve{\psi}^\star) \\ &\geqslant \breve{\mathrm{L}}(\mathrm{x}(\psi^\star, \breve{\phi}^\star(\psi^\star))) && \text{(by Proposition 3)} \\ &\overset{(3.21)}{\geqslant} \mathrm{L}(\mathrm{x}(\psi^\star, \breve{\phi}^\star(\psi^\star))) - \frac{\underline{\mu} N}{2\underline{\mu}+4} \end{aligned}$$

$$\geqslant \mathrm{L}(\mathrm{x}(\psi^\star, \phi^\star(\psi^\star))) - \frac{\underline{\mu} N}{2\underline{\mu} + 4} \quad \text{(by optimality of } \phi^\star\text{)}$$
$$= \mathcal{L} - \frac{\underline{\mu} N}{2\underline{\mu} + 4}.$$

Similarly, one can show $\mathcal{L} \geqslant \widehat{\mathcal{L}}$. □

Theorem 1 implies that the value of the sub-game $[\mathrm{AD}]$ with NPF can be lower (resp. upper) bounded by the value of $[\widehat{\mathrm{AD}}]$ (resp. $[\widetilde{\mathrm{AD}}]$). Our subsequent results show that both $[\widehat{\mathrm{AD}}]$ and $[\widetilde{\mathrm{AD}}]$ admit computationally efficient solutions.

Optimal defender response to fixed attacker strategy ψ

We consider the sub-problem $[\mathrm{AD}]^{\mathrm{d}}$ of computing optimal defender response $\phi^\star(\psi)$ for a fixed attack ψ.

The following Lemma shows that $[\mathrm{AD}]^{\mathrm{d}}$ is a Second-Order Cone Program (SOCP), and hence, can be solved efficiently.

Lemma 3. *Let $\mathcal{X}_{CPF} := conv(\mathcal{X})$ denote the set of states* x *satisfying (3.2)-(3.4), (3.5a), (3.5b), and the relaxation of (3.5c):*

For a fixed $\psi \in \Psi$, the problem of minimizing $\mathrm{L}(\mathrm{x}(\psi, \phi))$ *subject to* $\mathrm{x} \in \mathcal{X}_{CPF}$, *(3.8b), (3.8c) is a SOCP. Its optimal solution is also optimal for $[AD]^{\mathrm{d}}$.*

For fixed ψ (attack) and fixed load control parameter γ (e.g. when changing γ is not allowed), Proposition 4 below provides a range of optimal defender set-points $\widehat{\mathrm{sp}}^{d\star}$ and $\widetilde{\mathrm{sp}}^{d\star}$ for LPF and ϵ-LPF models, respectively. Note that, if γ is fixed, $\mathrm{L}_{\mathrm{LC}}(\hat{\mathrm{x}})$ is also fixed. Then, the defender set-points can be chosen by using $\mathrm{L}_{\mathrm{VR}}(\hat{\mathrm{x}})$ as a loss function, instead of $\widehat{\mathrm{L}}(\hat{\mathrm{x}})$. Similar argument holds for $\widetilde{\mathrm{L}}(\tilde{\mathrm{x}})$.

Proposition 4. *If we fix $\gamma \in \Gamma$ in $[\widehat{\mathrm{AD}}]^{\mathrm{d}}$, then $\forall i \in \mathcal{N}$,*

$$\delta_i = 0 \implies \left|\widehat{\mathrm{sp}}_i^{d\star}\right| = \overline{\mathrm{sp}}_i, \quad \angle \widehat{\mathrm{sp}}_i^{d\star} \in [\operatorname{arccot} \overline{K}, \operatorname{arccot} \underline{K}].$$

Furthermore, if the DN has identical $\boldsymbol{r}/\boldsymbol{x} \equiv K$ ratio, then

$$\delta_i = 0 \implies \left|\widehat{\mathrm{sp}}_i^{d\star}\right| = \overline{\mathrm{sp}}_i, \quad \angle \widehat{\mathrm{sp}}_i^{d\star} = \operatorname{arccot} K. \tag{3.22}$$

Similar results hold for $[\widetilde{\mathrm{AD}}]^{\mathrm{d}}$.

Optimal attack under fixed defender response ϕ

Now, we focus on the master problem $[\mathrm{AD}]^{\mathrm{a}}$, i.e., the problem of computing optimal attack for a fixed defender response ϕ. The following Theorem characterizes the optimal attacker set-point, denoted by $\mathrm{sp}_i^{a\star} = \mathbf{Re}(\mathrm{sp}_i^{a\star}) + \mathbf{jIm}(\mathrm{sp}_i^{a\star})$, when $\delta_i = 1$ (i.e. DER at node i is targeted by the attacker).

Theorem 2. *Consider* $[\mathrm{AD}]^{\mathrm{a}}$ *for a fixed* $\delta \in \mathcal{D}_k$ *(i.e., the DERs compromised by the attacker are specified by* δ *and the only decision variables in* $[\mathrm{AD}]^{\mathrm{a}}$ *are* sp^{a}*). Then*

$$\forall\ i \in \mathcal{N}\ \textit{s.t.}\ \delta_i = 1, \quad \mathrm{sp}_i^{a\star} = 0 - \boldsymbol{j}\overline{\mathrm{sp}}_i. \tag{3.23}$$

Same holds for both $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$ *and* $[\widetilde{\mathrm{AD}}]^{\mathrm{a}}$.

Proof. If $\delta_i = 1$, then $pg_i = \widehat{pg}_i = \mathbf{Re}(\mathrm{sp}_i) = \mathbf{Re}(\mathrm{sp}_i^{a\star})$.

We first prove the simpler case for $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$. From (3.6), one can check that as functions of $\widehat{pg}_i$, $\widehat{P}$ is strictly decreasing, $\widehat{Q}$ is constant, and $\widehat{\nu}$ is strictly increasing. Hence, $\widehat{\mathrm{L}}(\psi, \phi_f)$ is strictly increasing in $\widehat{pg}_i$ (because L_{VR} is non-decreasing as $\widehat{\nu}$ is decreasing; L_{LC} is constant). Hence, to minimize the loss L, the attacker chooses $\mathbf{Re}(\widehat{\mathrm{sp}}_i^{a\star}) = 0$. Similarly, $\mathbf{Im}(\widehat{\mathrm{sp}}_i^{a\star}) = -\mathbf{j}\overline{\mathrm{sp}}_i$. Similarly, we can show that in $[\widetilde{\mathrm{AD}}]^{\mathrm{a}}$, $\breve{\mathrm{sp}}^{a\star} = \mathbf{0} - \mathbf{j}\overline{\mathrm{sp}}$.

For the proof of $\mathrm{sp}^{\mathrm{a}\star} = \mathbf{0} - \mathbf{j}\overline{\mathrm{sp}}$, please refer to the supplementary material at the end of the document. □

Figure 3-3 shows the optimal attacker set-point $\mathrm{sp}_i^{a\star}$ for $\delta_i^\star = 1$, and the defender set-points for the DERs for $\delta_j^\star = 0$.

Thanks to Theorem 5, sc and sg are determined by δ and ϕ (since optimal $\mathrm{sp}^{\mathrm{a}\star}$ is given by (3.23)). Thus, for given (δ, ϕ), loss function can be denoted as $\mathrm{L}(\mathrm{x}(\left[\mathbf{0} - \mathbf{j}\overline{\mathrm{sp}}, \delta\right], \phi))$; and $[\mathrm{AD}]$ can be restated as follows:

$$\mathcal{L} \quad = \quad \max_{\delta \in \mathcal{D}_{\mathrm{k}}} \ \min_{\phi \in \Phi} \ \mathrm{L}(\mathrm{x}(\delta, \phi)) \quad \text{s.t.} \quad (3.45), (3.23).$$

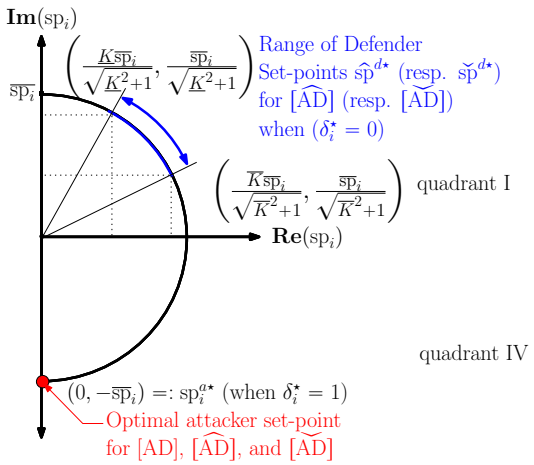


Figure 3-3: Optimal attacker set-points (Theorem 5) and range for optimal defender set-points (Proposition 4).

Same holds for $[\widehat{\mathrm{AD}}]$ (resp. $[\widetilde{\mathrm{AD}}]$) and $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$ (resp. $[\widetilde{\mathrm{AD}}]^{\mathrm{a}}$). Note that the attacker actions on DERs may not be limited to an incorrect set-point attack. For example, the attacker can simply choose to disconnect the DER nodes by choosing $\mathrm{sp}^{\mathrm{a}} = \mathbf{0} + \mathbf{0j}$. However, Theorem 5 shows that the attacker will induce more loss to the defender by causing the DERs to withdraw maximum reactive power rather than simply disconnecting them.

Let $\Delta_j(\widehat{\nu}_i)$ (resp. $\Delta_\delta(\widehat{\nu}_i)$) be the change in voltage at node i caused due to compromise of DER at node j (resp. compromise of DERs due to attack vector δ.) Similarly, define $\Delta_j(\breve{\nu}_i)$ and $\Delta_\delta(\breve{\nu}_i)$. We now state a useful result:

Lemma 4. *If ϕ is fixed, then*

$$\forall\, i,j \in \mathcal{N} \begin{cases} \Delta_j(\widehat{\nu}_i) = 2\mathbf{Re}(\bar{Z}_{ij}(\mathrm{sp}_j^{\mathrm{d}} + \boldsymbol{j}\overline{\mathrm{sp}}_j)) & \text{(3.24a)} \\ \Delta_j(\breve{\nu}_i) = 2(1+\epsilon)\mathbf{Re}(\bar{Z}_{ij}(\mathrm{sp}_j^{\mathrm{d}} + \boldsymbol{j}\overline{\mathrm{sp}}_j)) & \text{(3.24b)} \end{cases}$$

$$\forall\, \delta \subseteq \mathcal{D}_k \begin{cases} \Delta_\delta(\widehat{\nu}_i) = \sum_{j:\delta_j=1} \Delta_j(\widehat{\nu}_i) & \text{(3.25a)} \\ \Delta_\delta(\breve{\nu}_i) = \sum_{j:\delta_j=1} \Delta_j(\breve{\nu}_i). & \text{(3.25b)} \end{cases}$$

For a fixed $\phi \in \Phi$, let $\widehat{\mathcal{D}}_{\mathrm{k}}^i(\phi)$ be the set of optimal attack vectors that maximize voltage bounds violation under LPF at a pivot node, say i. Formally,

$$\widehat{\mathcal{D}}_{\mathrm{k}}^i(\phi) := \operatorname*{argmax}_{\delta \in \mathcal{D}_{\mathrm{k}}} W_i(\underline{\nu}_i - \widehat{\nu}_i) \;\text{ s.t. } \hat{\mathrm{x}}(\delta,\phi) \in \widehat{\mathcal{X}}, (3.8b), (3.8c) \tag{3.26}$$

Also, let

$$\widehat{\mathcal{D}}^{\star}_{\mathrm{k}}(\phi) := \bigcup_{i \in \mathcal{N}} \widehat{\mathcal{D}}^{i}_{\mathrm{k}}(\phi) \tag{3.27}$$

denote the set of candidate optimal attack vectors, and $\widehat{\delta}^{i} \in \widehat{\mathcal{D}}^{i}_{\mathrm{k}}(\phi)$ denote any vector in $\widehat{\mathcal{D}}^{i}_{\mathrm{k}}$. Similarly, define $\breve{\mathcal{D}}^{i}_{\mathrm{k}}(\phi)$, $\breve{\mathcal{D}}^{\star}_{\mathrm{k}}(\phi)$, and $\breve{\delta}^{i}$.

Using Lemma 4, Algorithm 10 computes optimal $\widehat{\delta}^{\star}$ to maximize L_{VR} for a fixed defender action $\phi \in \Phi$ [108]. In each iteration, the Algorithm selects one node as a pivot node. For a pivot node, say i, a set of target nodes $\widehat{\delta}^{i}$ is determined by selecting k nodes with largest $\Delta_j(\widehat{\nu}_i)$ (see Algorithm 5 in Appendix). Applying Lemma 4, the final nodal voltage at the current pivot node i is given by $\widehat{\nu}_i - \Delta_{\widehat{\delta}^i}(\widehat{\nu}_i)$. The attack strategy that maximizes L_{VR} is the set $\widehat{\delta}^{k}$ corresponding to a pivot node k that admits maximum voltage bound violation when DERs specified by $\widehat{\delta}^{k}$ are compromised. Algorithm 10 repeatedly calls procedure Algorithm 5, considering each node as the pivot node, and hence, requires $\mathcal{O}(n^2 \log n)$ time.

Algorithm 1 Optimal Attack for Fixed Defender Response

```
1: δ̂*(φ) ←OptimalAttackForFixedResponse(φ)
2: procedure OptimalAttackForFixedResponse(φ)
3:     Compute state vector for no attack x̂(0, φ) ∈ X̂
4:     for i ∈ N do
5:         δ̂^i ← GetPivotNodeOptimalAttack(i, sp^d), and calculate Δ_{δ̂^i}(ν̂_i) using Lemma. 4
6:         Calculate new voltage value ν̂'_i ← ν̂_i − Δ_{δ̂^i}(ν̂_i)
7:     end for
8:     k ← argmax_{i∈N} W_i(ν_i − ν̂'_i)
9:     return δ̂ ← δ̂^k (Pick δ̂^k which maximally violates (3.1))
10: end procedure
11: procedure GetPivotNodeOptimalAttack(i, sp^d)
12:     (J, N_{g^i}, m') ← OptimalAttackHelper(i, sp^d)
13:     Randomly choose k − m' nodes from N_{g^i} to form N'
14:     return δ̂^i ∈ D_k such that δ̂^i_k = 1 ⟺ k ∈ J ∪ N'
15: end procedure
```

The following proposition argues that Algorithm 10 computes the optimal attack vectors for $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$ and $[\widetilde{\mathrm{AD}}]^{\mathrm{a}}$.

Proposition 5. *For a fixed $\phi \in \Phi$, if $\widehat{\delta}$ is the optimal attack vector computed by Algorithm 10, then $\widehat{\delta}$ is also an optimal attack vector of $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$. Same holds for $[\widetilde{\mathrm{AD}}]^{\mathrm{a}}$.*

We now show that the effect of DER compromise at either node j or k on the node i depends upon the locations of nodes j and k relative to node i. The following Proposition states that if node j is upstream to node k relative to the pivot node i ($j \prec_i k$), then the DER compromise at node k impacts on $\widehat{\nu}_i$ more than the DER compromise on node j; and if $j =_i k$, then the effect of DER compromise at j, k on $\widehat{\nu}_i$ is identical.

Proposition 6. *[108] Consider* $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$. *Let nodes* $i, j, k \in \mathcal{N}$ *where* i *is the pivot node,* $\mathrm{sp}^{\mathrm{d}}_j = \mathrm{sp}^{\mathrm{d}}_k$, *and* $\overline{\mathrm{sp}}_j = \overline{\mathrm{sp}}_k$. *If* $j \prec_i k$ *(resp.* $j =_i k$*), then* $\Delta_j(\widehat{\nu}_i) < \Delta_k(\widehat{\nu}_i)$ *(resp.* $\Delta_j(\widehat{\nu}_i) = \Delta_k(\widehat{\nu}_i)$*). Same holds true for* $[\widetilde{\mathrm{AD}}]^{\mathrm{a}}$.

Proposition 6 implies that, broadly speaking, compromising downstream DERs is advantageous to the attacker than compromising the upstream DERs. In other words, compromising DERs by means of clustered attacks are more beneficial to the attacker than distributed attacks. Consequently, our results (see Sec. 3.5) on security strategy in Stage 1 show that the defender should utilize his security strategy to deter cluster attacks.

We, now, state a result that connects the optimal attack strategies for $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$ and $[\widetilde{\mathrm{AD}}]^{\mathrm{a}}$.

Proposition 7. *For a fixed* $\phi \in \Phi$, *the following holds:*

1) The sets of candidate optimal attack vectors that maximizes voltage bound violations under LPF and ϵ*-LPF are identical, i.e.,*

$$\widehat{\mathcal{D}}^{\star}_k(\phi) \equiv \widetilde{\mathcal{D}}^{\star}_k(\phi). \tag{3.28}$$

2) Furthermore, assume that $\underline{\nu}_i = \underline{\nu}_j =: \underline{\nu}$ *and* $W_i = W_j =: W \ \forall\ i, j \in \mathcal{N}$. *Also, let the sets of optimal attack strategies for* $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$ *and* $[\widetilde{\mathrm{AD}}]^{\mathrm{a}}$ *be denoted by* $\widehat{\Psi}^{\star}_k(\phi)$ *and* $\widetilde{\Psi}^{\star}_k(\phi)$, *respectively. Let* $\widehat{\psi}^{\star} \in \widehat{\Psi}^{\star}_k(\phi)$ *and* $\widetilde{\psi}^{\star} \in \widetilde{\Psi}^{\star}_k(\phi)$ *be any two attack strategies. Now, if*

$$\mathrm{L}_{VR}(\widehat{\mathrm{x}}(\widehat{\psi}^{\star}, \phi)) > 0 \quad \textit{and} \quad \mathrm{L}_{VR}(\widetilde{\mathrm{x}}(\widetilde{\psi}^{\star}, \phi)) > 0, \tag{3.29}$$

then the sets of optimal attack strategies for $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$ *and* $[\widetilde{\mathrm{AD}}]^{\mathrm{a}}$ *are identical, i.e.,*

$$\widehat{\Psi}^{\star}_k(\phi) \equiv \widetilde{\Psi}^{\star}_k(\phi). \tag{3.30}$$

As we will see in Sec. 3.4, Proposition 7 forms the basis of our overall computational approach.

3.4 Greedy solution approach

We now utilize results for sub- and master-problems to solve $[\mathrm{AD}]$. Consider the following assumption:

(A1) DN has identical $\mathbf{r}/\mathbf{x} \equiv K$ ratio, i.e., $\forall j \in \mathcal{N}, K_j = K$. In this subsection, we present an algorithm to solve $[\widehat{\mathrm{AD}}]$ and $[\widetilde{\mathrm{AD}}]$ under **(A0)** and **(A1)**, and then propose its extension, a greedy iterative approach, for solving $[\mathrm{AD}]$ under the general case.

Under **(A0)** and **(A1)**, the optimal defender set-points $\widehat{\mathrm{sp}}^{\mathrm{d}\star}$ and $\widetilde{\mathrm{sp}}^{\mathrm{d}\star}$ are as specified by Proposition 4, and hence fixed. For fixed optimal $\widehat{\mathrm{sp}}^{\mathrm{d}\star}$ (resp. $\widetilde{\mathrm{sp}}^{\mathrm{d}\star}$), we can solve the problem $[\widehat{\mathrm{AD}}]$ (resp. $[\widetilde{\mathrm{AD}}]$) by using Benders Cut method [72]. However, we present a computationally faster algorithm, Algorithm 2 that computes attacker's candidate optimal attack vectors $\widehat{\mathcal{D}}^{\star}_{\mathrm{k}}$ (resp. $\widetilde{\mathcal{D}}^{\star}_{\mathrm{k}}$) using Lemma 4.

Lemma 5. *Under **(A0)**, **(A1)**, for any two fixed $\widehat{\gamma}^1, \widehat{\gamma}^2 \in \Gamma$, $\widehat{\mathcal{D}}^{\star}_{k}(\left[\widehat{\mathrm{sp}}^{\mathrm{d}\star}, \widehat{\gamma}^1\right]) = \widehat{\mathcal{D}}^{\star}_{k}(\left[\widehat{\mathrm{sp}}^{\mathrm{d}\star}, \widehat{\gamma}^2\right])$. Same holds true for $\widetilde{\mathcal{D}}^{\star}_{k}$.*

Given $\widehat{\mathrm{sp}}^{\mathrm{d}} \in \mathcal{S}$, it can be checked that Algorithm 2, in fact, computes $\widehat{\mathcal{D}}^{i}_{\mathrm{k}}(\widehat{\mathrm{sp}}^{\mathrm{d}})$, and $\widehat{\mathcal{D}}^{\star}_{\mathrm{k}}(\widehat{\mathrm{sp}}^{\mathrm{d}}) = \bigcup_{i\in\mathcal{N}} \widehat{\mathcal{D}}^{i}_{\mathrm{k}}(\widehat{\mathrm{sp}}^{\mathrm{d}})$ is the set of candidate optimal attack vectors. The cardinality of the set $\widehat{\mathcal{D}}^{i}_{\mathrm{k}}$ (Line 4) in the worst-case can be as high as $\mathcal{O}(e^{\frac{n}{e}})$. Therefore, computing $\widehat{\mathcal{D}}^{\star}_{\mathrm{k}}$ can take $\mathcal{O}(n \exp{(\frac{n}{e})})$ time in the worst-case.

Algorithm 2 computes the set of attacks $\widehat{\mathcal{D}}^{\star}_{\mathrm{k}}(\widehat{\mathrm{sp}}^{\mathrm{d}\star})$, and iterates over each $\widehat{\delta} \in \widehat{\mathcal{D}}^{\star}_{\mathrm{k}}(\widehat{\mathrm{sp}}^{\mathrm{d}\star})$. In each iteration, since $\mathrm{sp}^{\mathrm{d}} = \widehat{\mathrm{sp}}^{\mathrm{d}\star}$ is fixed, the sub-problem $[\widehat{\mathrm{AD}}]^{\mathrm{d}}$ reduces to an LP over the variable γ. Let $\widehat{\gamma}^{\star}(\widehat{\delta})$ be the solution to the LP. Then, $\widehat{\phi}^{\star}(\widehat{\delta}) = \left[\widehat{\mathrm{sp}}^{\mathrm{d}\star}, \widehat{\gamma}^{\star}(\widehat{\delta})\right]$ is the optimal solution to $[\widehat{\mathrm{AD}}]^{\mathrm{d}}$. Choosing $\widehat{\delta}^{\star} = \mathrm{argmax}_{\widehat{\delta}\in\widehat{\mathcal{D}}^{\star}_{\mathrm{k}}} \mathrm{L}(\widehat{\mathrm{x}}(\widehat{\delta}, \widehat{\phi}^{\star}(\widehat{\delta})))$, Algorithm 2 computes the solution to be $(\widehat{\delta}^{\star}, \widehat{\phi}^{\star}(\widehat{\delta}^{\star}))$ to the problem $[\widehat{\mathrm{AD}}]$. Similarly, we can use Algorithm 2 to solve $[\widetilde{\mathrm{AD}}]$.

Theorem 3. *Under **(A0)**, **(A1)**, let $(\widehat{\delta}, \widehat{\phi})$ be a solution computed by Algorithm 2. Then $(\widehat{\delta}, \widehat{\phi})$ is also an optimal solution to $[\widehat{\mathrm{AD}}]$. Similar result holds for $[\widetilde{\mathrm{AD}}]$.*

Algorithm 2 Solution to $\widehat{[\mathrm{AD}]}$ for DNs with identical $\mathbf{r}/\mathbf{x}$

$(\widehat{\delta}^\star, \widehat{\phi}^\star, \widehat{\mathcal{L}}) \leftarrow$ GREEDY-ONE-SHOT()
procedure GREEDY-ONE-SHOT()
  $\widehat{\mathcal{L}} = 0$, $\widehat{\delta}^\star = \mathbf{0}$, $\widehat{\gamma}^\star = \mathbf{1}$, $\widehat{\mathrm{sp}}^{\mathrm{d}\star}$ as in Proposition 4
  Let $\widehat{\mathcal{D}}^i_{\mathrm{k}} =$ GETPIVOTNODEOPTIMALATTACKSET$(i, \widehat{\mathrm{sp}}^{\mathrm{d}\star})$
  $\widehat{\mathcal{D}}^\star_{\mathrm{k}} = \bigcup_{i\in\mathcal{N}} \widehat{\mathcal{D}}^i_{\mathrm{k}}$
  For each $\widehat{\delta} \in \widehat{\mathcal{D}}^\star_{\mathrm{k}}$, compute $\widehat{\gamma}^\star(\widehat{\delta})$ by solving $\widehat{[\mathrm{AD}]}^{\mathrm{d}}$ as an LP in γ. Let $\widehat{\phi}^\star(\widehat{\delta}) = \widehat{\mathrm{sp}}^{\mathrm{d}\star}, \widehat{\gamma}^\star(\delta)))$
  Let $\widehat{\delta}^\star := \underset{\widehat{\delta}\in\widehat{\mathcal{D}}^\star_{\mathrm{k}}}{\operatorname{argmax}} \widehat{\mathrm{L}}(\hat{\mathrm{x}}(\widehat{\delta}, \widehat{\gamma}^\star(\widehat{\delta}), \widehat{\mathrm{sp}}^{\mathrm{d}\star}))$
  return $\widehat{\delta}^\star, \widehat{\phi}^\star = \widehat{\phi}^\star(\widehat{\delta}^\star), \widehat{\mathcal{L}} = \widehat{\mathrm{L}}(\hat{\mathrm{x}}(\widehat{\delta}^\star, \widehat{\phi}^\star))$
end procedure
procedure GETPIVOTNODEOPTIMALATTACKSET$(i, \mathrm{sp}^{\mathrm{d}})$
  $(J, \mathcal{N}_{g^i}, m') \leftarrow$ OPTIMALATTACKHELPER$(i, \mathrm{sp}^{\mathrm{d}})$
  return $\mathcal{D}^i_{\mathrm{k}} \leftarrow \{\widehat{\delta} \in \mathcal{D}_{\mathrm{k}} | \widehat{\delta}_k = 1 \text{ iff } k \in J \cup \mathcal{N}',$ where $\mathcal{N}' \subseteq \mathcal{N}_{g^i}$ and $|\mathcal{N}'| = M - m'\}$
end procedure

Proof. Under **(A1)**, $\mathrm{sp}^{\mathrm{d}} = \widehat{\mathrm{sp}}^{\mathrm{d}\star}$ is fixed (Proposition 4). Then, for any $\gamma \in \Gamma$, by Lemma 5 and Proposition 5, the optimal attack $\widehat{\delta}^\star$ belongs to the set $\widehat{\mathcal{D}}^\star_{\mathrm{k}}(\widehat{\mathrm{sp}}^{\mathrm{d}\star})$. Algorithm 2 iterates over the attack vectors $\delta \in \widehat{\mathcal{D}}^\star_{\mathrm{k}}$, computes $\widehat{\gamma}^\star(\delta)$ by solving an LP, and calculates the loss $\widehat{\mathrm{L}}(\hat{\mathrm{x}}(\delta, \widehat{\phi}^\star(\delta)))$. Finally, it returns the solution corresponding to the maximum loss. Similar logic applies for optimal solution of $\widehat{[\mathrm{AD}]}$. □

We, now, describe an iterative greedy approach to compute the solution to $[\mathrm{AD}]$ that uses the optimal attacker strategy for fixed defender response (refer Algorithm 10).

Algorithm 3 initializes ϕ_c to the optimal defender response under no attack. In the first step of the iterative approach, the attacker assumes some defender response ϕ_c to be fixed, and computes the optimal attack strategy $\delta_c(\phi_c)$ using the greedy Algorithm 10. Then in the second step, the defender computes a new defense strategy ϕ_c optimal for fixed δ_c by solving the SOCP, and updates the defender response. If $\mathrm{L}(\mathrm{x}(\delta_c, \phi_c)) > \mathrm{L}(\mathrm{x}(\delta^\star, \phi^\star))$, then the current best solution $(\delta^\star, \phi^\star)$ is updated to (δ_c, ϕ_c). Then in the next iteration, the attacker uses this new defender response to update his attack strategy, and so on and so forth. If this δ_c has already been discovered in some previous iteration, the algorithm terminates successfully, with $\delta^\star, \phi^\star$ as the required optimal attack plan, and the corresponding optimal defense. The algorithm terminates unsuccessfully if the number of iterations exceeds a maximum limit.

Algorithm 3 Iterative Algorithm for Greedy Approach

$(\delta^\star, \phi^\star, \mathcal{L}) \leftarrow$ GREEDY-ITERATIVE()
procedure GREEDY-ITERATIVE
  Let $\delta^\star \leftarrow \mathbf{0}, \mathcal{L}^\star \leftarrow 0, \delta_c \leftarrow \mathbf{0}, iter \leftarrow 0, \Upsilon \leftarrow \varnothing, \phi_c, \phi^\star, \Upsilon$
  For $\delta = \delta_c$, compute $\phi^\star$ by solving SOCP $[\mathrm{AD}]^{\mathrm{d}}$ (Lemma 3)
  $\phi_c \leftarrow \phi^\star, \mathcal{L}^\star \leftarrow \mathrm{L}(\tilde{\mathrm{x}}(\delta, \phi^\star))$
  for $iter \leftarrow 0, 1, \ldots, maxIter$ **do**
    $\delta_c \leftarrow$ OPTIMALATTACKFORFIXEDRESPONSE(ϕ_c)
    ▷ If δ_c previously found, successfully terminate
    if $\delta_c \in \Upsilon$ **then return** $\delta^\star, \phi^\star$
    else $\Upsilon = \Upsilon \cup \{\delta_c\}$ ▷ Store the current best attack vector
    Compute ϕ_c by solving SOCP $[\mathrm{AD}]^{\mathrm{d}}$ Lemma 3
    if $\mathrm{L}(\tilde{\mathrm{x}}(\delta_c, \phi_c)) > \mathcal{L}^\star$ **then**
      $\delta^\star \leftarrow \delta_c, \phi^\star \leftarrow \phi_c, \mathcal{L}^\star \leftarrow \mathrm{L}(\tilde{\mathrm{x}}(\delta, \phi^\star))$
    end if
  end for ▷ Maximum Iteration Limit reached
  Return $\delta^\star, \phi^\star, \mathcal{L}^\star$ ▷ Return the last best solution
end procedure ▷ Algo terminates unsuccessfully

Note that in each iteration, the size of Υ increases by 1, hence, the algorithm is bound to terminate after exhausting all possible attack vectors.

Proposition 7 and Theorem 3 can be applied for any $u \in \mathcal{U}_B$, since if the DN has identical $\mathbf{r}/\mathbf{x}$ ratio, sp^{d} are also fixed.

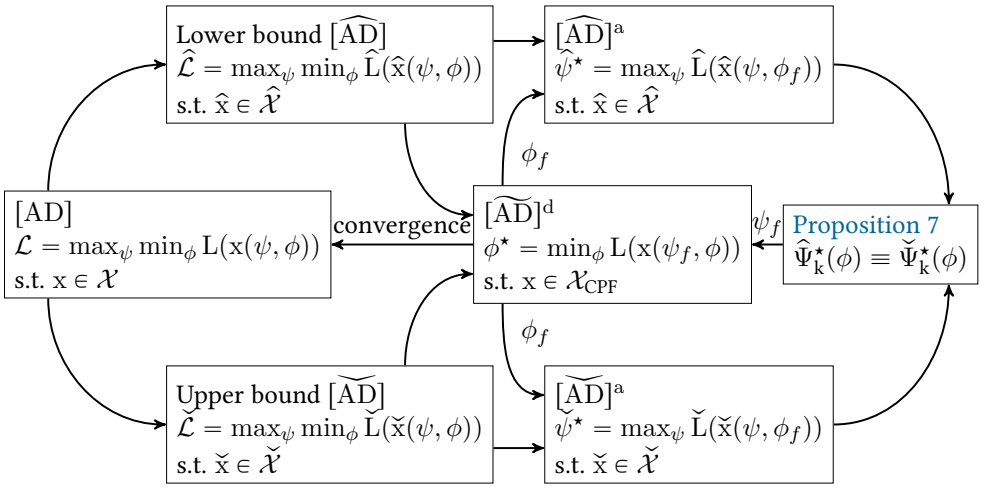


Figure 3-4: Overall computational approach.

Our overall computational approach to solving the problem $[\mathrm{AD}]$, thus far, can be summarized as in Figure 3-4. Given an instance of the problem $[\mathrm{AD}]$, we first solve the problems $\widehat{[\mathrm{AD}]}$ and $\widetilde{[\mathrm{AD}]}$. For this, we employ an iterative procedure that iterates be-

tween the master- and sub- problems. For a fixed attacker action we determine the optimal defender response ϕ for the $[\mathrm{AD}]^{\mathrm{d}}$ using the convex relaxation of (3.5c). Then, for the fixed defender response ϕ, we compute the optimal attacker strategies $\widehat{\psi}^{\star}$ and $\breve{\psi}^{\star}$ by solving $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$ and $[\widetilde{\mathrm{AD}}]^{\mathrm{a}}$, respectively. Proposition 7 provides us an useful result that $\psi^{\star}(\phi) := \widehat{\psi}^{\star} = \breve{\psi}^{\star}$. This optimal attacker strategy $\psi^{\star}(\phi)$ is then fed back to the master-problem $[\mathrm{AD}]^{\mathrm{a}}$. This procedure is repeated until we reach a convergence or we exceed the maximum iteration limit.

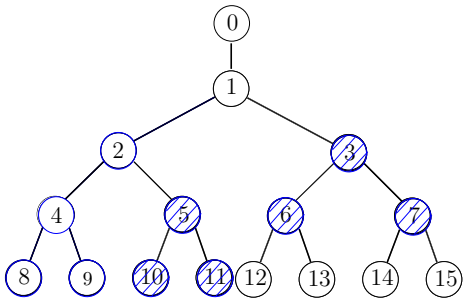
3.5 Security investments in customer-side devices

In this section, we consider the defender problem of optimal security investment in Stage 1. For simplicity, we restrict our attention to DNs that satisfy the following assumption:

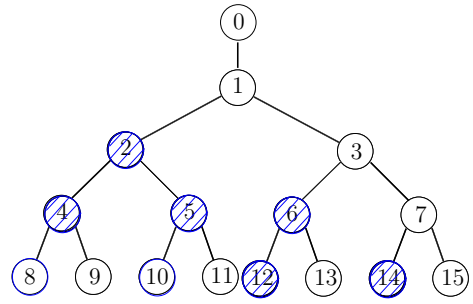
(A2) Symmetric Network. For every $i \in \mathcal{N}$, for any two nodes $j, k \in \mathcal{N}_i^c$, Λ_j and Λ_k are symmetrically identical about node i. That is, $z_j = z_k$, $\left|\mathcal{N}_j^c\right| = |\mathcal{N}_k^c|$, $\mathrm{sc}_j^{\mathrm{nom}} = \mathrm{sc}_k^{\mathrm{nom}}$, $\underline{\nu}_j = \underline{\nu}_k$, $W_j = W_k$, and $C_j = C_k$. However, all the DERs are homogeneous, i.e., $\forall\ j, k \in \mathcal{N}$, $\overline{\mathrm{sp}}_j = \overline{\mathrm{sp}}_k$.

Let B be a fixed security budget. Let $u, \widetilde{u} \in \mathcal{U}_B$, $u \neq \widetilde{u}$, be two security strategies. Strategy u is *more secure* than strategy $\widetilde{u}$ (denoted by $u \preccurlyeq \widetilde{u}$) under NPF (resp. LPF), if $\mathcal{L}^u \leqslant \mathcal{L}^{\widetilde{u}}$ (resp. $\widehat{\mathcal{L}}^u \leqslant \widehat{\mathcal{L}}^{\widetilde{u}}$). Finally, we ask what is the best security strategy $u^{\star}$, such that for $u = u^{\star}$, $\mathcal{L}^u$ is minimized. Figure 3-5 shows two possible security strategies u^1 (Figure 3-5a) and u^2 (Figure 3-5b), and gives a generic security strategy (Figure 3-5c). If we compare u^1 and u^2, while transitioning from u^1 to strategy u^2, 3 secure nodes in Λ_2 subtree go up a level each, while 3 secure nodes in Λ_3 subtree go down a level each. Then, between u^1 and u^2, which strategy is more secure? In this section, we provide insights about optimal security strategies under **(A2)**, which help show that u^2 is more secure than u^1.

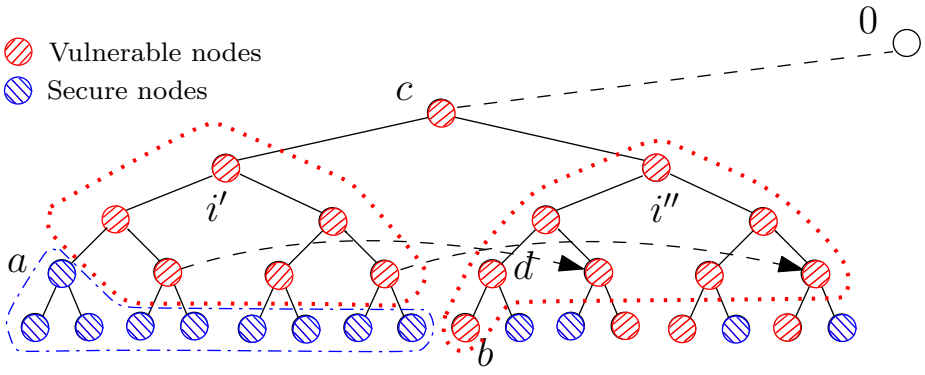
Algorithm 4 computes an optimal security strategy $[\widehat{\mathrm{DAD}}]$ under **(A0)**-**(A2)**. It initially assigns all nodes to be vulnerable. Then, DER nodes are secured sequentially in a bottom-up manner towards the root node. If the security budget is not adequate to secure a full level, the nodes in that level are uniformly secured and the remaining nodes are not secured. Under all the assumptions of Algorithm 4, it takes $\mathcal{O}(n)$ time.



(a) Security strategy u^1. $\mathcal{N}_s(u^1) = \{3, 5, 6, 7, 10, 11\}$.



(b) Security strategy u^2. $\mathcal{N}_s(u^2) = \{2, 4, 5, 6, 12, 14\}$.



(c) A generic security strategy on a tree DN.

Figure 3-5: Different defender security strategies.

Algorithm 4 Optimal security strategy

$\widehat{u}^\star \leftarrow$ OptimalSecurityStrategy()
procedure OptimalSecurityStrategy()
  $n_s \leftarrow 0, h \leftarrow H, \widehat{u} \leftarrow \mathbf{0}$ ▷ Initialize all nodes to vulnerable nodes
  For each $h \in [1, 2, \ldots, H]$, let $\alpha_h \leftarrow \sum_{j=h}^{H} |\mathcal{N}_j|$
  Let $h' \leftarrow \operatorname{argmax}_{h \in [1,\ldots,H]: \alpha_h \geqslant M} h$
  Let $\forall\ h \in [h', \ldots, H], \forall\ i \in \mathcal{N}_h, \widehat{u}_i \leftarrow 1$.
  Let $\mathcal{N}'_{h'} \subseteq \mathcal{N}_{h'}$ be a set of uniformly chosen $M - \alpha_{h'+1}$ nodes on level h'.
  For each $i \in \mathcal{N}'_{h'}, \widehat{u}_i \leftarrow 1$
  return $\widehat{u}$
end procedure

In the following theorem, we show that the security strategy computed by Algorithm 4 is an optimal solution to the Stage 1 of the $[\widehat{\text{DAD}}]$ and $[\widetilde{\text{DAD}}]$ problem.

Theorem 4. *Assume (A0), (A1), (A2). Let $\widehat{u}^\star$ be the security strategy computed by Algorithm 4. Furthermore, with $u = \widehat{u}^\star$, let $(\widehat{\psi}^\star, \widehat{\phi}^\star)$ be the solution computed by Algorithm 2. Then, $(\widehat{u}^\star, \widehat{\psi}^\star, \widehat{\phi}^\star)$ is an optimal solution to $[\widehat{\text{DAD}}]$. Similar result holds for $[\widetilde{\text{DAD}}]$.*

Finally, we state the following result:

Proposition 8. *1) Under **(A0)**, **(A1)**, **(A2)**, $\widehat{\mathcal{D}}_k^\star$ can be partitioned into at most N equivalence classes of attack vectors, one for each vulnerable node considered as pivot node. Any two attack vectors in the same equivalence class has identical impact on the corresponding pivot node. Additionally, any two equivalence classes can be considered homomorphic transformations of each other.*

*2) Under **(A0)**, **(A1)**, if $\forall\ i, j, k \in \mathcal{N}$ such that $\overline{\mathrm{sp}}_j > 0$ and $\overline{\mathrm{sp}}_k > 0$, $\Delta_j(\widehat{\nu}_i) \neq \Delta_k(\widehat{\nu}_i)$, then $\left|\widehat{\mathcal{D}}_k^\star\right| \leqslant |N|$, i.e., if for any pivot node, no two DERs have identical impact on the pivot node due to their individual DER compromises, then each equivalence class is a singleton set, and hence, the set for candidate optimal attack vectors is at most of size $|N|$.*

By Theorem 4, we can compute the optimal security investment $\widehat{\delta}^\star$ in $\mathcal{O}(N)$, and by Proposition 8, for fixed $\widehat{\delta}^\star$, we can compute the optimal attacker strategy $\widehat{\psi}^\star$ in $\mathcal{O}(N)$. Finally, for fixed $\widehat{\delta}^\star$ and $\widehat{\psi}^\star$, we can compute the optimal defender response $\widehat{\phi}^\star$ in $\mathcal{O}(poly(N))$. Hence, we can compute the optimal solution for $[\widehat{\mathrm{DAD}}]$, in $\mathcal{O}(poly(N))$. Same holds for $[\widetilde{\mathrm{DAD}}]$.

Admittedly, our structural results on optimal security investment in Stage 1 of the game are specific to assumption **(A2)**. Future work involves extending these results to a general radial DN with heterogeneous DER nodes. A key aspect in effort will be to understand how the defender's net value of securing an individual DER node depends on its capacity and location in the DN.

Computational Study

We describe a set of computational experiments to evaluate the performance of the iterative Greedy Approach (GA) in solving $[\mathrm{AD}]$; see Algorithm 3. We again assume $u = \mathbf{0}$. We compare the optimal attack strategies and optimal defender set-points obtained from GA with the corresponding solutions obtained by conducting an exhaustive search (or Brute Force (BF)), and by implementing the Benders Cut (BC) algorithm. We refer the reader to [102], [72], for the BC algorithm adopted here. The abbreviations BC-LPF and BC-NPF denote the solutions obtained by applying optimal attack strategies from $[\widehat{\mathrm{AD}}]$ to

LPF and NPF, respectively. Importantly, the experiments illustrate the impact of attacker's resource (k) and defender's load control capability $\underline{\gamma}$ on the optimal value of [AD]. The code for this computational study can be obtained by contacting the authors.

Network Description

Our prototypical DN is a modified IEEE 37-node network; see Figure 3-6. We consider two variants of this network: homogeneous and heterogeneous. **Homogeneous Network ($\mathcal{G}^I$)** has 14 homogeneous DERs with randomly assigned node locations, loads with equal nominal demand, and lines with identical $\mathbf{r}/\mathbf{x}$ ratio. Each line has impedance of $z_j = (0.33 + 0.38\mathbf{j})\ \Omega$. The nominal demand at each node i is $\mathrm{sc}_i^{\mathrm{nom}} = 15\ kW + \mathbf{j}4.5\ kvar$. The apparent power capability of each DER node i is $\overline{\mathrm{sp}}_i = 11.55\ kVA$. The nominal voltage at node 0 is $|V_0| = 4\ kV$. The cost of load control is $C = 7$ \$ per kW. **Heterogeneous Network ($\mathcal{G}^H$)** has same topology as $\mathcal{G}^I$, but has heterogeneous DERs (chosen at random from 3 different DER apparent power capabilities), heterogeneous loads, and lines with different $\mathbf{r}/\mathbf{x}$ ratios. The locations of DER nodes, the total nominal generation capacity, and the total nominal demand in $\mathcal{G}^H$ is roughly similar to the corresponding values for $\mathcal{G}^I$.

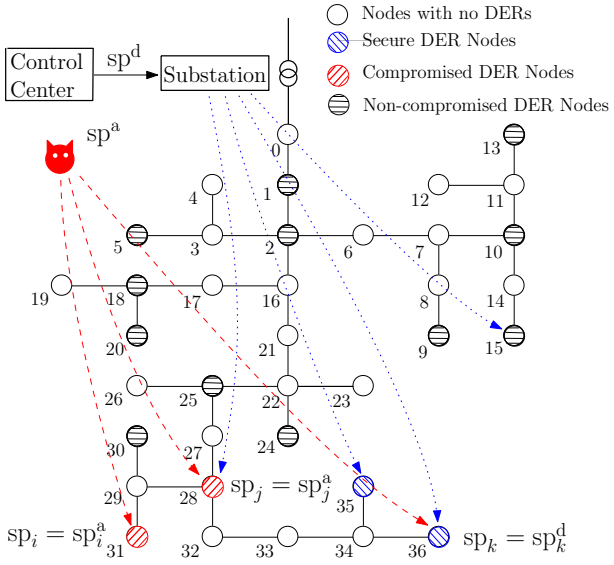
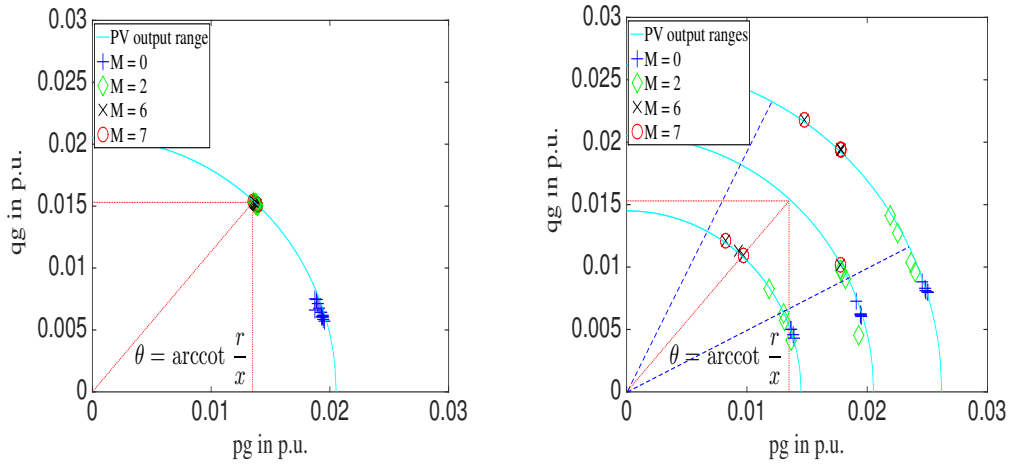


Figure 3-6: Illustration of the DER failure scenario proposed in [98] on a modified IEEE 37-node network.

DER output vs k. Figure 3-7 compares the DER output (sg) of uncompromised DERs

that form part of defender response in $\mathcal{G}^I$ and $\mathcal{G}^H$ for different k. When $\mathrm{k} = 0$ (no attack), there are no voltage violations, and the defender minimizes $\mathrm{L_{LL}}$, which results in $pg > qg$. For $\mathrm{k} > 0$, the voltage bounds may be violated. To limit $\mathrm{L_{VR}}$, the defender responds by increasing qg; and the output of uncompromised DERs lie in a neighborhood of $\theta = \operatorname{arccot} \mathbf{r}/\mathbf{x}$. For the case of $\mathcal{G}^H$ (Figure 3-7b), the set-points of the uncompromised DERs are more spread out to achieve voltage regulation over different $\mathbf{r}/\mathbf{x}$ ratios (Proposition 4). In Figure 3-7b the three semi-circles correspond to the uncompromised DERs with different apparent power capabilities. These observations on the defender response validate Proposition 4.



(a) Homogeneous network.

(b) Heterogeneous network.

Figure 3-7: Reactive power vs Real power output of DERs.

GA *vs.* BC-NPF, BC-LPF and BF. Figure 3-8 compares results obtained from *BC-NPF*, *GA*, and *BF* on $\mathcal{G}^I$. We consider two cases with the maximum controllable load percentage $\underline{\gamma} = 50\ \%$ and $\underline{\gamma} = 70\ \%$. For each case, we vary k from 0 to $|\mathcal{N}_v| = 14$; and also vary $\mathbf{w}/\mathrm{c}$ ratios to capture the effect of different weights on the terms $\mathrm{L_{VR}}$ and $\mathrm{L_{LC}}$.

In our study, we chose $C_i = 7\ cents/kWh$, converted appropriately to the per unit system. [6] The ratio $\mathbf{w}/\mathrm{c} = 2$ roughly corresponds to the maximum W/C ratio for which the

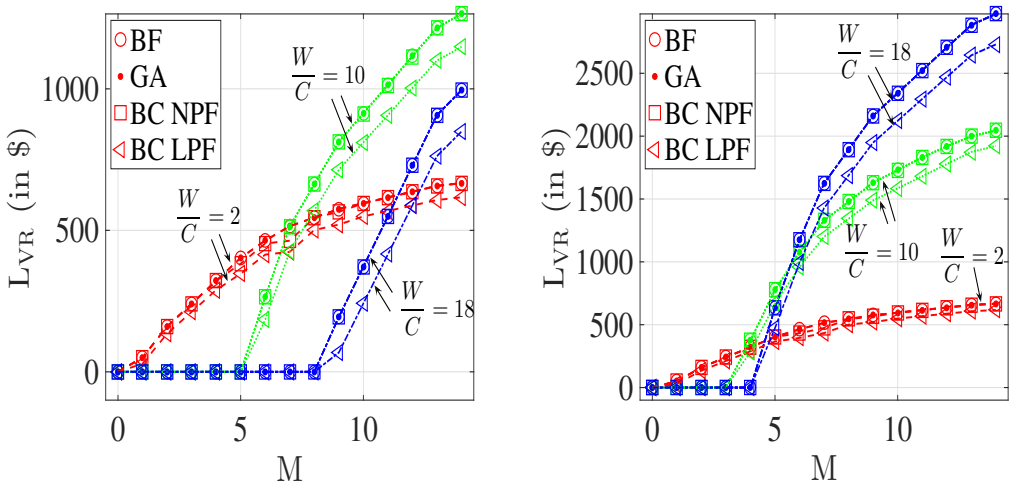
[6] From a practical viewpoint, the weights C_i can be obtained from the operator's rate compensation scheme for load control. For example, North Star Electric [96] provides a compensation of $9.1\ cents$ to their customers for $1\ kWh$ of load curtailment. One can argue that the net cost of shedding unit load should be adjusted to reflect the fact that the defender supplies additional power during the attack to meet the consumers' demand.

defender does not exercise load control, because the cost of doing load control is too high, i.e., at optimum defender response $\gamma^\star = \mathbf{1}_N$. In contrast, $\mathbf{W}/\mathbf{C} = 18$ roughly corresponds to the minimum W/C ratio for which the defender exercises maximum load control (i.e. $\gamma^\star = \underline{\gamma}$). We also consider an intermediate ratio, $\mathbf{W}/\mathbf{C} = 10$.

L *versus* k. Both $\mathrm{L_{VR}}$ and $\mathrm{L_{LC}}$ are zero when there is no attack. As k increases, one or both $\mathrm{L_{VR}}$ and $\mathrm{L_{LC}}$ start increasing. This indicates that as more DERs are compromised, the defender incurs $\mathrm{L_{VR}}$, and in addition, he imposes load control to better regulate the DN. Indeed, after the false set-points (Theorem 5) are used to compromise DERs, the net load in the DN increases. Without load control, the voltages at some nodes drop below the lower bounds, increasing $\mathrm{L_{VR}}$. Hence, the defender exercises load control, and changes the set-points of uncompromised DERs to limit the total loss.

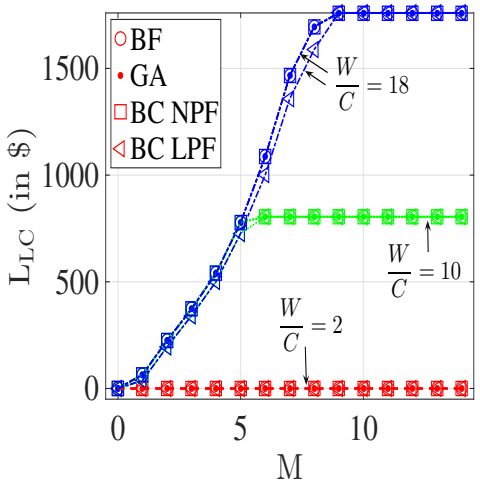
Perhaps a more interesting observation is that as k increases, $\mathrm{L_{LC}}$ first increases rapidly but then flattens out (Figures 3-8c and 3-8d). This can be explained as follows: depending on the W/C ratio, there is a subset of downstream loads that are beneficial in terms of the value that the defender can obtain by controlling them. That is, if the loads belonging to this subset are controlled, the decrease in $\mathrm{L_{VR}}$ outweighs the increase in $\mathrm{L_{LC}}$, hence, the defender imposes load control on these downstream loads to reduce the the total loss. In contrast, controlling the loads outside this subset, increases $\mathrm{L_{LC}}$ more than the decrease in $\mathrm{L_{VR}}$. Hence, the defender satisfies the demand at these loads fully. The $\mathrm{L_{LC}}$ increases until load control capability in the subset of beneficial downstream loads to the defender is fully exhausted. The size of this subset depends on the W/C ratio. The higher the ratio, the larger the size of the subset of the loads beneficial to the defender. Hence, the value of k, at which the $\mathrm{L_{LC}}$ cost curve flattens out, increases as the W/C ratio increases.

The cost curve for $\mathrm{L_{VR}}$ also shows interesting behavior as the number of compromised DER nodes increases (Figures 3-8a and 3-8b). The marginal increase in $\mathrm{L_{VR}}$ for every additional DER compromised reduces as k increases. This observation can be explained by the fact that the attacker prefers to compromise downstream nodes over upstream ones (Proposition 6). Initially, the attacker is able to rapidly increase L by compromising more beneficial downstream nodes. However, as the downstream nodes are eventually exhausted, the attacker has to target the relatively less beneficial upstream nodes. Hence,

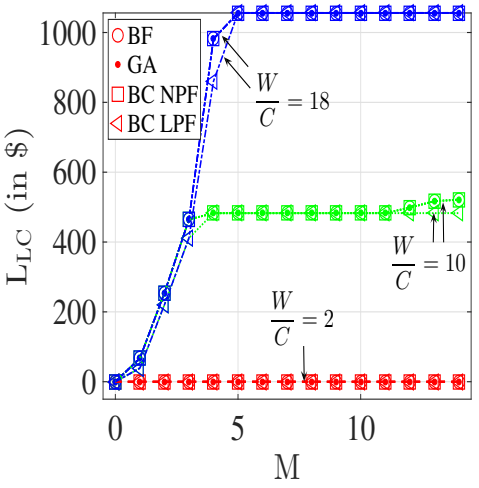


(a) L_{VR} vs k, $\underline{\gamma} = 0.5$.

(b) L_{VR} vs k, $\underline{\gamma} = 0.7$.



(c) L_{LC} vs k, $\underline{\gamma} = 0.5$.



(d) L_{LC} vs k, $\underline{\gamma} = 0.7$.

Figure 3-8: L_{VR} and L_{LC} vs M for $\mathcal{G}^I$. The results of $\mathcal{G}^H$ are more or less similar to those of $\mathcal{G}^I$.

the reduction in marginal increase of L_{VR}.

In L_{VR} plots, for small k, $^{W}/_{C} = 2$ curves are lower than the $^{W}/_{C} = 10$ curves which in turn are lower than the $^{W}/_{C} = 18$ curves. But, for larger k, this order reverses. The k where these lines cross each other decreases, as the $\underline{\gamma}$ increases (see Figures 3-8a and 3-8b). The reason is for some intermediate value of k, the defender exhausts the load control completely, and then the L increases at rates in the same order of increasing $^{W}/_{C}$ values.

Our computational study also validates that the GA is more efficient than BC method because GA calculates the exact impact the DER compromises will have on a pivot node. In contrast, BC overestimates the impact of DER compromises that are not the ancestors to the pivot nodes. Therefore, the feasible region probed by BC at every iteration is larger than the feasible region probed in the corresponding iteration of GA. Hence, although GA converges to a solution in 2-3 iterations, BC in most cases does not converge to the optimal solution even in 200 iterations.

Concluding Remarks

We focused on the security assessment of radial DNs for an adversary model in which multiple DERs (in this case, DER nodes) are compromised. The adversary can be a threat agent, who can compromise the operation of DERs, or a malicious insider in the control center. We considered a composite loss function that primarily accounts for the attacker's impact on voltage regulation and induced load control. The security assessment problem is formulated as a three-stage Defender-Attacker-Defender ([DAD]) sequential game. Our main technical contributions include: (i) Approximating the [DAD] game that has non-linear power flow model and mixed-integer decision variables with tractable formulations based on linear power flow; and (ii) characterization of structural properties of security investments in Stage 1 and the optimal attack in Stage 2 (i.e., the choice of DER node locations and the choice of false set-points).

Future work includes: (a) Extending Theorems 1 and 5 to cases where reverse power flows are permissible (e.g., when the DN is not under heavy loading conditions and the attacker can cause DER generation to exceed the demand); (b) Designing greedy algorithm to solve [AD] and proving optimality guarantees of Theorems 3 and 4 for DNs with

heterogeneous $\mathbf{r}/\mathbf{x}$ ratio, and heterogeneous DERs or loads.

Finally, note that we do not consider cascading failures in our paper. However, our analysis can be extended to a form of cascading failures within DNs reported by Kundu and Hiskens [74]. They study synchronous tripping of the loads (specifically, plug-in electric vehicles chargers) leading to over-voltages in the DN. Our result on optimal DER attack can be used to create voltage violations at some nodes. If these violations are too high, certain loads may start to trip. After sufficiently large number of loads trip, the attacker can further manipulate the DER setpoints to their maximum power generation capacity. In the absence of new loads, this may lead to overvoltages, as described in [74].

Supplementary Material

Parameters	Values
$r + \mathbf{j}x$	$(0.33 + 0.38\mathbf{j})\ \Omega$
$\mathrm{pc}_i^{\mathrm{nom}}$	$15\ kW$
$\mathrm{qc}_i^{\mathrm{nom}}$	$4.5\ kvar$
$\overline{\mathrm{sp}}_i$	$11.55\ kVA$
$\lvert V_0 \rvert$	$4\ kV$
C	7 \$ per kW

Table 3.2: Parameters of the Homogeneous Network

For a pivot node $i \in \mathcal{N}$, Algorithm 5 computes a sequence of sets of nodes in decreasing order of $\Delta_j(\widehat{\nu}_i)$ values. This sequence is used to compute the optimal attacks that maximize voltage bounds violation at node i.

Proof of Lemma 1. Recursively apply the power flow equations (3.5), (3.6), and (3.12), from the root node to leaf nodes. □

Proof of Lemma 2. We apply induction from leaf nodes to the root node.

Base case: For any leaf node $k \in \mathcal{N}_L$,

$$z_k \ell_k \overset{\text{(A0)}_5}{\leqslant} \epsilon_0 S_k \overset{(3.17a)}{=} \epsilon_0 (s_k + z_k \ell_k)$$

$$\therefore z_k \ell_k \leqslant \frac{\epsilon_0 s_k}{1-\epsilon_0} \overset{(3.17b)}{=} \frac{\epsilon_0 \widehat{S}_k}{1-\epsilon_0}.$$

Algorithm 5 Helper procedure

procedure OPTIMALATTACKHELPER(i, $\widehat{\mathrm{sp}}^{\mathrm{d}}$)
  For each $j \in \mathcal{N}$ compute $\Delta_j(\widehat{\nu}_i)$ using Lemma 4
  Create a sequence of sets $\{\mathcal{N}_j^i\}_{j=1}^N$ such that
  i) $\mathcal{N} = \bigcup_{j=1}^N \mathcal{N}_j^i$, $\forall\ 1 \leqslant j, k, \leqslant N,\ \mathcal{N}_j^i \cap \mathcal{N}_k^i = \varnothing$
  ii) if $1 \leqslant l \leqslant N,\ j, k \in \mathcal{N}_l^i$, then $\Delta_j(\widehat{\nu}_i) = \Delta_k(\widehat{\nu}_i)$, and
  iii) if $1 \leqslant l < m \leqslant N,\ j \in \mathcal{N}_l^i, k \in \mathcal{N}_m^i$, then $\Delta_j(\widehat{\nu}_i) > \Delta_k(\widehat{\nu}_i)$.
  Let, for $j \in [1, \ldots, N]$, $m_j^i \leftarrow \left|\mathcal{N}_j^i\right|$, $M_j^i := \sum_{k=1}^{j-1} m_k^i$.
  Let $g^i \leftarrow \operatorname{argmin}_{j \in [1,\ldots,N], M_j^i \geqslant M} \quad j$.
  $J \leftarrow \bigcup_{j=1}^{g^i-1} \mathcal{N}_{g^i}$, $m' = M - M_{g^i-1}^i$
  return $J, \mathcal{N}_{g^i}, m'$
end procedure

Now, for any $j \in \mathcal{N} \backslash \mathcal{N}_L$,

$$z_j \ell_j \overset{\text{(A0)}_5}{\leqslant} \epsilon_0 S_j \overset{(3.5a)}{=} \epsilon_0 \big[\textstyle\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j + z_j \ell_j \big]$$
$$\therefore z_j \ell_j \leqslant \frac{\epsilon_0}{1-\epsilon_0} \big[\textstyle\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j \big].$$

Adding $\sum S_k + s_j$ on both the sides:

$$\underbrace{\textstyle\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j + z_j \ell_j}_{S_j} \leqslant \frac{1}{1-\epsilon_0} \big[\textstyle\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j \big].$$

Inductive step: By inductive hypothesis (IH) on $\mathcal{N}_j^c$,

$$S_j \overset{\text{(IH)}}{\leqslant} \frac{1}{(1-\epsilon_0)^{H-|P_k|+2}} \big[\textstyle\sum_{k:(j,k)\in\mathcal{E}} \widehat{S}_k + s_j \big]$$
$$= \frac{\widehat{S}_j}{(1-\epsilon_0)^{H-|P_j|+1}} \quad (\because |\mathcal{P}_j| = |\mathcal{P}_k| - 1).$$

□

Proof of Proposition 3. The inequalities $\widehat{S} \leqslant S$ and $\widehat{\nu} \geqslant \nu$ are proved in [58].

The rest of the proof of Proposition 3 utilizes two lemmas. From Lemma 2, for any

$(i,j) \in \mathcal{E}$,

$$S_j \leqslant \frac{\widehat{S}_j}{(1-\epsilon_0)^{H-|\mathcal{P}_j|+1}} \leqslant \frac{\widehat{S}_j}{(1-\epsilon_0)^H} = (1+\epsilon)\widehat{S}_j \overset{(3.16a)}{=} \breve{S}_j. \tag{3.31}$$

For nodal voltages,

$$\begin{aligned} \nu_j &\overset{(3.5b)}{=} \nu_i - 2\mathbf{Re}(\bar{z}_j S_j) + |z|_j^2 \ell_j \\ &\geqslant \nu_i - 2\mathbf{Re}(\bar{z}_j S_j) \\ &\overset{(3.31)}{\geqslant} \nu_i - 2\mathbf{Re}(\bar{z}_j \breve{S}_j). \end{aligned} \tag{3.32}$$

Applying (3.32) recursively from the node j till root node:

$$\nu_j \geqslant \nu_0 - 2\textstyle\sum_{k\in\mathcal{P}_j} \mathbf{Re}(\bar{z}_k \breve{S}_k) \overset{(3.18d)}{=} \breve{\nu}_j.$$

Thus, $\widehat{S}_j \leqslant S_j \leqslant \breve{S}_j$ and $\widehat{\nu}_j \geqslant \nu_j \geqslant \breve{\nu}_j$. Furthermore,

$$\begin{aligned} &\widehat{S}_j \leqslant S_j \leqslant \breve{S}_j \overset{\textbf{(A0)}_3}{\implies} \left|\widehat{S}_j\right|^2 \leqslant |S_j|^2 \leqslant \left|\breve{S}_j\right|^2 \\ \implies &\frac{\left|\widehat{S}_j\right|^2}{\widehat{\nu}_j} \leqslant \frac{|S_j|^2}{\nu_j} \leqslant \frac{\left|\breve{S}_j\right|^2}{\breve{\nu}_j} \implies \widehat{\ell} \leqslant \ell \leqslant \breve{\ell}. \end{aligned}$$

Finally, (3.49) immediately follows from (3.9), (3.10), and (3.15). □

Proof of Lemma 3. Let $\widetilde{[\mathrm{AD}]}^{\mathrm{d}}$ denote the following problem:

$$\begin{aligned} \widetilde{[\mathrm{AD}]}^{\mathrm{d}} \quad \widetilde{\phi}^\star(\psi) \quad &\in \operatorname*{argmin}_{\phi\in\Phi} \mathrm{L}(\mathrm{x}(\psi,\phi)) \\ &\text{s.t. } \widehat{\mathrm{x}}(u,\psi,\phi) \in \mathcal{X}_{\mathrm{CPF}}, (3.8b), (3.8c). \end{aligned} \tag{3.33}$$

$(\mathbf{A0})_2$ implies that a feasible solution exists for $[\mathrm{AD}]^{\mathrm{d}}$. Since, $\mathcal{X} \subset \mathcal{X}_{\mathrm{CPF}}$, a feasible solution $\widetilde{\mathrm{x}} \in \mathcal{X}_{\mathrm{CPF}}$ also exists for $\widetilde{[\mathrm{AD}]}^{\mathrm{d}}$.

Let $(\widetilde{\phi}, \widetilde{\ell})$ denote the decision variables for $\widetilde{[\mathrm{AD}]}^{\mathrm{d}}$. Note that, for a fixed ψ, $\widetilde{\mathrm{x}}$ is affine in the variables $(\widetilde{\phi}, \widetilde{\ell})$, and can be very efficiently computed using (3.5a) and (3.5b).

Now, L is convex in $\widetilde{\phi}$ (because the L_{VR} is a maximum over affine functions, L_{LC} is affine in $\widetilde{\phi}$, and L_{LL} is affine in $\widetilde{\ell}$. Also, Φ is a convex compact set. Further, for a fixed ϕ, L

is strictly increasing in $\widetilde{\ell}$ (because, $\mathrm{L_{VR}}$ is non-decreasing in $\widetilde{\ell}$ as $\widetilde{\nu}$ is affine decreasing in $\widetilde{\ell}$; $\mathrm{L_{LC}}$ does not change with $\widetilde{\ell}$; $\mathrm{L_{LL}}$ is strictly increasing in ℓ). From Theorem 1 [52], $(\widetilde{\phi}^\star, \widetilde{\ell}^\star)$ can be computed using a SOCP. To argue that $\widetilde{\ell}^\star$ satisfy (3.5c), assume for contradiction that $\exists\ (i,j) \in \mathcal{E}$, s.t. $\widetilde{\ell}^\star_j > \left|\widetilde{s}^\star_j\right|^2/\widetilde{\nu}^\star_i$. Then, construct $(\phi^\star, \widetilde{\ell}')$ such that $\forall\ j \in \mathcal{N}\ : j \neq i$, $\widetilde{\ell}'_j = \widetilde{\ell}^\star_j$, and $\widetilde{\ell}'_i = \left|\widetilde{s}^\star_j\right|^2/\widetilde{\nu}^\star_i$. Since $\forall\ (j,k) \in \mathcal{E}$, $\left|\widetilde{s}_k\right|^2/\widetilde{\nu}_j$ is strictly decreasing in $\widetilde{\ell}_i$, $\forall\ (j,k) \in \mathcal{E}:\ \widetilde{\ell}'_k \geqslant \left|\widetilde{s}^\star_k\right|^2/\widetilde{\nu}^\star_j > \left|\widetilde{s}'_k\right|^2/\widetilde{\nu}'_j$. Hence, one can further minimize the loss function by choosing a new feasible solution $(\phi^\star, \widetilde{\ell}')$, thus violating the optimality of $(\widetilde{\phi}^\star, \widetilde{\ell}^\star)$. □

Proof of Proposition 4. Let (d_i, θ_i) denote $\widehat{\mathrm{sp}}^{\mathrm{d}}_i$ in the polar coordinates, i.e., $d_i = \left|\widehat{\mathrm{sp}}^{\mathrm{d}}_i\right|, \theta_i = \angle\widehat{\mathrm{sp}}^{\mathrm{d}}_i$.

For $\delta_i = 0$, $\widehat{\mathrm{sp}}_i = \widehat{\mathrm{sp}}^{\mathrm{d}}_i$. Then from (3.18a), $\forall\ j \in \mathcal{N}$,

$$\widehat{\nu}_j = \widehat{\nu}'_j + 2d_i(R_{ij}\cos\theta_i + X_{ij}\sin\theta_i), \tag{3.34}$$

where $\widehat{\nu}'_j = \nu_0 - 2\sum_{k\in\mathcal{N},k\neq j}\mathbf{Re}(\bar{Z}_{jk}s_k) - 2\mathbf{Re}(\bar{Z}_{ij}sc_j)$. Note that $\widehat{\nu}'_j$ does not depend on (d_i, θ_i).

It is clear from (3.34) that $\widehat{\nu}_j$ is greater if $\theta_i \in [0, \pi/2]$ than if $\theta_i \in [-\pi/2, 0]$. Furthermore, the impedances are positive. Hence, $\forall\ j, \partial_{d_i}\widehat{\nu}_j = 2(R_{ij}\cos\theta_i + X_{ij}\sin\theta_i) > 0$. Hence, $\partial_{d_i}\mathrm{L_{VR}} > 0$. But, from (3.4), $d_i \leqslant \overline{\mathrm{sp}}_i$. Hence, $d^\star_i = \overline{\mathrm{sp}}_i$. Further, $\partial_{\theta_i}\widehat{\nu}_j = 2d_i(-R_{ij}\sin\theta_i + X_{ij}\cos\theta_i)$.

$$\partial_{\theta_i}\widehat{\nu}_j \quad \begin{cases} > 0 & \text{if} \quad \theta_i \in [0, \operatorname{arccot}(R_{ij}/X_{ij})) \\ = 0 & \text{if} \quad \theta_i = \operatorname{arccot}(R_{ij}/X_{ij})) \\ < 0 & \text{if} \quad \theta_i \in (\operatorname{arccot}(R_{ij}/X_{ij})), \pi/2] \end{cases}$$

Now, $\operatorname{arccot}\overline{K} \leqslant \operatorname{arccot}(X_{ij}/R_{ij}) \leqslant \operatorname{arccot}\underline{K}$. Hence,

$$\forall \quad j \in \mathcal{N}, \quad \partial_{\theta_i}\widehat{\nu}_j \quad \begin{cases} < 0 & \text{if } \theta_i > \quad \operatorname{arccot}\underline{K} \\ > 0 & \text{if } \theta_i < \quad \operatorname{arccot}\overline{K} \end{cases} \tag{3.35}$$

Suppose, for contradiction, $\theta^\star_i \notin [\operatorname{arccot}\overline{K}, \operatorname{arccot}\underline{K}]$. Holding all else equal, for $\theta_i = \widetilde{\theta}_i$, let $\widehat{\nu}(\widetilde{\theta}_i)$ and $\mathrm{L_{VR}}(\widetilde{\theta}_i)$ be the $\widehat{\nu}$ and $\mathrm{L_{VR}}$. From (3.35), for any $\widetilde{\theta}_i \in [\operatorname{arccot}\overline{K}, \operatorname{arccot}\underline{K}]$,

$\widehat{\nu}(\widetilde{\theta}_i) > \widehat{\nu}(\widetilde{\theta}_i^\star)$. Since, $\mathrm{L_{VR}} > \mathrm{L_{LL}} \geqslant 0$, $\mathrm{L_{VR}}(\widetilde{\theta}_i) < \mathrm{L_{VR}}(\widetilde{\theta}_i^\star)$, violating the optimality of $\widetilde{\theta}_i^\star$. Furthermore, under identical $\mathbf{r}/\mathbf{x}$ ratio, $\underline{K} = \overline{K} = K$, which implies $\theta_i = \operatorname{arccot} K$. □

Claim 1. *Theorem 5 also holds for* $[\mathrm{AD}]^{\mathrm{a}}$.

Proof. Now, we prove the case for $[\mathrm{AD}]^{\mathrm{a}}$ by contradiction. Suppose that there exists $i \in \mathcal{N}$ s.t. $\mathbf{Re}(\mathrm{sp}_i^{a\star}) > 0$. Then we can construct another attacker strategy $\widetilde{\psi}^\star = [\widetilde{\delta}, \widetilde{\mathrm{sp}}^{\mathrm{a}}]$ that can further maximize L, such that $\mathbf{Re}(\mathrm{sp}_i^{a\star}) = 0$, holding all else equal, i.e., $\widetilde{\delta} = \delta, \forall\ j \in \mathcal{N},\ \mathbf{Im}(\widetilde{\mathrm{sp}}_j^{\mathrm{a}}) = \mathbf{Im}(\mathrm{sp}_j^{a\star}), \forall\ j \in \mathcal{N} : j \neq i,\ \mathbf{Re}(\widetilde{\mathrm{sp}}_j^{\mathrm{a}}) = \mathbf{Re}(\mathrm{sp}_j^{a\star})$.

Let $(\mathrm{sp}^{\mathrm{a}}, \ell)$ be the decision variables for $[\mathrm{AD}]^{\mathrm{a}}$, as for fixed ϕ, the other decision variables P, Q, ν can then be written as affine functions of $(\mathrm{sp}^{\mathrm{a}}, \ell)$ from (3.5). Let $(\mathrm{sp}^{\mathrm{a}\star}, \ell^\star)$ (resp. $(\widetilde{\mathrm{sp}}^{\mathrm{a}}, \widetilde{\ell})$) be the solution to $[\mathrm{AD}]^{\mathrm{a}}$ when $\psi = \psi^\star$ (resp. $\psi = \widetilde{\psi}$).

Let $f \in \mathbb{R}_+^N$ such that, for any $(i,j) \in \mathcal{E}$, $f_j(\mathrm{sp}^{\mathrm{a}}, \ell) := \frac{P_j^2 + Q_j^2}{\nu_i}$. Let $f^\star = f(\mathrm{sp}^{\mathrm{a}\star}, \ell^\star)$, $f' = f(\widetilde{\mathrm{sp}}^{\mathrm{a}}, \ell^\star)$, and $\widetilde{f} = f(\widetilde{\mathrm{sp}}^{\mathrm{a}}, \widetilde{\ell})$.

Since $(\mathrm{sp}^{\mathrm{a}\star}, \ell^\star)$ and $(\widetilde{\mathrm{sp}}^{\mathrm{a}}, \widetilde{\ell})$ are solutions to $[\mathrm{AD}]^{\mathrm{a}}$, they satisfy (3.5c). Hence, $f^\star = \ell^\star$, and $\widetilde{f} = \widetilde{\ell}$. Furthermore, it can be checked that $f' > f^\star$. We want to show that $\widetilde{f} > f'$. Assume that $\widetilde{f} > f'$. Then, $\widetilde{f} > f^\star$. Hence, $\mathrm{L}(\widetilde{\mathrm{x}}) > \mathrm{L}(\mathrm{x}^\star)$, (because, $\mathrm{L_{VR}}(\widetilde{\mathrm{x}}) > \mathrm{L_{VR}}(\mathrm{x}^\star)$, $\mathrm{L_{LC}}(\widetilde{\mathrm{x}}) = \mathrm{L_{LC}}(\mathrm{x}^\star)$, $\mathrm{L_{LL}}(\widetilde{\mathrm{x}}) > \mathrm{L_{LL}}(\mathrm{x})$). However, this is a contradiction, as it violates the optimality of $\mathrm{sp}^{\mathrm{a}\star}$. By similar logic, we can show that $\forall\ i \in \mathcal{N},\ \mathbf{Im}(\mathrm{sp}_i^{\mathrm{a}\star}) = -\overline{\mathrm{sp}}_i$.

We now prove that $\widetilde{f} > f'$, with the help of an illustrative diagram (see Figure 3-9).

Note that from (3.5), one can show that for any ℓ, $f(\mathbf{Re}(\widetilde{\mathrm{sp}}^{\mathrm{a}}, \ell)) > f(\mathbf{Re}(\mathrm{sp}^{\mathrm{a}\star}, \ell))$. Now, consider the $(j,k)^{th}$ entry of Jacobian $\mathbf{J}_f(\ell)$.

$$\partial_{\ell_k} f_j = \frac{\nu_i\big(2P_j\partial_{\ell_k}P_j + 2Q_j\partial_{\ell_k}Q_j\big)}{\nu_i^2} - \frac{(P_j^2 + Q_j^2)\partial_{\ell_k}\nu_i}{\nu_i^2}$$

$$\begin{aligned}
\therefore \quad 0 \overset{(A3)}{\leqslant} \partial_{\ell_k} f_j &\overset{(A4)}{<} \frac{(2r_k + 2x_k)}{\nu_i} + \frac{(4R_{ik}r_k + 4X_{ik}x_k)}{\nu_i^2} \\
\implies \quad 0 \leqslant \partial_{\ell_k} f_j &\overset{(A4)}{<} (r_k + x_k)(2/\mu + 4/\mu^2) \quad \leqslant 1 \\
\implies \quad 0 \leqslant \partial_{\ell_k} f_j &< 1.
\end{aligned}$$

At $\ell = \mathbf{0}$, $f > \mathbf{0}$, and each entry of Jacobian $\mathbf{J}_f(\ell)$ is positive and smaller than 1.

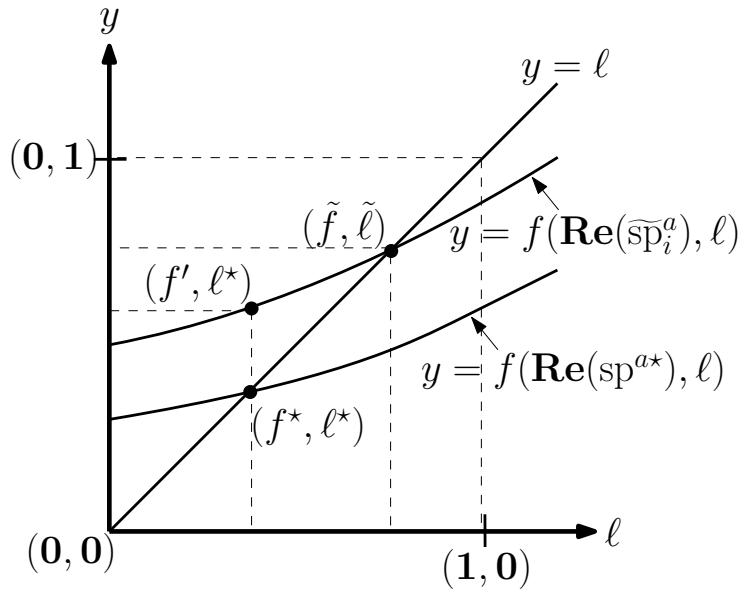


Figure 3-9: Illustrative diagram showing how ℓ changes with sp^{a}

Hence, f intersects the hyper-plane $y = \ell$, exactly once. Furthermore, $f(\mathbf{Re}(\widetilde{\mathrm{sp}}^{\mathrm{a}}, \ell)) > f(\mathbf{Re}(\mathrm{sp}^{\mathrm{a}\star}, \ell))$. Hence, we can conclude that $\widetilde{\ell} = \widetilde{f} > f' > f^\star = \ell^\star$. □

Proof of Proposition 5. Note that for fixed $\phi \in \Phi$, maximizing $\widehat{\mathrm{L}}(\hat{\mathrm{x}}(\widehat{\delta}, \phi))$ (resp. $\check{\mathrm{L}}(\check{\mathrm{x}}(\widehat{\delta}, \phi))$) is equivalent to maximizing $\mathrm{L}_{\mathrm{VR}}(\hat{\mathrm{x}}(\widehat{\delta}, \phi))$ (resp. $\mathrm{L}_{\mathrm{VR}}(\check{\mathrm{x}}(\check{\delta}, \phi))$). Let $\widehat{\delta}^\star$ be the optimal solution to $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$.

Case (i). $\mathrm{L}_{\mathrm{VR}}(\hat{\mathrm{x}}(\widehat{\delta}^\star, \phi)) = 0$. Then Algorithm 10 computes $\widehat{\delta}^\star$ trivially, because $\mathrm{L}_{\mathrm{VR}}(\hat{\mathrm{x}}(\widehat{\delta}^\star, \phi)) \geqslant \mathrm{L}_{\mathrm{VR}}(\hat{\mathrm{x}}(\widehat{\delta}, \phi)) \geqslant 0$. Hence, $\mathrm{L}_{\mathrm{VR}}(\hat{\mathrm{x}}(\widehat{\delta}, \phi)) = \mathrm{L}_{\mathrm{VR}}(\hat{\mathrm{x}}(\widehat{\delta}^\star, \phi)) = 0$.

Case (ii). $\mathrm{L}_{\mathrm{VR}}(\hat{\mathrm{x}}(\widehat{\delta}^\star, \phi)) > 0$. Let $\widehat{\nu}_j(\delta, \phi)$ denote the nodal voltage at node j after the attack δ. Since, $\widehat{\delta} = \widehat{\delta}^k$, for some pivot node $k \in \mathcal{N}$ (see Algorithm 10), $\widehat{\delta}^k$ maximally violates (3.1) over all $\widehat{\delta}^i$, i.e.,

$$\forall\ i \in \mathcal{N}, \quad \underline{\nu}_k - \widehat{\nu}_k(\widehat{\delta}^k, \phi) \geqslant \underline{\nu}_i - \widehat{\nu}_i(\widehat{\delta}^i, \phi), \tag{3.36}$$

where $\widehat{\delta}^i$ is the optimal pivot node attack as computed by Algorithm 10 for node i, i.e.,

$$\forall\ i \in \mathcal{N},\ \forall\ \delta \in \mathcal{D}_{\mathrm{k}} \quad \underline{\nu}_i - \widehat{\nu}_i(\widehat{\delta}^i, \phi) \geqslant \underline{\nu}_i - \widehat{\nu}_i(\delta, \phi). \tag{3.37}$$

Let $i = \operatorname{argmax}_{j\in\mathcal{N}} W_j(\underline{\nu}_j - \widehat{\nu}_j(\widehat{\delta}^\star, \phi))_+$. Furthermore, since $\mathrm{L}_{\mathrm{VR}}(\widehat{\mathrm{x}}(\widehat{\delta}^\star, \phi)) > 0$,

$$\mathrm{L}_{\mathrm{VR}}(\widehat{\mathrm{x}}(\widehat{\delta}^\star, \phi)) = W_i(\underline{\nu}_i - \widehat{\nu}_i(\widehat{\delta}^\star, \phi)) \tag{3.38}$$

$$\begin{aligned}
\therefore \mathrm{L}_{\mathrm{VR}}(\widehat{\mathrm{x}}(\widehat{\delta}, \phi)) &= \mathrm{L}_{\mathrm{VR}}(\widehat{\mathrm{x}}(\widehat{\delta}^k, \phi)) \\
&\overset{(3.10a)}{=} \max_{j\in\mathcal{N}} W_j(\underline{\nu}_j - \widehat{\nu}_j(\widehat{\delta}^k, \phi))_+ \\
&\overset{(3.36)}{\geqslant} W_i(\underline{\nu}_i - \widehat{\nu}_i(\widehat{\delta}^i, \phi)) \\
&\overset{(3.37)}{\geqslant} W_i(\underline{\nu}_i - \widehat{\nu}_i(\widehat{\delta}^\star, \phi)) \\
&\overset{(3.38)}{=} \mathrm{L}_{\mathrm{VR}}(\widehat{\mathrm{x}}(\widehat{\delta}^\star, \phi)).
\end{aligned}$$

Furthermore, for a fixed ϕ $\mathrm{L}_{\mathrm{LC}}(\widehat{\mathrm{x}}(\widehat{\delta}, \phi)) = \mathrm{L}_{\mathrm{LC}}(\widehat{\mathrm{x}}(\widehat{\delta}^\star, \phi))$. Hence, $\quad \widehat{\mathrm{L}}(\widehat{\mathrm{x}}(\widehat{\delta}, \phi)) \geqslant \widehat{\mathrm{L}}(\widehat{\mathrm{x}}(\widehat{\delta}^\star, \phi))$.

□

Proof of Lemma 4. Let sp_j be the DER set-point of node j before the attack. If sp_j is the pre-attack set-point, let $\Delta_j(\mathrm{sp}_j)$ denote the change in the set-point of DER j after it is compromised. By Theorem 5, $\Delta(\mathrm{sp}_j) = \mathrm{sp}_j - \mathrm{sp}_j^{\mathrm{a}} = \mathrm{sp}_j - (0 - \mathbf{j}\overline{\mathrm{sp}}_j) = \mathrm{sp}_j + \mathbf{j}\overline{\mathrm{sp}}_j$; and by linearity in (3.18a),

$$\Delta_j(\nu_i) = 2\mathbf{Re}(\bar{Z}_{ij}\Delta_j(\mathrm{sp}_j)) = 2\mathbf{Re}(\bar{Z}_{ij}(\mathrm{sp}_j^{\mathrm{d}} + \mathbf{j}\overline{\mathrm{sp}}_j)).$$

Again, by invoking the linearity in (3.18a), (3.25a) follows.

Similarly, one can show (3.24b) and (3.25b). □

Proof of Lemma 5. The computation of $\widehat{\mathcal{D}}_{\mathrm{k}}^\star(\phi)$ depends on $\Delta_j(\widehat{\nu}_i)$ values which depend only on sp^{d}, and not on $\widehat{\gamma}$ (see Lemma 4). □

Proof of Proposition 6. When $\delta_j = 1$, i.e., the DER j is compromised, only the power supplied at node j changes. Using (3.24a), we get,

$$\begin{aligned}
\therefore \Delta_j(\widehat{\nu}_i) &= 2\mathbf{Re}(\bar{Z}_{ij}\Delta(\mathrm{sp}_j^{\mathrm{d}})) \\
&= 2\mathbf{Re}(\bar{Z}_{ij}(\mathrm{sp}_j^{\mathrm{d}} + \mathbf{j}\overline{\mathrm{sp}}_j)).
\end{aligned}$$

$$\text{Now, } j \prec_i k \implies \mathcal{P}_i \cap \mathcal{P}_j \subset \mathcal{P}_i \cap \mathcal{P}_k \implies Z_{ij} < Z_{ik}.$$

$$\begin{aligned}\therefore \Delta_j(\widehat{\nu}_i) &= 2\mathbf{Re}(\bar{Z}_{ij}(\mathrm{sp}_j^{\mathrm{d}} + \mathbf{j}\overline{\mathrm{sp}}_j)) \\ &< 2\mathbf{Re}(\bar{Z}_{ik}(\mathrm{sp}_k^{\mathrm{d}} + \mathbf{j}\overline{\mathrm{sp}}_k)) = \Delta_k(\widehat{\nu}_i)\end{aligned}$$

Similarly, we can prove the case for $j =_i k$.

Under the ϵ-LPF model, $\Delta_j(\check{\nu}_i) = 2(1+\epsilon)\mathbf{Re}(\bar{Z}_{ij}(\mathrm{sp}_j^{\mathrm{d}} + \mathbf{j}\overline{\mathrm{sp}}_j))$. The rest of the proof follows similarly. □

Remark 1. Proposition 6 implies that, broadly speaking, compromising downstream DERs is advantageous to the attacker than compromising the upstream DERs. The following illustrative example suggests that compromising DERs by means of clustered attacks are more beneficial to the attacker than distributed attacks.

Example 1. Consider the $\widehat{[\mathrm{AD}]}^{\mathrm{a}}$ with $M = 2$ instantiated on the DN in Figure 3-1. Assume that all loads and DERs are homogeneous, all lines have equal impedances, i.e., $\forall i \in \mathcal{N}, sc_i = sc_a, \mathrm{sp}_i^{\mathrm{d}} = \mathrm{sp}_a^{\mathrm{d}}, \overline{\mathrm{sp}}_i = \overline{\mathrm{sp}}_a, z_i = z_a$. By Proposition 4, the outputs of all the DERs are fixed and identical to each other.

Let $\alpha = 2(\mathbf{Re}(\bar{z}_a(sc_a - \mathrm{sp}_a^{\mathrm{d}})))$, and $\beta = 2(\mathbf{Re}(\bar{z}_a(\mathbf{Re}(\mathrm{sp}_a^{\mathrm{d}}) + \mathbf{j}(\mathbf{Im}(\mathrm{sp}_a^{\mathrm{d}}) + \overline{\mathrm{sp}}_a))))$. Then ν values for different attack vectors are given in Table 3.3. The optimal attack compromises nodes i and m, which is a cluster attack.

Attacked Nodes	ν_m	ν_j	ν_k
$\varnothing$	$\nu_0 - 23\alpha$	$\nu_0 - 13\alpha$	$\nu_0 - 20\alpha$
$\{i, m\}$	$\nu_0 - 23\alpha - 9\beta$	$\nu_0 - 13\alpha - 2\beta$	$\nu_0 - 20\alpha - 4\beta$
$\{j, m\}$	$\nu_0 - 23\alpha - 6\beta$	$\nu_0 - 13\alpha - 4\beta$	$\nu_0 - 20\alpha - 3\beta$
$\{k, m\}$	$\nu_0 - 23\alpha - 7\beta$	$\nu_0 - 13\alpha - 2\beta$	$\nu_0 - 20\alpha - 6\beta$
$\{g, j\}$	$\nu_0 - 23\alpha - 2\beta$	$\nu_0 - 13\alpha - 5\beta$	$\nu_0 - 20\alpha - 2\beta$
$\{d, k\}$	$\nu_0 - 23\alpha - 4\beta$	$\nu_0 - 13\alpha - 2\beta$	$\nu_0 - 20\alpha - 7\beta$

Table 3.3: ν vs Different Attack Combinations.

Consequently, our results (see Sec. 3.5) on security strategy in Stage 1 show that the defender should utilize his security strategy to deter cluster attacks.

Proof of Proposition 7. For a fixed defender action ϕ, we have from (3.16b) that $\forall\ j \in \mathcal{N}, \Delta_j(\breve{\nu}_i) = (1+\epsilon)\Delta_j(\widehat{\nu}_i)$. Hence, the sequence of partitions of the nodes for every pivot node is the same in both the LPF and the ϵ-LPF model. Hence, $\widehat{\mathcal{D}}^{\star}_{\mathrm{k}}(\phi) = \breve{\mathcal{D}}^{\star}_{\mathrm{k}}(\phi)$.

Now, for any $\psi_1, \psi_2 \in \Psi$,

$$\begin{aligned} &\mathrm{L}_{\mathrm{LC}}(\widehat{\mathrm{x}}(\psi_1,\phi)) = \mathrm{L}_{\mathrm{LC}}(\widehat{\mathrm{x}}(\psi_2,\phi)) \quad \text{and} \\ &\mathrm{L}_{\mathrm{LC}}(\breve{\mathrm{x}}(\psi_1,\phi)) = \mathrm{L}_{\mathrm{LC}}(\breve{\mathrm{x}}(\psi_2,\phi)). \end{aligned} \tag{3.39}$$

Suppose $\widehat{\psi}^{\star}$ is not an optimal solution to $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$. Then,

$$\begin{aligned}
& \breve{\mathcal{L}}(\breve{\mathrm{x}}(\breve{\psi}^{\star},\phi)) && > \breve{\mathcal{L}}(\breve{\mathrm{x}}(\widehat{\psi}^{\star},\phi)) \\
\overset{(3.39)}{\iff} & \mathrm{L}_{\mathrm{VR}}(\breve{\mathrm{x}}(\breve{\psi}^{\star},\phi)) && > \mathrm{L}_{\mathrm{VR}}(\breve{\mathrm{x}}(\widehat{\psi}^{\star},\phi)) \\
\iff & \max_{i\in\mathcal{N}} W_i(\underline{\nu}_i - \breve{\nu}_i(\breve{\psi}^{\star},\phi))_+ && > \max_{j\in\mathcal{N}} W_j(\underline{\nu}_j - \breve{\nu}_j(\widehat{\psi}^{\star},\phi))_+ \\
\overset{(3.29)}{\iff} & \max_{i\in\mathcal{N}}(\underline{\nu} - \breve{\nu}_i(\breve{\psi}^{\star},\phi)) && > \max_{j\in\mathcal{N}}(\underline{\nu} - \breve{\nu}_j(\widehat{\psi}^{\star},\phi)) \\
\iff & \max_{i\in\mathcal{N}}(\nu_0 - \breve{\nu}_i(\breve{\psi}^{\star},\phi)) && > \max_{j\in\mathcal{N}}(\nu_0 - \breve{\nu}_j(\widehat{\psi}^{\star},\phi)) \\
\overset{(3.16b)}{\iff} & (1+\epsilon)\left\|(\nu_0 - \widehat{\nu}_i(\breve{\psi}^{\star},\phi))\right\|_{\infty} && > (1+\epsilon)\left\|(\nu_0 - \widehat{\nu}_j(\widehat{\psi}^{\star},\phi))\right\|_{\infty} \\
\overset{(3.29)}{\iff} & \max_{i\in\mathcal{N}} W_i(\underline{\nu}_i - \widehat{\nu}_i(\breve{\psi}^{\star},\phi))_+ && > \max_{j\in\mathcal{N}} W_j(\underline{\nu}_j - \widehat{\nu}_j(\widehat{\psi}^{\star},\phi))_+ \\
\iff & \mathrm{L}_{\mathrm{VR}}(\widehat{\mathrm{x}}(\breve{\psi}^{\star},\phi)) && > \mathrm{L}_{\mathrm{VR}}(\widehat{\mathrm{x}}(\widehat{\psi}^{\star},\phi)) \\
\overset{(3.39)}{\iff} & \widehat{\mathcal{L}}(\widehat{\mathrm{x}}(\breve{\psi}^{\star},\phi)) && > \widehat{\mathcal{L}}(\widehat{\mathrm{x}}(\widehat{\psi}^{\star},\phi)).
\end{aligned}$$

Hence, the contradiction that $\widehat{\psi}^{\star}$ is an optimal solution to $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$. Similarly, we can show that $\breve{\psi}^{\star}$ is an optimal solution to $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$. □

Proof of Proposition 8. **(A0)** implies that for any $(\psi,\phi) \in \Psi \times \Phi$, the node with least voltage will be one of the leaf nodes due to no reverse power flows. Therefore, the attacker will prefer to attack some leaf node as the pivot node. **(A1)** and **(A2)** imply that for any two nodes $i, j \in \mathcal{N}_L$, the radial network *as seen from node* i is just a homomorphic transformation of the radial network *as seen from node* j. Hence, the candidate set of optimal attack vectors for node i will be a homomorphic transformation of the candidate set of optimal attack vectors for node j. By definition, the candidate set of optimal attack

vectors for pivot node $i \in \mathcal{N}_L$ forms an equivalence class due to their identical impact on the node i. Since there can at most be N leaf nodes, the number of such equivalence classes is $\leqslant N$. The candidate set of optimal attack vectors is just a union over all leaf nodes $i \in \mathcal{N}_L$, the candidate set of optimal attack vectors for the pivot node i.

If for a pivot node, no two individual DER disruptions have identical impact on that pivot node, then Algorithm 5 computes a unique optimal attack vector for the pivot node. That is, the equivalence class for the pivot node is a singleton set. Therefore, the candidate set of optimal attack vectors is atmost of size N. □

To prove Theorem 4, we first introduce Propositions 9 to 11. Consider any security strategy $u \in \mathcal{U}_B$ such that

$$u = \left[\underbrace{u_1}_{1} \quad \underbrace{u_2}_{2} \quad \cdots \quad \underbrace{1}_{a} \quad \cdots \quad \underbrace{0}_{b} \quad \cdots \quad \underbrace{u_N}_{N}\right]. \tag{3.40}$$

Construct $\widetilde{u}$ from u by only flipping the bits at nodes a and b as follows:

$$\widetilde{u} = \left[\underbrace{u_1}_{1} \quad \underbrace{u_2}_{2} \quad \cdots \quad \underbrace{0}_{a} \quad \cdots \quad \underbrace{1}_{b} \quad \cdots \quad \underbrace{u_N}_{N}\right], \tag{3.41}$$

i.e., $\widetilde{u}_i = u_i \quad \forall \quad i \in \mathcal{N} \backslash \{a, b\}$. Similarly, let $\delta \in \mathcal{D}_{\mathrm{k}}(u)$ such that $\delta_a = 0, \delta_b = 1$; and construct $\widetilde{\delta}$ from δ as in (3.41) such that $\widetilde{\delta}_i = \delta_i \quad \forall \quad i \in \mathcal{N} \backslash \{a, b\}$. Note that, $\widetilde{\delta} \in \mathcal{D}_{\mathrm{k}}(\widetilde{u})$.

We use Propositions 9 to 11 to compare the security strategies u and $\widetilde{u}$ under various conditions. Refer to Figure 3-5c for the purpose of proofs of Propositions 9 to 11.

Proposition 9. *Assume **(A0)**, **(A1)**, **(A2)**. Let $u \in \mathcal{U}_B$ (resp. $\widetilde{u} \in \mathcal{U}_B$) be as in (3.40) (resp. (3.41)). If $b \in \Lambda_a$, then $u \preccurlyeq \widetilde{u}$.*

Proof of Proposition 9. Let $(\delta^\star, \phi^\star)$ and $(\widetilde{\delta}^\star, \widetilde{\phi}^\star)$, denote the optimal solutions of $[\widehat{\mathrm{AD}}]$ with $u = \widehat{u}$ (resp. $u = \widetilde{u}$). **(A1)** $\implies$ $\mathrm{sp}^{\mathrm{d}\star}$ is fixed (Proposition 4). Hence, $\phi^\star$ depends only on $\delta^\star$, and not u. Then, let $\phi^\star(\delta)$ denote optimal defender response to δ. We want to show $\widehat{\mathcal{L}}^{\widetilde{u}} \leqslant \widehat{\mathcal{L}}^{u}$.

Case $\widetilde{\delta}^\star_a = 0$. Then $\widetilde{\delta}^\star \in \mathcal{D}_{\mathrm{k}}(u)$. Thus,

$$\begin{aligned}\widehat{\mathcal{L}}^{\widetilde{u}} &= \widehat{\mathrm{L}}(\hat{\mathrm{x}}(\widetilde{u}, \widetilde{\delta}^\star, \phi^\star(\widetilde{\delta}^\star))) \\ &= \widehat{\mathrm{L}}(\hat{\mathrm{x}}(u, \widetilde{\delta}^\star, \phi^\star(\widetilde{\delta}^\star))) \\ &\leqslant \widehat{\mathrm{L}}(\hat{\mathrm{x}}(u, \delta^\star, \phi^\star(\delta^\star))),\end{aligned}$$

where the inequality follows due to the optimality of $\delta^\star$.

Case $\widetilde{\delta}^\star_a = 1$. Let $\delta \in \mathcal{D}_{\mathrm{k}}(u) : \delta_a = 0, \delta_b = 1, \forall i \in \mathcal{N}\backslash\{a,b\}, \delta_i = \widetilde{\delta}^\star_i$. We have assumed that $b \in \Lambda_a$; see Figure 3-5c. Therefore, $\forall\ i \in \mathcal{N},\ a \preceq_i b$. Hence, by Proposition 6,

$$\forall\ i \in \mathcal{N},\ \Delta_b(\widehat{\nu}_i) \geqslant \Delta_a(\widehat{\nu}_i).$$

Then, by Lemma 4, for fixed ϕ, $\Delta_\delta(\widehat{\nu}) \geqslant \Delta_{\widetilde{\delta}^\star}(\widehat{\nu})$. Hence,

$$\begin{aligned}\widehat{\mathcal{L}}^{\widetilde{u}} &= \widehat{\mathrm{L}}(\hat{\mathrm{x}}(\widetilde{u}, \widetilde{\delta}^\star, \phi^\star(\widetilde{\delta}^\star))) \\ &\leqslant \widehat{\mathrm{L}}(\hat{\mathrm{x}}(\widetilde{u}, \widetilde{\delta}^\star, \phi^\star(\delta))) \\ &\leqslant \widehat{\mathrm{L}}(\hat{\mathrm{x}}(u, \delta, \phi^\star(\delta))) \\ &\leqslant \widehat{\mathrm{L}}(\hat{\mathrm{x}}(u, \delta^\star, \phi^\star(\delta^\star))) \\ &= \widehat{\mathcal{L}}^{u}.\end{aligned}$$

Here, the first (resp. last) inequality follows due to optimality of $\phi^\star(\widetilde{\delta}^\star)$ (resp. $\delta^\star$). Hence, $u \preccurlyeq \widetilde{u}$. □

Remark 2. Starting with any strategy $u' \in \mathcal{U}_B$, Proposition 9 can be applied recursively to obtain a more secure strategy $u \in \mathcal{U}_B : u' \preccurlyeq u$, which has the property that if a node i is secure, then all its successor nodes (i.e. all nodes in subtree Λ_i) are also secured by the defender, i.e.,

$$\forall\ i \in \mathcal{N},\ u_i = 1 \implies \forall\ j \in \Lambda_i,\ u_j = 1. \tag{3.42}$$

Proposition 10. *Assume (A0), (A1), (A2). Let $u \in \mathcal{U}_B$ (resp. $\widetilde{u} \in \mathcal{U}_B$) be as in (3.40) (resp. (3.41)). Let $A_u = \{(i,j) \in \mathcal{N} \times \mathcal{N} \mid u_i = 1, u_j = 0, h_i \geqslant h_j + 1\}$. If u satisfies (3.42), and $(a,b) \in \operatorname{argmax}_{(i,j)\in A_u} |\mathcal{P}_i \cap \mathcal{P}_j|$, then $u \preccurlyeq \widetilde{u}$.*

Proof of Proposition 10. Let $c = \operatorname{argmax}_{(i \in \mathcal{P}_a \cap \mathcal{P}_b)} h_i$, be the lowest common ancestor of a and b. Let $i', i'' \in \mathcal{N}_c^c \ : \ a \in \Lambda_{i'}$ and $b \in \Lambda_{i''}$. From Theorem 3, we know that the optimal attack $\delta^\star$ will be a pivot node attack $\widehat{\delta}^i$ for some node, say $i \in \mathcal{N}$. Let $\mathcal{N}' = \Lambda_{i'} \cup \Lambda_{i''}$.

Case $i \in \mathcal{N}'$. Now $u_j = 1 \ \forall \ j \in \Lambda_{i'} \backslash \Lambda_{i'}^a \cup \{a\}$ by maximality of $|\mathcal{P}_a \cap \mathcal{P}_b|$. Similarly, $u_j = 0 \ \forall \ j \in \Lambda_{i''}^d \cup \{b\}$. Thus, $\forall \ j \in \Lambda_{i'}$ s.t. $u_j = 0$ there exists a separate node $k \in \Lambda_{i''}$ such that j and k are homomorphic, and $u_k = 0$ (see Figure 3-5c). Hence, the subtree $\Lambda_{i''}$ is more vulnerable than the subtree $\Lambda_{i'}$, and it will be more beneficial for the attacker to target a pivot node in $\Lambda_{i''}$. Now, $i \in \Lambda_{i''}$, and $\forall \ i \in \Lambda_{i''}, \ a \prec_i b$. Hence, by using Proposition 6, we get, $\Delta_a(\widehat{\nu}_i) < \Delta_b(\widehat{\nu}_i)$.

Case $i \notin \mathcal{N}'$. Then $a =_i b$, and by Proposition 6, we have $\Delta_a(\widehat{\nu}_i) = \Delta_b(\widehat{\nu}_i)$.

We now want to show that $\widehat{\mathcal{L}}^{\widetilde{u}} \leqslant \widehat{\mathcal{L}}^u$. The rest of the proof is similar to the proof of Proposition 9. □

Remark 3. Again, starting with any strategy $u' \in \mathcal{U}_B$, we can apply Proposition 10 recursively to obtain a more secure strategy $u \in \mathcal{U}_B : u' \leqslant u$, in which, if a node is secure, then all nodes in lower levels are also secured by the defender, i.e.,

$$\forall \ i, j \in \mathcal{N}, \ (u_i = 1 \text{ and } h_j > h_i) \implies u_j = 1. \tag{3.43}$$

Thus, Proposition 10 is a generalization of Proposition 9.

Proposition 11. *Assume (A0), (A1), (A2). Let $u \in \mathcal{U}_B$ be such that u satisfies (3.43). Let $h' = \operatorname{argmin}_{(\exists \ a \in \mathcal{N}_h : u_a = 1)} h$. If the secure nodes on level h' are uniformly distributed over the level h', i.e., $\left|\mathcal{N}_j^c \cap \mathcal{N}_s\right| \in \{T, T+1\}, \ \forall \ j \in \mathcal{N}_{h'}$, where $T \in \mathbb{Z}_+$, then u is an optimal security strategy, i.e., $\forall \ \widetilde{u} \in \mathcal{U}_B, \ \widetilde{u} \leqslant u$.*

Proof of Proposition 11. Similar to the proof of Proposition 10. □

Remark 4. Proposition 11 implies that there exists an optimal security strategy in which there is a top-most level with DER nodes that are uniformly chosen for security investment, while all the lower levels are fully secure.

Propositions 9 and 10 capture the attacker preference for the downstream DERs, whereas

Proposition 11 capture the attacker preference for cluster attacks. Hence, the optimal security strategy has distributed secured nodes.

Proof of Theorem 4. Let $u^{\star 1} \in \mathcal{U}_B$ be any optimal security strategy. From $u^{\star 1}$, by sequentially applying Proposition 9, Proposition 10, and Proposition 11, we can obtain an optimal security strategy $u^{\star 2}$ that satisfies (3.42), (3.43), and has the top-most level with secure nodes having uniformly distributed secured nodes.

Now, let $\widehat{u}^\star$ be the output of Algorithm 4. Since in Algorithm 4, nodes are secured from the leaf nodes to the root node level-by-level, $\widehat{u}^\star$ also satisfies (3.42) and (3.43). The Algorithm 4 also secures the top-most level with secure nodes with uniformly distributed secured nodes, $\widehat{u}^\star$ is the same as $u^{\star 2}$ upto a homomorphic transformation.

Finally, we argue that under **(A0)**-**(A2)**, $\widehat{u}^\star$ can be combined with previous results to obtain full solution of $[\widehat{\mathrm{DAD}}]$. Under **(A1)**, the defender set-points are fixed. Since, $\widehat{u}$ and $\widehat{\mathrm{sp}}^{\mathrm{d}\star}$ are both fixed, we can compute the set of candidate optimal attack vectors $\widehat{\mathcal{D}}_{\mathrm{k}}^\star$, by considering only vulnerable DERs. Then for a fixed $\delta \in \widehat{\mathcal{D}}_{\mathrm{k}}^\star$, the sub-problem $[\widehat{\mathrm{AD}}]^{\mathrm{d}}$ reduces to an LP in γ. Hence, Algorithm 2 solves for $(\widehat{\psi}^\star, \widehat{\phi}^\star)$, the optimal solution of $[\widehat{\mathrm{AD}}]$ for $u = \widehat{u}$, by iterating over $\delta \in \widehat{\mathcal{D}}_{\mathrm{k}}^\star$. The strategy profile $(\widehat{u}^\star, \widehat{\psi}^\star, \widehat{\phi}^\star)$, thus obtained, is an optimal solution to for DNs that satisfy **(A0)**, **(A1)**, **(A2)**. Similarly, we can solve $[\widetilde{\mathrm{DAD}}]$. □

Remark 5. We revisit the security strategies u^1 and u^2 in Figure 3-5: which one is better? Firstly, we use symmetricity **(A2)** to argue that securing nodes 2, 4, 5 is equivalent to securing nodes 3, 6, 7. Then, Λ_3 subtree of u^2 has more distributed secured nodes than Λ_2 in u^1. Hence, strategy 2 is better. Theorem 4 will, of course, give the optimal security strategy $\widehat{u}^\star$ in which nodes $\mathcal{N}_s(\widehat{u}^\star) = \{8, 9, 10, 12, 13, 14\}$, or other homomorphic strategies of $\widehat{u}^\star$.

3.6 Sequential game with linear power flow

In this Stackelberg game, Ψ_M denotes the set of attacker strategies in Stage 1; and $\Phi(\psi)$ denotes the set of defender actions in Stage 2. Formally, the attacker-defender $[\mathrm{AD}]$ game

is defined as follows:

$$[\mathrm{AD}] \quad \mathcal{L} \quad := \quad \max_{\psi \in \Psi_M} \ \min_{\phi \in \Phi(\psi)} \ \mathrm{L}(\mathrm{x}(\psi, \phi)) \tag{3.44}$$

$$\begin{aligned}
\text{s.t.} \ \ & \mathrm{x}(\psi, \phi) && \in \mathcal{X} && \text{(3.45a)} \\
& sc(\psi, \phi) && = \gamma \odot \mathrm{sc}^{\mathrm{nom}} && \text{(3.45b)} \\
& sg(\psi, \phi) && = \delta \odot \mathrm{sp}^{\mathrm{a}} + (\mathbf{1}_N - \delta) \odot \mathrm{sp}^{\mathrm{d}} && \text{(3.45c)} \\
& \Delta f_{0,max}(\psi, \phi) && = -H^{BG} S_0(\psi, \phi) - S_0^{\mathrm{nom}}, && \text{(3.45d)}
\end{aligned}$$

where (3.45b) specifies that the *actual power consumed* at node i is equal to the nominal power demand scaled by the defender's corresponding load control parameter $\gamma_i \in [\underline{\gamma}_i, 1]$.

The constraint (3.45c) models the net effect of the attacker choice $(\mathrm{sp}_i^{\mathrm{a}}, \delta_i)$ in Stage 1, and the defender choice $\mathrm{sp}_i^{\mathrm{d}}$ in Stage 2 on the *actual power generated* at node i. Thus, (3.45c) is the *adversary model* of $[\mathrm{AD}]$ game: the DER i is compromised *if and only if* it was targeted by the attacker ($\delta_i = 1$). Specifically, if i is compromised, $\mathrm{sp}_i = \mathrm{sp}_i^{\mathrm{a}}$, where $\mathrm{sp}_i^{\mathrm{a}} \in \mathcal{S}_i$ is the false set-point chosen by the attacker (different from the nominal set-point). The set-points of non-compromised DERs are governed by the defender, i.e., if DER i is not compromised ($\delta_i = 0$), then $\mathrm{sp}_i = \mathrm{sp}_i^{\mathrm{d}}$. Note that our adversary model assumes that the DER power output, sg, quickly attain the set-points specified by (3.45c), i.e., the model does not consider dynamic set-point tracking.

The constraint (3.45d) models the maximum frequency deviation due to the sudden active power imbalance.

The loss function in $[\mathrm{AD}]$ is defined as follows:

$$\mathrm{L}(\mathrm{x}(\psi, \phi)) \ := \ \mathrm{L}_{\mathrm{VR}}(\mathrm{x}) + \mathrm{L}_{\mathrm{FR}}(\mathrm{x}), \tag{3.46}$$

where L_{VR} denotes the cost due to loss of voltage regulation; and L_{FR} the cost due to loss

of frequency regulation. These costs are defined as follows:

$$\mathrm{L}_{\mathrm{VR}}(\mathrm{x}) \;:=\; ||W \odot (\underline{\nu} - \nu)_+||_\infty \tag{3.47a}$$

$$\mathrm{L}_{\mathrm{FR}}(\mathrm{x}) \;:=\; C(\Delta \underline{f}_{th} - \Delta f_{0,max})_+, \tag{3.47b}$$

where $W \in \mathbb{R}^N_+$, and $C \in \mathbb{R}_+$. Here, W_i is the weight assigned to violation of voltage bound, and L_{VR} is the maximum over all nodes the weighted non-negative difference between the lower bound $\underline{\nu}_i$ and nodal voltage square ν_i; C is the cost of unit frequency deviation, $\Delta \underline{f}_{th}$ is the lower threshold bound with which we will compare the system frequency deviation, and $\Delta f_{0,max}$ is the maximum frequency deviation attained as a result of the sudden supply-demand mismatch.

Now, consider the following simplified and approximate version of the sequential game $[\mathrm{AD}]$:

$$\begin{aligned} [\widehat{\mathrm{AD}}] \quad \widehat{\mathcal{L}} \quad &:= \quad \max_{\psi \in \Psi} \; \min_{\phi \in \Phi} \; \mathrm{L}(\hat{\mathrm{x}}(\psi, \phi)) \\ &\text{s.t.} \quad \hat{\mathrm{x}}(\psi, \phi) \in \widehat{\mathcal{X}}, (3.45b), (3.8c), (3.45d) \end{aligned}$$

where the NPF equations (3.5) are replaced by the LPF equations (3.6). In this section, we first compute the optimal attacker set-points and defender set-points (Sec. 3.6.1), and then present a greedy algorithm to come up with the optimal solution for $[\widehat{\mathrm{AD}}]$ (Sec. 3.6.2).

Following the computational approach in the literature to solve (bilevel) interdiction problems [102], [72], we define the master-problem $[\mathrm{AD}]^{\mathrm{a}}$ (resp. sub-problem $[\mathrm{AD}]^{\mathrm{d}}$) for fixed $\phi \in \Phi$ (resp. fixed $\psi \in \Psi$):

$$\begin{aligned} &[\mathrm{AD}]^{\mathrm{a}} \quad \psi^\star(\phi) \in \operatorname{argmax}_{\psi \in \Psi} \quad \mathrm{L}(\mathrm{x}(\psi, \phi)) \quad \text{s.t.} \quad (3.45), \\ &[\mathrm{AD}]^{\mathrm{d}} \quad \phi^\star(\psi) \in \operatorname{argmin}_{\phi \in \Phi} \quad \mathrm{L}(\mathrm{x}(\psi, \phi)) \quad \text{s.t.} \quad (3.45). \end{aligned}$$

Similarly, define master- and sub- problems $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$ $(\hat{\psi}^\star(\phi))$ and $[\widehat{\mathrm{AD}}]^{\mathrm{d}}$ $(\hat{\phi}^\star(\psi))$ for the variant $[\widehat{\mathrm{AD}}]$.

Proposition 12. *Let $(\psi^\star, \phi^\star)$ and $(\hat{\psi}^\star, \hat{\phi}^\star)$ be the optimal solutions to $[\mathrm{AD}]$ and $[\widehat{\mathrm{AD}}]$ with the corresponding optimal losses $\mathcal{L}$ and $\widehat{\mathcal{L}}$, respectively. Then, $\mathcal{L} \geqslant \widehat{\mathcal{L}}$.*

Proof. We first prove a preliminary result relating $\mathrm{x}(\psi, \phi)$ and $\widehat{\mathrm{x}}(\psi, \phi)$.

Lemma 6. *For a fixed strategy profile* (ψ, ϕ)*,*

$$S \geqslant \widehat{S}, \quad \nu \leqslant \widehat{\nu}, \quad \Delta f_{0,max} \geqslant \Delta \widehat{f}_{0,max} \tag{3.48}$$

Hence,

$$\left.\begin{aligned} \mathrm{L}_{VR}(\mathrm{x}) &\geqslant \mathrm{L}_{VR}(\widehat{\mathrm{x}}) \\ \mathrm{L}_{\mathrm{FR}}(\mathrm{x}) &\geqslant \mathrm{L}_{\mathrm{FR}}(\widehat{\mathrm{x}}) \end{aligned}\right\} \implies \mathrm{L}(\mathrm{x}) \geqslant \mathrm{L}(\widehat{\mathrm{x}}). \tag{3.49}$$

Proof. The relationships $S \geqslant \widehat{S}$ and $\nu \leqslant \widehat{\nu}$ is already proved in [52]. Since, $S \geqslant \widehat{S}$ implies $S \geqslant \widehat{S}$, from (3.45d) we get, $\Delta f_{0,max} \geqslant \Delta \widehat{f}_{0,max}$. □

From Lemma 6, we get,

$$\begin{aligned} \mathcal{L} &= \mathrm{L}(\mathrm{x}(\psi^\star, \phi^\star(\psi^\star))) \\ &\geqslant \mathrm{L}(\mathrm{x}(\widehat{\psi}^\star, \phi^\star(\widehat{\psi}^\star))) && \text{(by optimality of } \psi^\star) \\ &\geqslant \mathrm{L}(\widehat{\mathrm{x}}(\widehat{\psi}^\star, \phi^\star(\widehat{\psi}^\star))) && \text{(by Lemma 6)} \\ &\geqslant \mathrm{L}(\widehat{\mathrm{x}}(\widehat{\psi}^\star, \widehat{\phi}^\star(\widehat{\psi}^\star))) && \text{(by optimality of } \widehat{\phi}^\star) \\ &= \widehat{\mathcal{L}}. \end{aligned}$$

□

Lemma 6 implies that if there is a successful attack strategy for $[\widehat{\mathrm{AD}}]$, then there also exists a successful attack strategy for $[\mathrm{AD}]$. However, the converse need not be true.

3.6.1 Optimal attacker and defender set-points

The following theorem proven in [108] provides the optimal attacker set-points:

Theorem 5 (Optimal attacker set-points)**.** *The optimal attacker DER set-points* $\widehat{\mathrm{sp}}^{\mathrm{a}}$ *to the problem* $[\widehat{\mathrm{AD}}]$ *are given as:*

$$\widehat{\mathrm{sp}}_i^{\mathrm{a}} = 0 - \boldsymbol{j}\overline{\mathrm{sp}}_i \tag{3.50}$$

Proof. Similar to the proof of Thm. 1 in [108]. □

Thanks to the Theorem 5, the loss function $\mathrm{L}(\hat{\mathrm{x}}(\psi, \phi))$ can be written as $\mathrm{L}(\hat{\mathrm{x}}(\delta, \phi))$, as the optimal attacker preferred setpoints are already known.

Now, consider the following definition:

Definition 1. *Let $\mathcal{S}^+ := \{s \in \mathcal{S} \mid s \geqslant 0\}$. For a given attacker strategy $\psi \in \Psi$, if there exists a node that has the least voltage among all nodes regardless of the defender response, then it is called as the* worst-affected *node, i.e.,*

$$\forall\ \mathrm{sp}^{\mathrm{d}} \in \mathcal{S}^+ : \hat{\mathrm{x}}(\psi, [\mathrm{sp}^{\mathrm{d}}, \underline{\gamma}]) \in \widehat{\mathcal{X}},\ t(\psi) = \underset{i \in \mathcal{N}}{\operatorname{argmax}}(\underline{\nu}_i - \widehat{\nu}_i).$$

In this section, we compute the optimal defender setpoints under the following assumptions:

(A3) For a fixed $\psi \in \Psi$, *worst-affected* node $t(\psi)$ exists.

(A4) For a given $\psi \in \Psi$, under optimal defender response, the loss of voltage regulation and the loss of frequency regulation are both positive, i.e., $\mathrm{L}_{\mathrm{VR}}(\hat{\mathrm{x}}(\psi, \widehat{\phi}^{\star}(\psi))) > 0$ and $\mathrm{L}_{\mathrm{FR}}(\hat{\mathrm{x}}(\psi, \widehat{\phi}^{\star}(\psi))) > 0$.

Similar to the intuition presented in [108] the optimal attacker strategy in $\widehat{[\mathrm{AD}]}$ is to impose clustered DER compromises on a target pivot node, so that that pivot node has the least voltage **(A3)**. Further, as we see in Proposition 13, there is a trade-off for the defender between L_{VR} and L_{FR}. If the defender minimizes only L_{VR}, then the frequency deviations will be too high, and other DERs may disconnect. On the other hand, if he minimizes only L_{FR}, then the voltage quality at all nodes will suffer. Hence, assumption **(A4)**.

The following proposition computes the optimal defender DER set-points under the knowledge of *worst-affected* node.

Proposition 13 (Optimal Defender Set-points)**.** *Assume **(A3)** and **(A4)**. For a fixed $\psi \in \Psi$, let t be the* worst-affected *node under **(A3)**. Let $\widehat{\mathrm{sp}}^{c}$ denote the optimal defender set-point under the centralized control strategy. Then*

$$\forall\ i \in \mathcal{N}, \quad |\widehat{\mathrm{sp}}_i^{c}| = \overline{\mathrm{sp}}_i \text{ and } \angle \widehat{\mathrm{sp}}_i^{c} = \angle \lambda_{it}, \tag{3.51}$$

where $\lambda_{it} = CH^{BG} + 2W_t Z_{it}$.

Proof. Under (A3) and (A4), it can be checked that the loss function L can be written as:

$$\begin{aligned}
&\mathrm{L}(\widehat{\mathrm{x}}(\psi, \widehat{\phi^\star})) \\
&= W_t(\underline{\nu}_t - \widehat{\nu}_t) + C(\Delta \underline{f}_{th} - \Delta \widehat{f}_{0,max}) \\
&= \text{const.} + \textstyle\sum_{i \in \mathcal{N}} -CH^{BG} \widehat{\mathrm{sp}}_i^c - 2W_t \bar{Z}_{it} \widehat{\mathrm{sp}}_i^c \\
&= \text{const.} - \textstyle\sum_{i \in \mathcal{N}} \lambda_{it} \cdot \widehat{\mathrm{sp}}_i^c \\
&= \text{const.} - \textstyle\sum_{i \in \mathcal{N}} |\lambda_{it}| \, |\widehat{\mathrm{sp}}_i^c| \cos(\angle \lambda_{it} - \angle \widehat{\mathrm{sp}}_i^c)
\end{aligned}$$

It can be checked that[7] L is minimized when $|\widehat{\mathrm{sp}}_i^c| = \overline{\mathrm{sp}}_i$, and $\angle \widehat{\mathrm{sp}}_i^c = \angle \lambda_{it}$. □

3.6.2 Greedy Algorithm to solve $\widehat{[\mathrm{AD}]}$

We now present a greedy algorithm to solve for $\widehat{[\mathrm{AD}]}$.

Under (A3), we know that for the optimal attacker strategy $\widehat{\psi}^\star$, some node is the worst-affected node. Consider node t as a candidate worst-affected node, which we call a pivot node. Assuming that pivot node t is a worst-affected node for some attacker strategy, we compute the attacker strategy ψ that will maximize $\mathrm{L}^t := W_t(\underline{\nu}_t - \widehat{\nu}_t) + CH^{BG}(\Delta \underline{f}_{th} - \Delta \widehat{f}_{0,max})$. For pivot node t, we know the optimal defender set-points by Proposition 13. We also know the optimal attacker set-points, thanks to Theorem 5. Hence, the DER set-points sp^{d} are fixed by (3.8c). Furthermore, since $\gamma = \underline{\gamma}$, the defender strategy $\phi = [\mathrm{sp}^{\mathrm{d}}, \underline{\gamma}]$ is fixed. Hence, the problem $\widehat{[\mathrm{AD}]}$ becomes an integer optimization problem over δ. To solve this, we present a greedy algorithm to compute the optimal attack vector δ for the pivot node t.

Let $\Delta_i(\mathrm{L}^t)$ (resp. $\Delta_\delta(\mathrm{L}^t)$) be the change in loss function at node t caused due to compromise of DER at node j (resp. compromise of DERs due to attack vector δ). The following Lemma computes $\Delta_i(\mathrm{L}^t)$ and $\Delta_\delta(\mathrm{L}^t)$.

Lemma 7. *Assume (A3) and (A4). For a fixed $\psi \in \Psi$, let t be the* worst-affected *node under (A3). Let $\widehat{\mathrm{sp}}^{\mathrm{a}}$ (resp. $\widehat{\mathrm{sp}}^c$) denote the optimal attacker (resp. defender) set-points as computed*

[7] If $a, b \in \mathrm{W}$, then $\bar{a}b$ is the dot product of complex numbers a and b, and is maximized when $|a|$ and $|b|$ are maximized, and $\angle a = \angle b$.

in Theorem 5 (resp. Proposition 13). Further, let $\mathrm{L}^t := W_t(\underline{\nu}_t - \widehat{\nu}_t) + CH^{BG}(\Delta \underline{f}_{th} - \Delta \widehat{f}_{0,max})$. *Then,*

$$\Delta_i(\mathrm{L}^t) = \lambda_{it} \cdot (\widehat{\mathrm{sp}}_i^{\mathrm{a}} - \widehat{\mathrm{sp}}_i^{c}) \tag{3.52}$$

$$\Delta_\delta(\mathrm{L}^t) = \textstyle\sum_{i:\delta_i=1} \Delta_i(\mathrm{L}^t) \tag{3.53}$$

Proof. As seen in Proposition 13, the individual contribution of DER i when t is the worst-affected node is equal to $\lambda_{it} \cdot \widehat{\mathrm{sp}}_i^{\mathrm{d}}$. Since, the set-point changes from $\widehat{\mathrm{sp}}_i^{\mathrm{d}}$ to $\widehat{\mathrm{sp}}_i^{\mathrm{a}}$, the change in the loss L^t is $\lambda_{it} \cdot (\widehat{\mathrm{sp}}_i^{\mathrm{a}} - \widehat{\mathrm{sp}}_i^{c})$. (3.53) follows because L^t is a linear function of $\widehat{\mathrm{sp}}^{\mathrm{d}}$. □

The following greedy algorithm can be used to find δ that generate the worst impact.

Algorithm 6 Solution to $\widehat{[\mathrm{AD}]}$ under **(A3)**, **(A4)**

$(\widehat{\psi}^\star, \widehat{\phi}^\star, \widehat{\mathcal{L}}^*) \leftarrow$ Solve($\widehat{[\mathrm{AD}]}$)
procedure Solve($\widehat{[\mathrm{AD}]}$)
  for $i \in \mathcal{N}$ **do**
    $(\psi^i, \phi^i, \mathcal{L}^i) \leftarrow$ OptimalAttackForPivotNode(i)
  end for
  Compute worst-affected node as $t \leftarrow \mathrm{argmax}_{i \in \mathcal{N}} \mathcal{L}^i$
  return $\psi^t, \phi^t, \mathcal{L}^t$
end procedure
procedure OptimalAttackForPivotNode(t)
  Compute $\widehat{\mathrm{sp}}^{\mathrm{d}}$ as in Proposition 13 and $\widehat{\mathrm{sp}}^{\mathrm{a}}$ as in Theorem 5
  Sort nodes in $\mathcal{N}$ in decreasing order of their $\Delta_j(\widehat{\nu}_t, f)$ (computed using Lemma 7), and choose the top M DERs
  Compute $\delta^t \in \mathcal{D}_{\mathrm{k}}$ such that if a node i is chosen, $\delta_i^t = 1$
  return $\psi^t \leftarrow [\widehat{\mathrm{sp}}^{\mathrm{a}}, \delta^t]$, $\phi^t \leftarrow [\widehat{\mathrm{sp}}^{\mathrm{d}}, \underline{\gamma}]$, $\mathcal{L}^t \leftarrow \mathrm{L}(\hat{\mathrm{x}}(\psi^t, \phi^t))$
end procedure

3.7 A distributed control strategy

Proposed Design

Under nominal conditions, the defender is able to remotely configure optimal DER set-points by solving the OPF problem. However, under our adversarial model, during a contingency, the DER controllers can no longer rely on the set-points received from the control center as they can also be compromised by the adversary. Thus, our goal is to establish

a distributed control strategy to enable the non-compromised DERs to reduce defender loss (i.e., improve voltage and frequency regulation).

Now, we present a distributed control strategy in which we impose that each non-compromised DER should either contribute to the voltage or frequency regulation (but not both).

Definition 2. *1. First the node controllers detect an attack due to sudden drop in local voltage and frequency, and they set the load control parameter to the minimum load control parameter* $\underline{\gamma}$.

2. *Second, the DERs communicate with other nodes to estimate the identity of the* worst-affected *node in terms of the voltage violation, i.e. the DERs determine the node* $t = \operatorname{argmax}_{i \in \mathcal{N}} W_i(\underline{\nu}_i - \nu_i)$.

3. *For every node* $i \in \mathcal{N}$*, the DER controller of* $i-$*th DER has a precomputed partition of the nodes* $\mathcal{N}_t^f$ *and* $\mathcal{N}_t^v$*, such that* $\mathcal{N}_t^f \cap \mathcal{N}_t^v = \varnothing$ *and* $\mathcal{N}_t^f \cup \mathcal{N}_t^v = \mathcal{N}$.

4. *Finally, each DER configures a new DER set-point such that if* $i \in \mathcal{N}_t^f$*, the* $i-$*th DER controller contributes to only frequency regulation, otherwise it contributes to only voltage regulation.*

In order to compute the *worst-affected node*, we assume a fairly simple communication protocol for the secondary distributed control strategy. We assume that the communication topology is similar to the physical network topology. Every DER controller has the current best knowledge of the node with the least voltage. Initially, every DER just stores its own identity and corresponding nodal voltage value. In every iteration, each DER controller sends updates to its neighbors about the current minimum ν_i value and the corresponding node i. Then, the DER controller compares its current best knowledge with the information it receives from its neighbors, computes the new minimum ν_j value and determines the corresponding node j. And, so on and so forth. It can be shown that this process converges in at most $D + 1$ iterations, where D is the diameter of network $\mathcal{G}$. For a more detailed discussion of such protocols, we refer the reader to [37], [36].

The advantage of the proposed design is that during an attack scenario (or more broadly under a range of contingency situations), the DER controllers need not rely upon the possibly compromised control center set-points. Moreover, since the DERs use the distributed control strategy only to communicate with their neighboring DER controllers (and not with every other DER controller), the communication requirements are relatively less stringent.

The following proposition computes the optimal defender set-points for non-compromised DERs should they contribute to either only frequency regulation or only voltage regulation.

Proposition 14. *Assume (A3), (A4), (A1). Let* $\widehat{\mathrm{sp}}^{d}$ *denote the optimal defender set-points under the distributed control strategy as in Definition 2. Consider fixed* $\psi \in \Psi$*. For a node* $i \in \mathcal{N}$*, assume fixed* $\widehat{\mathrm{sp}}^{\mathrm{d}}_{-i} \in \mathcal{S}_{-i}$*, where* $\widehat{\mathrm{sp}}^{\mathrm{d}}_{-i}$ *denotes the vector of all defender set-points except for node* i*. Furthermore, let* $\phi = [\widehat{\mathrm{sp}}^{\mathrm{d}}, \underline{\gamma}]$*. Then,*

1. $\forall\ i \in \mathcal{N}_t^f,\ \widehat{\mathrm{sp}}^{\mathrm{f}}_i \in \operatorname{argmin}_{\widehat{\mathrm{sp}}^{\mathrm{d}}_i \in \mathcal{S}_i} \mathrm{L}_{\mathrm{FR}}(\hat{\mathrm{x}}(\psi, \phi))$*, where*

$$\left|\widehat{\mathrm{sp}}^{\mathrm{f}}_i\right| = \overline{\mathrm{sp}}_i, \text{ and } \angle \widehat{\mathrm{sp}}^{\mathrm{f}}_i = 0 \tag{3.54}$$

2. $\forall\ i \in \mathcal{N}_t^v,\ \widehat{\mathrm{sp}}^{\mathrm{v}}_i \in \operatorname{argmin}_{\widehat{\mathrm{sp}}^{\mathrm{d}}_i \in \mathcal{S}_i} \mathrm{L}_{VR}(\hat{\mathrm{x}}(\psi, \phi))$*, where*

$$|\widehat{\mathrm{sp}}^{\mathrm{v}}_i| = \overline{\mathrm{sp}}_i, \text{ and } \angle \widehat{\mathrm{sp}}^{\mathrm{v}}_i = \angle z_u \tag{3.55}$$

Proof. If node $i \in \mathcal{N}$ contributes to only frequency regulation, then L_{FR} can be written as:

$$\mathrm{L}_{\mathrm{FR}}(\hat{\mathrm{x}}) = -H^{BG}\widehat{\mathrm{sp}}^{d}_i + \text{const.}$$

Hence, L_{FR} is a decreasing function of $\widehat{\mathrm{sp}}^{\mathrm{d}}_i$, and will be minimized when $\widehat{\mathrm{sp}}^{d}_i = \overline{\mathrm{sp}}_i$. However, $\widehat{\mathrm{sp}}^{d}_i \in \mathcal{S}_i$ implies that $\mathbf{Im}(\widehat{\mathrm{sp}}^{d}_i) = 0$.

If node $i \in \mathcal{N}$ contributes to only voltage regulation, then L_{VR} can be written as:

$$\mathrm{L}_{\mathrm{FR}}(\widehat{\mathrm{x}}) = -2W_t Z_{it} \cdot \widehat{\mathrm{sp}}_i^d + \text{const.}$$

Under identical $\mathbf{r}/\mathbf{x}$ ratio, $\angle Z_{it} = \angle z_u$. The rest of the proof follows similarly to the proof of Proposition 13. □

Theorem 6. *Assume (A3), (A4), (A1). For a fixed $\psi \in \Psi$, let t be the worst-affected node. Let $\mathcal{N}_t^f, \mathcal{N}_t^v$ form a disjoint partition of $\mathcal{N}_{NC}$ (the set of non-compromised DERs), such that for all $j \in \mathcal{N}_t^f$ (resp. for all $k \in \mathcal{N}_t^v$), $\widehat{\mathrm{sp}}_j^d = \widehat{\mathrm{sp}}_j^{\mathrm{f}}$ (resp. $\widehat{\mathrm{sp}}_k^d = \widehat{\mathrm{sp}}_k^{\mathrm{v}}$) is as specified by (3.54) (resp. (3.55)). Then*

$$\begin{aligned} j \in \mathcal{N}_t^f \quad &\implies \quad 0 \quad &&\leqslant \angle\lambda_{jt} \quad \leqslant \frac{\angle z_u}{2} \\ k \in \mathcal{N}_t^v \quad &\implies \quad \frac{\angle z_u}{2} \quad &&< \angle\lambda_{kt} \quad \leqslant \angle z_u \end{aligned}$$

Proof. Under (A3) and (A4), it can be checked that the loss function L can be written as:

$$\begin{aligned} \mathrm{L}(\widehat{\mathrm{x}}(\psi, \phi)) &= W_t(\underline{\nu}_t - \widehat{\nu}_t) + C(\Delta \underline{f}_{th} - \Delta \widehat{f}_{0,max}) \\ &= \text{const.} + \textstyle\sum_{i \in \mathcal{N}} -\lambda_{it} \cdot \mathrm{sp}_i, \end{aligned}$$

where $\lambda_{it} = CH^{BG} + 2W_t Z_{it}$.

Under (A3), (A4), (A1), let $\widehat{\mathrm{sp}}_i^{\mathrm{f}}$ and $\widehat{\mathrm{sp}}_i^{\mathrm{v}}$ be the defender set-points as in (3.54) and (3.55), respectively. Let the change in the value of the loss function, holding all else the same, if the $j-$th DER is used for frequency regulation (resp. voltage regulation) be denoted by $\Delta_{jt}^f(\mathrm{L})$ (resp. $\Delta_{jt}^v(\mathrm{L})$). Then the difference in these two changes, holding all else equal, is given by

$$\begin{aligned} \Delta_{jt}^f(\mathrm{L}) - \Delta_{jt}^v(\mathrm{L}) &= \lambda_{jt} \cdot \widehat{\mathrm{sp}}_j^{\mathrm{f}} - \lambda_{jt} \cdot \widehat{\mathrm{sp}}_j^{\mathrm{v}} \\ &= |\lambda_{jt}| \, \overline{\mathrm{sp}}_j (\cos(\angle z_u - \angle\lambda_{jt}) - \cos\angle\lambda) \\ &= 2\,|\lambda_{jt}| \, \overline{\mathrm{sp}}_j \sin\frac{z_u}{2} \sin(\angle\lambda_{jt} - \frac{\angle z_u}{2}) \end{aligned}$$

Clearly, $\Delta_{jt}^f(\mathrm{L}) > \Delta_{jt}^v(\mathrm{L}) \iff \angle\lambda_{jt} < \frac{\angle z_u}{2}$.

Now, $\cot \angle\lambda_{it} = \frac{CH^{BG}+2W_tR_{it}}{2W_tX_{it}} = \frac{CH^{BG}}{2W_tX_{it}} + \frac{1}{z_u}$, which decreases when X_{it} increases, or equivalently, $\angle\lambda_{it}$ increases when Z_{it} increases. Now, Z_{it} is minimum (resp. maximum) when $i = 0$ (resp. $i = t$). Hence, $\angle\lambda_{it}$ is minimum (resp. maximum) when $i = 0$ (resp. $i = t$). If $\angle\lambda_{0t} \leqslant \frac{\angle z_u}{2} < \angle\lambda_{tt}$, then there must exist a node $t_c \in \mathcal{P}_t$ where $\angle\lambda_{it}$ changes from less than $\frac{\angle z_u}{2}$ to greater than $\frac{\angle z_u}{2}$. This node t_c is the critical node which gives us the partition $\mathcal{N}_t^f = \{i \in \mathcal{N} \ : \ i \prec_t t_c\}$ and $\mathcal{N}_t^v = \{i \in \mathcal{N} \ : \ t_c \preceq_t i\}$. Note that $\forall\ i \in \mathcal{N}_t^f,\ \angle\lambda_{it} < \angle\lambda_{t_ct}$ and $\forall\ i \in \mathcal{N}_t^v,\ \angle\lambda_{it} \geqslant \angle\lambda_{t_ct}$.

Finally, if $\forall\ j \in \mathcal{N},\ \angle\lambda_{jt} < \frac{\angle z_u}{2}$, then $\mathcal{N}_t^f = \mathcal{N}$ and $\mathcal{N}_t^v = \varnothing$. If $\forall\ j \in \mathcal{N},\ \angle\lambda_{jt} > \frac{\angle z_u}{2}$, then $\mathcal{N}_t^v = \mathcal{N}$ and $\mathcal{N}_t^f = \varnothing$.

□

As per the existing IEEE 1547 DER interconnection guidelines, if the voltages fall below $\underline{\nu}$, then the DERs should disconnect from the network. Let us denote these defender DER setpoints by $\widehat{\mathrm{sp}}^{\mathrm{d}} = \mathbf{0}$. Let $\widehat{\phi}^0 := [\mathbf{0}, \underline{\gamma}]$ be the defender *"Disconnect-DERs"* strategy when $\widehat{\mathrm{sp}}^{\mathrm{d}} = \mathbf{0}$. Furthermore, let $(\widehat{\psi}^\star, \widehat{\phi}^\star)$ be the optimal solution to $\widehat{[\mathrm{AD}]}$. Let $\widehat{\phi}^c$ (resp. $\widehat{\phi}^d$) be the defender strategies when defender set-points are as specified by the centralized (resp. distributed) strategy. Also, let $\widehat{\mathcal{L}}$, $\widehat{\mathcal{L}}_d$, and $\widehat{\mathcal{L}}_0$ be the optimal losses corresponding to the strategy profiles $(\widehat{\psi}^\star, \widehat{\phi}^c)$, $(\widehat{\psi}^\star, \widehat{\phi}^d)$, and $(\widehat{\psi}^\star, \widehat{\phi}^0)$, respectively. The following proposition compares the performance of distributed control strategy with that of centralized control strategy relative to the *Disconnect-DERs* strategy.

Proposition 15.

$$\frac{\widehat{\mathcal{L}}_d - \widehat{\mathcal{L}}_0}{\widehat{\mathcal{L}}_c - \widehat{\mathcal{L}}_0} \geqslant \cos\left(\frac{\angle z_u}{2}\right), \tag{3.56}$$

where z_u is the impedance per unit length.

Proof. Under the distributed control strategy, node i contributes to either frequency regulation or voltage regulation, depending upon which contribution is larger, i.e., $\lambda_{it}.\widehat{\mathrm{sp}}_i^c =$

$\max(\lambda_{it}.\widehat{\mathrm{sp}}_i^{\mathrm{f}}, \lambda_{it}.\widehat{\mathrm{sp}}_i^{\mathrm{v}})$. Now, node $i \in \mathcal{N}_t^f$ if

$$\begin{aligned} & \lambda_{it} \cdot \widehat{\mathrm{sp}}_i^{\mathrm{f}} && \geqslant && \lambda_{it} \cdot \widehat{\mathrm{sp}}_i^{\mathrm{v}} \\ \Longleftarrow\ & |\lambda_{it}|\, \overline{\mathrm{sp}}_i \cos(\angle\lambda_{it}) && \geqslant && |\lambda_{it}|\, \overline{\mathrm{sp}}_i \cos(\angle z_u - \angle\lambda_{it}) \\ \Longleftarrow\ & \cos(\angle\lambda_{it}) && \geqslant && \cos(\angle z_u - \angle\lambda_{it}) \end{aligned}$$

Also, if $\cos(\angle\lambda_{it}) \geqslant \cos(\angle z_u - \angle\lambda_{it})$, then $\cos(\angle\lambda_{it}) \geqslant \max(\cos(\angle\lambda_{it}), \cos(\angle z_u - \angle\lambda_{it})) \geqslant \cos(\frac{\angle z_u}{2})$. Hence,

$$\begin{aligned} & \widehat{\mathcal{L}}_d - \widehat{\mathcal{L}}_0 \\ & = \textstyle\sum_{i\in\mathcal{N}} \max(\lambda_{it} \cdot \widehat{\mathrm{sp}}_i^{\mathrm{f}}, \lambda_{it} \cdot \widehat{\mathrm{sp}}_i^{\mathrm{v}}) \\ & = \textstyle\sum_{i\in\mathcal{N}} |\lambda_{it}|\, \overline{\mathrm{sp}}_i \max(\cos(\angle\lambda_{it}), \cos(\angle z_u - \angle\lambda_{it})) \\ & \geqslant \textstyle\sum_{i\in\mathcal{N}} |\lambda_{it}|\, \overline{\mathrm{sp}}_i \cos(\frac{\angle z_u}{2}) \\ & = \cos(\tfrac{\angle z_u}{2}) \textstyle\sum_{i\in\mathcal{N}} \lambda_{it} \cdot \widehat{\mathrm{sp}}_i^{c} = \cos(\tfrac{\angle z_u}{2})(\widehat{\mathcal{L}}_c - \widehat{\mathcal{L}}_0). \end{aligned}$$

□

3.8 Case study

We present a simple case study to illustrate the main aspects of our distributed control approach. We consider the 14 node radial network illustrated in Figure 3-10. Each node represent a DER connected to loads. The DERs are heterogeneous (please refer to caption of Fig. 3-10). We assume that the DER units closer to the substation are owned by the utility, and these units possess larger power injection capacities. On the other hand, downstream DERs (e.g., roof-top PVs) are smaller in their capacities, and are owned by users. As we have shown in Sec. 3.6, attacks on the downstream nodes cause larger voltage deviations, while attacks to the larger generators primarily impact the frequency deviations, independent of their location.

The test circuit is homogeneous, i.e., all the lines and loads have similar physical properties. The impedance per unit length for all lines is $z_u = 0.1 + 0.3\mathbf{j}\ \Omega/km$, and nominal power demand is $\mathrm{sc}_i^{\mathrm{nom}} = 25\ kW + \mathbf{j}7.5\ kvar$. DERs supply 50% of the total demand.

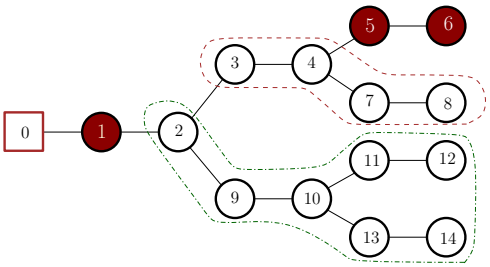


Figure 3-10: Tree topology of heterogeneous 14 nodes. The attacker selects nodes $1, 5$ and 6. Using our proposed distributed control strategy, the DERs cooperatively react to the attacker's strategy: nodes $2, 9, 10, 11, 12, 13, 14$ contribute toward reducing frequency deviation, whereas, nodes $3, 4, 7, 8$ contribute toward maintaining voltage regulation.

The maximum apparent power that generator i can produce is $\overline{\text{sp}}_i = 20.7\ kVA$ for i=1,2; $14.6\ kVA$ for i=3,4,9,10; and $11.8\ kVA$ otherwise. The voltage at each node is constrained to be within 0.95 and 1.05 *p.u.* Frequency should be maintained above 59.7 Hz (assuming nominal frequency to be $60\ Hz$) to avoid the LAARS (Load Acting As Resource) tripping. The bulk generator parameters are $\text{M} = 5\ s$, $\text{D} = 5x10^{-4}\ Hz/kW$, $\text{K}_\text{P} = 5.1$, $\text{K}_\text{I} = 2$ s. $C = 1000$ and $\forall\ i \in \mathcal{N},\ W_i = 70$, where C and W are the weights for LOFR and LOVR, respectively.

An attacker compromises the set point information delivered by the control center after $1000\ s$, and simultaneously modifies the setpoints to DERs attached to nodes $1, 5$ and 6. The attack causes a frequency and voltage deviation that activates the contingency response. Note that $C > W$, i.e., frequency regulation is a priority. Using the exchange of information between DERs about the node voltages described in section 3.6, the *worst-affected* node t is determined to be node 6. Also, we find the critical node $t_c = 3$, which results in the partition of non-compromised nodes as shown in figure 3-10. As a consequence, nodes $3, 4, 7, 8$ start contributing to voltage regulation, and $2, 9, 10, 11, 12, 13, 14$ to frequency regulation, as depicted in Figures 3-10 and 3-11. Further, $\cos\frac{\angle z_u}{2} = 0.937$. Hence, Proposition 15 implies that the distributed control strategy performs at least as good as 86.7% compared to the centralized control strategy.

The minimum voltage level and the grid frequency dynamics are illustrated in Figure 3-12 for the case without a defense action, i.e., maintaining the nominal set points, and with the defender response. Note that frequency deviation is rapidly driven to zero

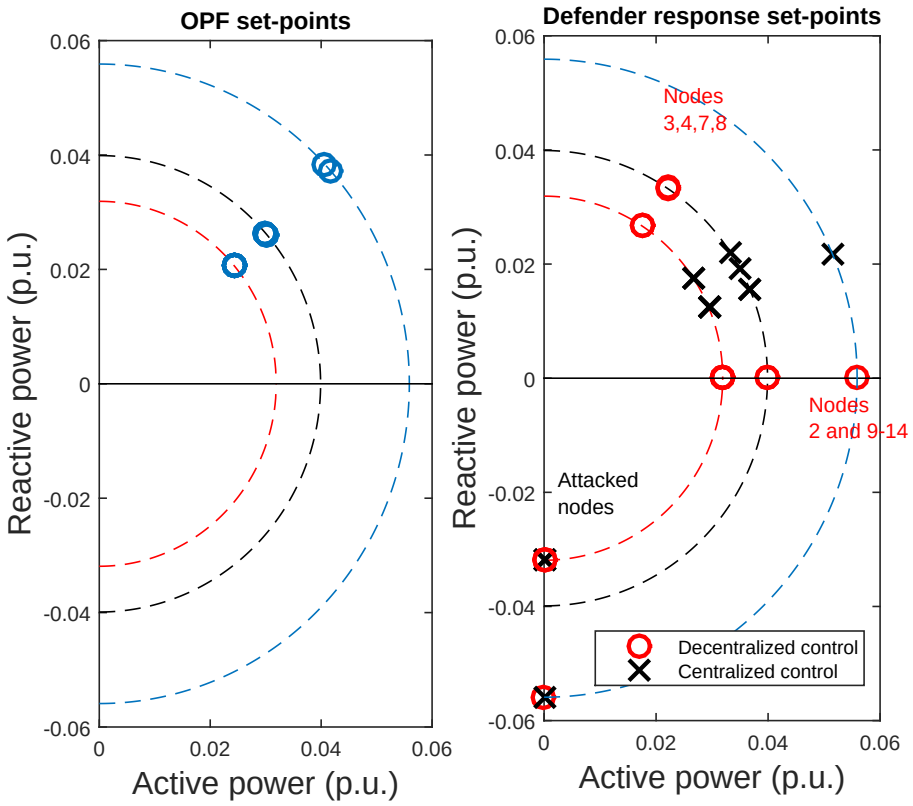


Figure 3-11: Apparent power set points from the OPF (left) and after the attack (right). According to the proposed distributed control strategy, each DER either contributes to voltage regulation or toward reducing frequency deviation.

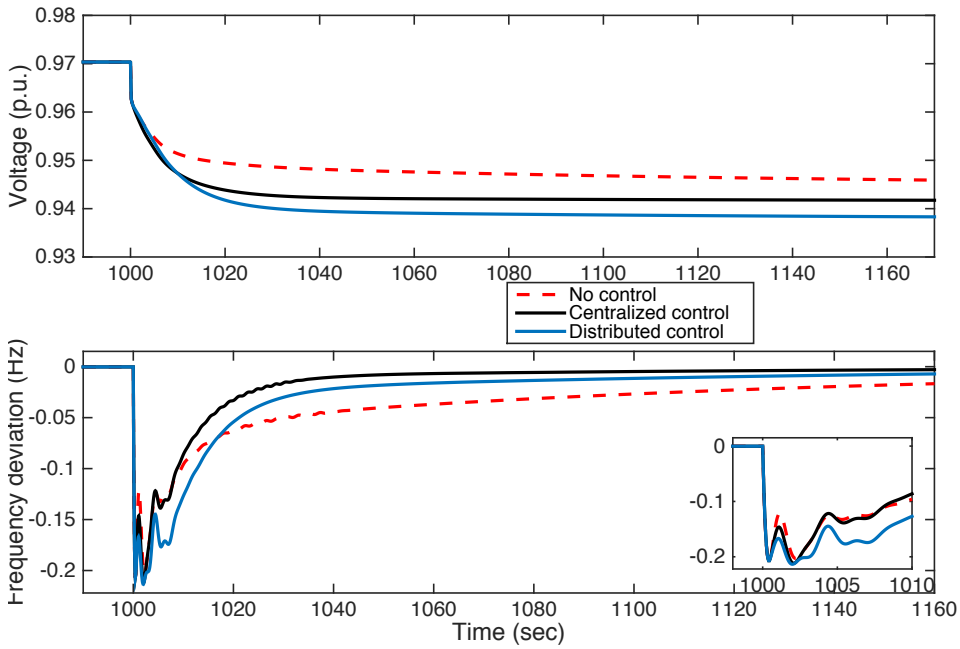


Figure 3-12: Dynamic response of the voltage in node 6 and the bulk generator frequency. An attack occurs at $t = 2000$ s.

using the centralized and distributed strategies. However, due to the trade-off between frequency and voltage regulation, the voltage levels are lower than without any defense action. Depending on the system operator requirements, the selection of C and W will determine the priority to voltage or to frequency regulation. Figures 3-11 and 3-12 compare the performance of centralized and distributed control strategies. Clearly, the solution obtained with the centralized strategy performs better than the distributed one, but it requires the central control to process all the information from the entire network. However, the new set-points may also been compromised. On the other hand, using the proposed distributed method results in a simple solution where each node only needs to decide to contribute to frequency or to voltage regulation based on knowing the worst node location, which is found using a local communication network. Due to the fact that set-points are predefined, it does not require to solve any optimization problem.

Chapter 4

Resilience-aware Optimal Power Flow

In the previous chapter, we considered a DN model with an infinite bus, i.e. the voltage at the substation node remains constant. However, any supply-demand disturbances in a DN will lead to change in the substation voltage as well as the system frequency. In this chapter, we relax the infinite bus assumption, and allow these parameters to change.

We introduce the *Resilience-Aware Optimal Power Flow* (RAOPF) problem, and discuss its relevance to optimal allocation and dispatch of contingency resources in the face of cyber-physical failures in electricity distribution networks. Our contribution is motivated by the need to adapt (and extend) the classical Security Constrained Optimal Power Flow (SCOPF) problem [5, 91] to the contingencies resulting from targeted compromise (attack) of remotely accessible nodes in distribution networks (DNs), for e.g., security attacks to DERs or electric vehicle (EV) charging facilities. We model DN as a radial network with bulk generator (BG) at the substation node as well as spatially distributed DERs. We assume that the BG has a finite ramp rate; thus, regulation of system frequency becomes relevant in our formulation (in addition to voltage regulation).[1] The RAOPF problem provides optimal dispatch of DERs and optimal shedding of controllable loads to limit the cost of maintaining regulation objectives during attack-induced contingencies.

The underlying challenge that motivates for our work is optimal resource allocation to improve resilience of DNs to simultaneous component failures that can lead to contingency events. We view DERs and controllable loads as *resources* that can be used

[1] Thus, our formulation is especially relevant to resiliency issues in isolated microgrids.

(dispatched) after the contingency events. For a given attack (or a compromised set of components), we say that a resource allocation is *more resilient* than another if an appropriately defined post-contingency cost (weighted sum of network costs and the cost of load control) is less than the cost in the latter case. Furthermore, we say that a resource allocation is *optimal* if it minimizes the sum of cost of resource allocation and the "worst-case" post-contingency cost under a set of failure scenarios. To capture these properties, we formulate a three-stage optimization problem with network and resource constraints to evaluate the total cost for a range of resource allocation strategies under security attacks to the DN nodes. We call this formulation as RAOPF to emphasize the resiliency improving aspect of the resulting allocation. Our solution illustrates important trade-offs in allocating spatially distributed resources by accounting for the nature of their contribution (active *vs.* reactive power) *and* their spatial location (upstream *vs.* downstream).

The RAOPF problem is constrained by the power flow equations which are physical laws and, therefore, must be satisfied. The other constraints include technological specifications of BG (droop characteristics), DERs (apparent power capability, active and reactive power setpoints), EV facilities (charging rate), and loads (controllable versus non-controllable parts). Finally, the operating constraints, which model the frequency and voltage regulation as well as line capacities, are imposed in the nominal mode. However, one or more of these operating constraints may be violated as a result of an adversarial action of the attacker; in our formulation, such violations result in a contingency. Thus, we view a *contingency* as a sudden, unplanned incident caused due to failure of one or more components that has a direct effect on the operating constraints of the DN [22].

To prevent or limit the impact of contingencies, we allow DERs to be allocated at the nodes of the DN, in addition to the supply by the BG; see Figure 4-1. Any point on the supply-demand balance line is a resource allocation that determines the amount of power supplied by the BG and the amount of power supplied by the DERs. If the controllable loads are also curtailed, then the supply-demand line shifts inwards due to reduction in aggregate demand. In our formulation, the capacity of an energy resource (BG or the DERs) in *excess* of the power supplied by the resource determines the *reserves* provided by that energy resource.

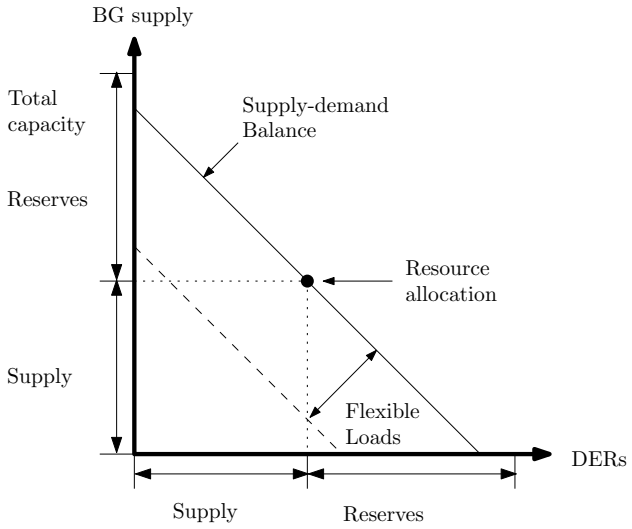


Figure 4-1: An illustration of power allocation through a BG and spatially distributed DERs.

In the post-contingency situation, violations of operational constraint(s) must be contained by the system operator (SO). If such violations are not resolved in a timely manner, additional components may fail, which can result in new contingencies. For example, significant loss of DER supply in highly loaded DNs may result in a drop in node voltages below a critical threshold causing other supply sources to trip, potentially resulting in a network effect (or cascade) [101]. Thus, planning for sufficient resources is essential so that the SO is able to meet regulation objectives in contingency situations. Typically, these objectives include voltage regulation (VR), frequency regulation (FR), and capacity management (CM) [30]. In particular, lack of adequate active power resources can cause loss of frequency regulation, and the scarcity of reactive power resources can lead to voltage fluctuations. In addition, in many situations, the capacity of one or more lines limits the reallocation of power that is needed to serve demand during contingencies [22, 35]. These factors have been identified as crucial for resilience of electricity grids [9, 22, 131], and are poised to become significant even for DNs.

In recent years, thanks to technological improvements and reduced cost of deployment, DERs have emerged as a promising solution for provision of reserves; in particular, by means of active and reactive power control [30, 128]. These functionalities are enabled by the appropriate power electronics and allow the DERs to respond to a range of fluc-

tuations in a fast manner (order of milliseconds) as opposed to the slower response via traditional means, which is typically in the order of few seconds to few minutes. Thus, allocation of DERs as reserves to facilitate fast response for meeting regulation objectives is an important problem in its own right; in this work, we instantiate this problem in the context of DN resilience.

Our work is also motivated by the SCOPF formulation which is used for contingency planning in transmission networks. In many transmission systems, the SOs solve some form of the SCOPF problem for the operational planning and dispatch by considering a given (a priori known) set of reliability failures [33]. By solving SCOPF, the SO is able to compute a resource allocation strategy which allows for timely response to any contingency resulting from these reliability failures. [5, 21, 91]. The idea behind our formulation is similar to SCOPF; the main distinction is that we capture the contingency situations resulting from the action of a strategic attacker to DN components.

We argue that the RAOPF problem can be used by the SO to compute the optimal resource allocation as well as response for DNs under strategic disruptions of supply/demand nodes. The problem is challenging because the individual objectives VR, FR and CM are not exactly aligned with each other. As a result, there are tradeoffs in the optimal resource allocation, which our modeling framework captures. Admittedly, the focus of RAOPF is limited to adversarial compromise of supply/demand DN nodes, and its extension to *all* possible N-k contingencies is an open question.[2] Still, RAOPF provides important insights regarding the structure of the optimal attack and the SO's strategies (both allocation and dispatch of reserves).

We formulate the RAOPF problem as a Stackelberg Game consisting of three levels (stages). The upper level (Stage 0) problem represents the SO's problem of resource allocation for optimal power flow and planning of reserves in anticipation of an attack. The middle level (Stage 1) problem represents a contingency model that captures the impact of attacker-induced failures on the aggregate supply-demand balance. In the lower level (Stage 2) problem, the SO controls available reserves to utilize the existing reserves, and

[2]If we explicitly enumerated all N-k contingencies, the number of constraints will increase exponentially with N and k. For example, with $N = 100$ and $k = 10$, the number of constraints will be of order 10^{13}, which makes the problem computationally hard.

if required, also impose load shedding. In the last two stages of the game, the objective of the attacker (resp. SO) is to maximize (resp. minimize) the post-contingency cost (i.e. weighted sum of cost incurred due to violation in VR, FR, and CM) and cost of load shedding subject to constraints due to power flow, and DER/load models. In the Stage 0, the SO's objective is to minimize the sum of cost of resource allocation and the maximin post-contingency cost.

The decisions in each of the three stages can be summarized as follows:

- *Stage 2*: Given a fixed reserve allocation and a fixed contingency, what is the optimal SO response in terms of dispatch of available resources (and load shedding)?
- *Stage 1*: Given a fixed reserve allocation, and the assumed attacker model, what is the optimal attack that maximizes the post-contingency cost, assuming the SO will respond optimally?
- *Stage 0*: What should be the optimal allocation of supply resources across the BG and DERs, assuming the optimal strategies of the attacker and the SO in stages 1 and 2, respectively?

In Sec. 4.1, we introduce our DN model and operating constraints. Then, in Sec. 4.2, we formulate the last two stages of the RAOPF problem as a bilevel optimization problem. Next, in Sec. 4.2, we present our computational approach to the bilevel problem, and evaluate its performance with the help of a case study. In Sec. 4.3, we append the Stage 0 to the bilevel problem and present the complete formulation of the RAOPF problem. Developing a computationally tractable solution approach to the RAOPF formulation is part of our ongoing work (and thus, it is beyond the scope of this contribution); however, we present a few insights on the optimal attacker strategy, and also discuss the main trade-offs faced by the SO in minimizing the post-contingency cost. These tradeoffs directly influence the qualitative structure of SO's resource allocation strategy. While the allocation strategies that we consider not necessarily optimal (in the sense of our RAOPF problem), we argue that their qualitative structure is relevant for construction of optimal allocation strategy.

4.1 Network model with "finite" substation bus

In this section, we first introduce the basic notations in our network model and define the state variables. Then, we describe the operating constraints, namely the power flow equations and operating limits. These constraints also include approximate models that relate the deviations in the frequency and nodal voltages in pre- and post-contingency modes (i.e., before and after an adversarial compromise).

Radial distribution network model

We build on the classical model for radial DNs [41, 113, 130] ; see Table 3.1 for notations. Consider a tree network of nodes and distribution lines $\mathcal{G} = (\mathcal{N} \bigcup \{0\}, \mathcal{E})$, where $\mathcal{N}$ denotes the set of all DN nodes. The substation node is labeled as 0. Let $N := |\mathcal{N}|$. A distribution line connecting node j to its parent node i in the tree network is denoted $(i, j) \in \mathcal{E}$. Each distribution line $(i, j) \in \mathcal{E}$ has a complex impedance $\mathbf{z}_j = \mathbf{r}_j + \mathbf{j}\mathbf{x}_j$, where $\mathbf{r}_j > 0$ and $\mathbf{x}_j > 0$ denote the resistance and inductance of the line (i, j), respectively, and $\mathbf{j} = \sqrt{-1}$.

We distinguish between two *modes*, denoted $\eta \in \{o, c\}$, where o and c denote the pre- and post- contingency modes, respectively. The state vector in mode η, denoted $\mathrm{x}^\eta \in \mathbb{R}^{4N}$, is defined as:

$$\mathrm{x}^\eta := \left[pc^\eta, qc^\eta, pg^\eta, qg^\eta \right],$$

where pc_j^η and pg_j^η (resp. qc_j^η and qg_j^η) denote the active (resp. reactive) power consumption and generation at node j. For a given mode η, let P_j^η and Q_j^η denote the active and reactive power flowing from node i to node j on the line $(i, j) \in \mathcal{E}$; V_i^η denote the voltage magnitude of node i; see power flow equations in (4.1) below. Throughout this chapter, $\mathrm{x}^\eta, V^\eta, pc^\eta, qc^\eta, pg^\eta, qg^\eta, P^\eta, Q^\eta$ are row vectors of appropriate dimensions.

In our model, the BG is connected to the substation node 0, and any other node $i \in \mathcal{N}\backslash\{0\}$ may or may not have a DER connected to it. Let f_0^η denote the frequency of the BG, and f_i^η denote the frequency of DER at node i. Throughout, we will assume that the frequencies of individual DERs are synchronized with that of the BG, i.e. $f_i^\eta = f_0^\eta$. Thus, we refer the BG frequency as the *system frequency*, and drop the subscript 0 in f_0^η. We

will nominally assume that $f^n = 60$ Hz and $V_0^n = 1$ pu in the pre-contingency mode.

Constraints

The constraints in our network model comprise of the power flow equations, voltage/frequency deviation models, operating limits in the pre-contingency mode, and models of generators (BG and DERs) and loads (EV and non-EV components).

Linear Power Flows (LPF): For a state x^η, the standard LPF model can be written as [41, 53]:

$$P_j^\eta = \sum_{k:(j,k)\in\mathcal{E}} P_k^\eta + pc_j^\eta - pg_j^\eta \qquad \forall\, j \in \mathcal{N}, \eta \in \{o, c\} \tag{4.1a}$$

$$Q_j^\eta = \sum_{k:(j,k)\in\mathcal{E}} Q_k^\eta + qc_j^\eta - qg_j^\eta \qquad \forall\, j \in \mathcal{N}, \eta \in \{o, c\} \tag{4.1b}$$

$$V_j^\eta = V_i^\eta - \mathbf{r}_j P_j^\eta - \mathbf{x}_j Q_j^\eta \qquad \forall\, (i,j) \in \mathcal{E}, \eta \in \{o, c\} \tag{4.1c}$$

Here, (4.1a) (resp. (4.1b)) is the active (resp. reactive) power conservation equations; (4.1c) relates the voltage drop and the power flows. We will use the notation $\mathcal{X}^n$ and $\mathcal{X}^c$ to denote the sets of states that satisfy (4.1) for $\eta = o$ and $\eta = c$, respectively.[3]

Frequency and voltage deviation models: In our model, the ramp rate of BG is a limiting factor and impacts the deviation in system frequency as well as the deviation in nodal voltages between pre- and post-contingency modes. Following [10, 26], the change in frequency and substation voltage from the pre-contingency state x^n to post-contingency state x^c are related as follows:

$$f^n - f^c = -\boldsymbol{f^{reg}} \left(P_0^n - P_0^c\right) \tag{4.2a}$$

$$V_0^n - V_0^c = -\boldsymbol{V^{reg}} \left(Q_0^n - Q_0^c\right), \tag{4.2b}$$

where $\boldsymbol{f^{reg}}$ is the frequency regulation (or droop) constant of the BG that captures the change in frequency (in Hz) per unit additional active power supplied into the substation node, and $\boldsymbol{V^{reg}}$ is the voltage regulation constant of the BG that captures the per unit

[3] Note that, in this contribution, we used the LPF model for the sake of simplicity and computational tractability. However, our main ideas are also relevant to DN with nonlinear power flows.

change in voltage per unit additional reactive power supplied into the substation node.

Operating limits: Let $\boldsymbol{f_i^{min}}$ and $\boldsymbol{f_i^{max}}$ denote the (given) allowable lower and upper bounds within which the system frequency should operate for the DER at node i, and define $\underline{\mathbf{f}} := \max_{i\in\mathcal{N}} \boldsymbol{f_i^{min}}$ and $\overline{\mathbf{f}} := \min_{i\in\mathcal{N}} \boldsymbol{f_i^{max}}$. Similarly, let $\underline{\mathbf{V}}_i$ and $\overline{\mathbf{V}}_i$ denote the lower and upper bounds within which the voltage at node i should be maintained. Finally, let $\overline{\mathbf{S}}_j$ denote the maximum power carrying capacity of line (i,j).

Now, we can state the operating limits for the pre-contingency state x^n:

$$\underline{\mathbf{f}} \leqslant f^n \leqslant \overline{\mathbf{f}} \tag{4.3a}$$

$$\underline{\mathbf{V}}_i \leqslant V_i^n \leqslant \overline{\mathbf{V}}_i \quad \forall\, i \in \mathcal{N} \tag{4.3b}$$

$$\left(P_j^n\right)^2 + \left(Q_j^n\right)^2 \leqslant \overline{\mathbf{S}}_j{}^2 \quad \forall\, j \in \mathcal{N} \quad \text{s.t. } (i,j) \in \mathcal{E} \tag{4.3c}$$

where (4.3a) and (4.3b) specify the lower and upper bounds for the system frequency and nodal voltages, and (4.3c) models the capacity of the distribution lines.

In principle, similar regulation requirements can also be stated for the post-contingency state x^c. However, in our framework the post-contingency state is a result of attacker-SO interaction and thus, cannot be expressed explicitly. Thus, we choose to model the worst-case contingency (see Sec. 4.2) and consider violations in operating limits in the post-contingency mode as costs (as opposed to constraints).

Bulk Generator and DER model: Let $sg_i := pg_i + \mathbf{j}qg_i$ denote the complex power supplied by the generator at the node i, where pg_i and qg_i denote the active and reactive power components. The generator output is constrained as follows:

$$sg_i \in \mathcal{S}_i,$$

where $\mathcal{S}_i$ is assumed to be a convex set [28, 130]. We consider the following convex sets as candidates for $\mathcal{S}_i$:

$$\mathcal{S}_i^{circ} := \{(p,q) \mid 0 \leqslant p \leqslant \overline{\mathbf{pg}}_i, \underline{\mathbf{qg}}_i \leqslant q \leqslant \overline{\mathbf{qg}}_i, p^2 + q^2 \leqslant \overline{\mathbf{sg}}_i{}^2\}, \text{or} \tag{4.4}$$

$$\mathcal{S}_i^{poly} := \{(p,q) \mid 0 \leqslant p \leqslant \overline{\mathbf{pg}}_i, \underline{\mathbf{qg}}_i \leqslant q \leqslant \overline{\mathbf{qg}}_i, A_i^p p + A_i^q q \leqslant b_i\}, \tag{4.5}$$

where $\overline{\mathbf{pg}}_i$ denotes the maximum active power bound for the DER output, and $\underline{\mathbf{qg}}_i$, $\overline{\mathbf{qg}}_i$ denote the minimum and maximum reactive power bounds. Note that if node i has no DER, we can conveniently choose $\overline{\mathbf{sg}}_i = 0$. Finally, we denote the set of feasible set-points for all the generators (i.e., BG and DERs) by $\mathcal{S} := \prod_{i \in \mathcal{N}} \mathcal{S}_i$.

Load models: For the sake of illustration, we consider that Electric Vehicles (EVs) connected to the DN are the only nodes vulnerable to compromise by the attacker. Without loss of generality, we assume that each node has an EV load and a non-EV load. For the mode η, let se_i^η and sn_i^η denote power consumed by the EV and non-EV load at node i. Then, the total power consumed, sc_i^η can be written as:

$$sc_i^\eta = se_i^\eta + sn_i^\eta. \tag{4.6}$$

Next, we introduce non-EV and EV load models.

Non-EV load model: We assume that non-EV loads are constant power loads.[4] Let $\overline{\mathbf{sn}}_i$ denote the nominal demand of non-EV load at node i. However, to maintain the operating limits of the DN in the post-contingency mode, we allow the SO to shed a part of nominal load. This flexibility is modeled by introducing a parameter $\beta_i^\eta \in [0, \overline{\beta}_i]$, where $\overline{\beta}_i \in [0, 1]$ denotes the maximum load control capability at the node i. As an example, $\overline{\beta}_i = 0.1$ would mean that a maximum of 10% of the non-EV load at node i can be shed. Thus, the actual power consumed by the non-EV load can be expressed as follows:

$$sn_i^\eta = (1 - \beta_i^\eta)\overline{\mathbf{sn}}_i. \tag{4.7}$$

For simplicity, we also assume that the SO fulfills all non-EV demand in the pre-contingency mode, i.e. $\beta_i^n = 0 \; \forall \; i \in \mathcal{N}$.

EV load model: Typically, EV loads are modeled as constant power loads. For simplicity, we only allow two charging rates for each EV; viz. slow and fast. Let $\mathcal{S}_i^e = \{\underline{\mathbf{se}}_i, \overline{\mathbf{se}}_i\}$ denote the set of charging rates of EV at node i, where $\underline{\mathbf{se}}_i$ (resp. $\overline{\mathbf{se}}_i$) is the slow (resp.

[4] More generally, non-EV loads can be modeled using the constant impedance (Z), constant current (I), constant power (P) or a general ZIP model. The non-EV power consumption can also change due to frequency deviations. Our network model can be extended to include these general load models.

fast) charging rate of EV at node i. Thus, the power consumed by the EV load is given by:

$$se_i^\eta = \delta_i^\eta \overline{\mathbf{se}}_i + (1 - \delta_i^\eta)\underline{\mathbf{se}}_i, \tag{4.8}$$

where the binary variable $\delta_i^\eta = 0$ (resp. $\delta_i^\eta = 1$) indicates the slow (resp. fast) charging rate.

Henceforth, we will limit our attention to attacker-induced compromise of EVs, i.e. we focus on a scenario in which a subset of EVs can be simultaneously compromised by an external adversary to induce the contingency mode. Before moving further, we want to emphasize that we selected the specific scenario of attack to EVs for the sake of concreteness. Indeed, our approach can be adopted to other scenarios that require resource allocation and dispatch on part of the SO to resolve the supply-demand imbalance created as a result of cyber-physical failures (attack).

4.2 Bilevel problem

In this section, we describe the attacker-SO interactions during the contingency caused by compromise of vulnerable EV loads. Specifically, we consider the contingency caused by a simultaneous compromise of EV loads from low to high charging rates which results in a sudden increase in the aggregate demand [13]. The attacker selects the EVs in a targeted manner to induce violations in one or more operating limits, which can result in an increased cost of regulation for the SO in the post-contingency mode. To limit this cost, the SO responds by dispatching the DERs as contingency reserves, and if necessary, by exercising load control. Thus, the attacker's (resp. SO's) objective is to maximize (resp. minimize) the post-contingency cost (sum of attacker-induced network operating costs and forced /load shedding).

We model the attacker-SO interaction as a sequential game in which, the attacker moves first, and the SO responds next. We now describe these stages in detail.

Attack stage: Let $\mathcal{D}_{\mathrm{k}} := \{\delta \in \{0,1\}^{\mathcal{N}} \mid \sum_{i\in\mathcal{N}} \delta_i \leqslant \mathrm{k}\}$ denote the set of feasible strategies of a resource-constrained attacker. In our model, the attacker chooses a subset of EVs to compromise, and sets their rate of charging to $\delta^a \in \mathcal{D}_{\mathrm{k}}$. Here, $\delta_i^a = 1$ means

that EV at node i is compromised and starts charging at the faster rate; $\delta_i^a = 0$ implies otherwise. The attacker's action is constrained as follows:

$$\sum_{i \in \mathcal{N}} \delta_i^a \leqslant \mathrm{k}, \tag{4.9}$$

where (4.9) states that at most k EV nodes are compromised. Recalling (4.8), we know that the attacker's action determines the effective charging rates in the post-contingency mode:

$$\delta^c = \delta^a. \tag{4.10}$$

The resource constraint (4.9) on attacker's action captures his limited capability in compromising spatially distributed EVs. We justify this constraint in the following way: First, the EV nodes are likely to be heterogeneous in their design and manufacturer type. The attacker may not have specific attack paths for each EV type. Second, the process of EV integration with DNs is gradual in nature, and there aren't any security regulations that the EV facilities must implement. Some of them may install intrusion prevention/detection tools to safeguard the software controlling the charging rate and/or preventing the EVs from over-charging; however, the remaining facilities will remain vulnerable. Third, certain electric cars may have a buggy control software that is vulnerable to a virus, which can compromise certain types of EV facilities [98]. Hence, the number of facilities that could be compromised simultaneously may be proportional to the number of electric cars with the buggy control software.

Without much loss of generality, we assume that the EVs when fully charged do not remain connected to the DN and, hence, are not vulnerable to attack; i.e., the attacker only targets the EVs that are not fully charged. As a consequence, we do not include the state-of-charge constraints of the EVs in our model. Furthermore, to induce the maximal impact in the post-contingency mode, the attacker will only target EVs that were charging at the slow rate in the pre-contingency mode. Hence, for simplicity, we can assume that for all EV nodes, $\delta_i^n = 0$ in (4.8), i.e. $se_i^n = \underline{\mathbf{se}}_i$.

Note that attacks to other components (e.g., DERs, non-EV loads) can be modeled in a similar manner. For e.g., in our previous work [111, 113], we considered attacks

that manipulated DER setpoints. Thus, while the specific channel of attack might vary across different scenarios, the net effect is change in network state between pre- and post-contingency modes (to see this, notice how (4.6)-(4.8) and (4.10) affect (4.1) and (4.2)). Also note that, although issues such as reverse power flows and overvoltages do not arise in our model, they may become relevant in other scenarios, for e.g., when the attacker introduces sudden disconnection of loads or simultaneously turns a large number of EVs to slow charging rate. We expect that even in such scenarios, the basic nature of attacker-SO interaction will be similar to our model.

SO response stage: Let $\mathcal{U} := \mathcal{S} \times \Gamma$, where $\Gamma := \prod_{i\in\mathcal{N}}[0, \overline{\beta}_i]$. In our model, the SO responds to attacker actions by choosing the set-points of the non-compromised DERs and, if needed, impose load curtailment at one or more nodes according to a strategy $\left[sg^c, \beta^c\right] =: u \in \mathcal{U}$. Essentially, the SO chooses new set-points sg^c of non-compromised DERs, and load control parameters β^c to reduce the post-contingency cost. These choice variables are captured by strategy vector ϕ.

We make the standard assumption that the SO knows the nominal non-EV ($\overline{\mathbf{sn}}$) and EV demand ($\underline{\mathbf{se}}$). Additionally, we assume that, the SO has full observability of network state; this can be achieved by continuously monitoring nodal voltages. Under this assumption, the SO can determine the identity of compromised EVs and use this knowledge to compute the optimal response to attack. Relaxing this assumption would entail designing SO response with imperfect state information. While this issue is of practical relevance, we do not pursue it here.

For a fixed resource allocation in the pre-contingency mode (i.e., for given x^n), we can now represent attack and SO response stages in the following maximin (or bilevel) formulation as follows:

$$\begin{aligned}[\text{Maxmin}]\ \mathcal{L}(\mathrm{x}^n) \ :=\quad & \max_{\delta^a\in\mathcal{D}_{\mathrm{k}}} \ \min_{u\in\mathcal{U}} \ C_{\text{loss}}(\mathrm{x}^n, \mathrm{x}^c(\delta^a, u)) \\ & \text{s.t. } (4.1), (4.2), (4.6) \text{ - } (4.8), (4.10)\end{aligned} \tag{4.11}$$

Here, we model the post-contingency cost as a sum of the cost due to voltage bound violation (C_{VR}), the cost due to frequency bound violation (C_{FR}), and the cost due to load

control:[5]

$$C_{\text{loss}} := C_{\text{VR}} + C_{\text{FR}} + C_{\text{LC}} \tag{4.12a}$$

$$C_{\text{VR}}(\mathrm{x}^n, \mathrm{x}^c) := \mathrm{W}_{\text{VR}} \max_{i \in \mathcal{N}} \max\left(\underline{\mathbf{V}}_i - V_i^c, V_i^c - \overline{\mathbf{V}}_i, 0\right) \tag{4.12b}$$

$$C_{\text{FR}}(\mathrm{x}^n, \mathrm{x}^c) := \mathrm{W}_{\text{FR}} \max\left(\underline{\mathbf{f}} - f^c, f^c - \overline{\mathbf{f}}, 0\right) \tag{4.12c}$$

$$L_{\text{LC}}(\mathrm{x}^n, \mathrm{x}^c) := \mathrm{W}^{\text{LC}} \cdot \beta^c, \tag{4.12d}$$

where W_{VR} and W_{FR} denote the coefficients assigned to the voltage and frequency regulation objectives, and the vector $\mathrm{W}^{\text{LC}} \in \mathbb{R}_+^N$ represents the cost of unit load shedding after the contingency. Note that, in (4.12b), the cost of voltage regulation is the defined as the maximum voltage bound violation over all nodes.

Although the [Maxmin] problem does not consider nonlinear power flow, it turns out that optimal value of this problem is a lower bound of the maximin loss in the post-contingency mode under nonlinear power flows [19]. Furthermore, under certain additional assumptions, we can also use solution to the [Maxmin] problem for an appropriately modified LPF model to upper bound the maximin loss. For more details on establishing these bounds, we refere the reader to [19].

Greedy heuristic approach for [Maxmin] problem

We now focus on solving the [Maxmin] problem which is a bilevel mixed integer linear program with the inner problem being a linear program. A standard approach to solving such problems is the KKT-based reformulation approach which gives a single level mixed-integer linear program (MILP) [92, 142, 145]. In principle, the MILP reformulation can be used to solve the [Maxmin] problem for small-sized networks. However, scaling this approach to larger networks is not straightforward, and entails finding reasonable upper bounds on the Lagrange multipliers in the KKT conditions. In our previous work [111, 113], we have investigated an alternative approach which exploits the properties of linear power flows on radial networks to develop a greedy heuristic that is scalable to large-

[5]For simplicity, we only focus on voltage and frequency regulation, and do not consider congestion management (CM) as a regulation objective. That is, we assume that constraints (4.3c) will not be active.

sized networks. We apply this heuristic to the [Maxmin] problem. With the help of a case study, we also compare the results obtained from this heuristic with those obtained by the KKT-based MILP reformulation approach and brute force (when possible).

Before proceeding further, we need to introduce some additional notation. For any

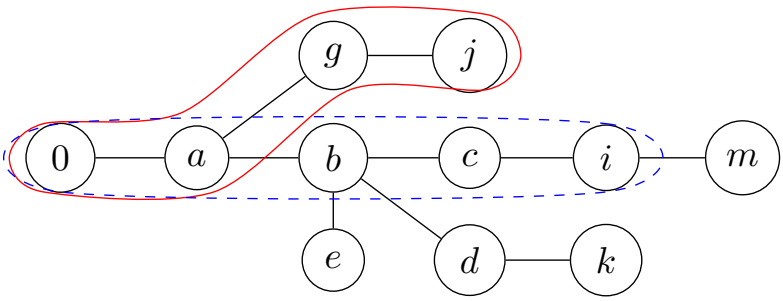


Figure 4-2: Precedence description of the nodes for a tree network. Here, $j \prec_i k$, $e =_i k$, $b \prec k$, $\mathcal{P}_j = \{a, g, j\}$, $\mathcal{P}_i \cap \mathcal{P}_j = \{a\}$.

given node $i \in \mathcal{N}$, let $\mathcal{P}_i$ be the path from the root node to node i. Thus, $\mathcal{P}_i$ is an ordered set of nodes starting from the root node and ending at node i, excluding the root node; see Figure 4-2. We say that node j is an *ancestor* of node k ($j \prec k$), or equivalently, k is a successor of j *iff* $\mathcal{P}_j \subset \mathcal{P}_k$. We define the *relative ordering* $\preceq_i$, with respect to a "pivot" node i as follows:

- j *precedes* k ($j \preceq_i k$) *iff* $\mathcal{P}_i \cap \mathcal{P}_j \subseteq \mathcal{P}_i \cap \mathcal{P}_k$.

- j *strictly precedes* k ($j \prec_i k$) *iff* $\mathcal{P}_i \cap \mathcal{P}_j \subset \mathcal{P}_i \cap \mathcal{P}_k$.

- j is at the *same precedence level* as k ($j =_i k$) *iff* $\mathcal{P}_i \cap \mathcal{P}_j = \mathcal{P}_i \cap \mathcal{P}_k$.

We define the common path impedance between any two nodes $i, j \in \mathcal{N}$ as the sum of impedances of the lines in the intersection of paths $\mathcal{P}_i$ and $\mathcal{P}_j$, i.e., $\boldsymbol{Z_{ij}} := \sum_{k \in \mathcal{P}_i \cap \mathcal{P}_j} \mathbf{z}_k$, and denote the resistive (real) and inductive (imaginary) components of $\boldsymbol{Z_{ij}}$ by $\boldsymbol{R_{ij}}$ and $\boldsymbol{X_{ij}}$, respectively. $\boldsymbol{Z}$, $\boldsymbol{R}$ and $\boldsymbol{X}$ denote the corresponding matrices of appropriate sizes.

We can use the abovementioned notion of node precedence to describe the structure of an optimal attack given a *fixed* SO action (or response).

4.2.1 Optimal attack for fixed SO response

Following the standard approach [72, 102], we define the master problem [Maxmin-a] (respectively, subproblem [Maxmin-d]) for fixed SO action $u \in \mathcal{U}$ (respectively, fixed attacker action $d \in \mathcal{D}_{\mathrm{k}}$) as follows:

$$\text{[Maxmin-a]} \quad d^{\star}(\phi) \in \underset{d \in \mathcal{D}_{\mathrm{k}}}{\operatorname{argmax}} C_{\text{loss}}\left(\mathrm{x}^{n}, \mathrm{x}^{c}(d, u)\right)$$
$$\text{s.t. } (4.1), (4.2), (4.6) \text{ - } (4.8), (4.10)$$
$$\text{[Maxmin-d]} \quad u^{\star}(d) \in \underset{u \in \mathcal{U}}{\operatorname{argmin}} C_{\text{loss}}\left(\mathrm{x}^{n}, \mathrm{x}^{c}(d, u)\right)$$
$$\text{s.t. } (4.1), (4.2), (4.6) \text{ - } (4.8), (4.10)$$

Recall that the inner problem [Maxmin-d] is a linear program, whereas the outer problem [Maxmin-a] is a mixed-integer program. We now focus on understanding the properties of the master problem which will help in developing a greedy heuristic for the [Maxmin] problem.

For a fixed SO response, the cost of load control becomes constant. Hence, the post-contingency cost, C_{loss}, only comprises of C_{VR} and C_{FR} terms. We make three claims which provide insights about the attacker's optimal attack strategy. We refer the reader to [111, 113] to gain intuition about formal proofs of these claims.

Let $\Delta_j(f)$ denote the change in the system frequency due to an individual disruption of EV at node j. Then, thanks to LPF model, if two EVs are identical, then the change in system frequency due to individual disruption of the EVs will also be identical regardless of the location of the EVs in the network:

Claim 1. $\quad \mathcal{S}_j^e = \mathcal{S}_k^e \implies \Delta_j(f_0) = \Delta_k(f_0).$

Claim 1 implies that if the attacker focuses only on maximizing FR, then the attacker has no preference between attacking one of the two identical EVs regardless of their location in the network.

Now, with a slight abuse of notation, let $\Delta_j(V_i)$ denote the change in the voltage at

node i due to an individual disruption of EV at node j. Our second claim is as follows: if the EVs at node j and k are identical, and node j is upstream of node k relative to node i ($j \prec_i k$), then the impact on V_i due to individual EV disruption at node j will be smaller than the impact due to individual EV disruption at node k, that is:

Claim 2. $\mathcal{S}_j^e = \mathcal{S}_k^e$ and $j \prec_i k \implies \Delta_j(V_i) < \Delta_k(V_i)$.

Finally, let $\Delta_J(V_i)$ (resp. $\Delta_J(f)$) denote the change in the voltage at node i (resp. system frequency) due to disruption of EVs at nodes $j \in J$. Then, our third claim directly follows from the linearity of LPF model:

Claim 3. $\Delta_J(V_i) = \sum_{j\in J} \Delta_j(V_i)$ and $\Delta_J(f) = \sum_{j\in J} \Delta_j(f)$.

In summary, while voltage regulation is affected by both spatial structure and extent of compromise, the frequency regulation is only affected by the latter factor.

4.2.2 Greedy Heuristic

Algorithm 7 Pivot node Algorithm

```
Calculate V^n (pre-contingency voltage profile).
for i ∈ 𝒩 do
    for j ∈ 𝒩 do
        Compute Δ_j(V_i, f)
        Sort j s in decreasing order of Δ_j(V_i, f) → (π_1, ..., π_N)   ▷ (Claims 1 and 2)
        Set J_i^⋆ = (π_1, ··· , π_k) by choosing first k nodes.
        Calculate Δ_{J_i^⋆}(V_i, f) = Σ_{j∈J_i^⋆} Δ_j(V_i, f)           ▷ (Claim 3)
    end for
end for
Find i^⋆ = argmax_{k∈𝒩} (L_k + Δ_{J_k^⋆}(V_k, f))
return J_{i^⋆}^⋆.
```

Based on our claims in Sec. 4.2.1, we propose our the following greedy heuristic. (This heuristic was first presented in [18].) But first, we need to introduce Algorithm 10 which computes an optimal attack for a given (fixed) SO response, i.e., it solves [Maxmin-a].

Consider an arbitrary "pivot" EV as a candidate node targeted by the attacker, who aims to maximize the weighted sum of losses due to voltage and frequency bound violations. (Again, since we are considering SO action as fixed, the cost of load control can be ignored.) Thus, the attacker's objective is maximize the affine function $L_i =$

$\mathrm{W_{VR}}(\underline{\mathbf{V}}_i - V_i^c) + \mathrm{W_{FR}}(\underline{\mathbf{f}} - f^c)$. Infact, for compromise of any pivot EV node, the resulting effect on (or contribution to) L_i can be computed very easily, thanks to the linear power flow assumption. Let this effect be denoted by $\Delta_j(V_i, f)$. Now, sort the EV nodes in decreasing order of the effects on L_i due to their individual disruptions $\Delta_j(V_i, f)$, and pick the top k nodes.[6] Assuming that the attacker will target these k EV nodes, compute the optimal SO response and the post-contingency loss.

Then, repeat the same procedure with a different node as a pivot node. If the post-contingency loss with the new node as the pivot node is higher, update the values for the current best attacker strategy and the current best post-contingency cost. Iterate over the remaining nodes and repeat the procedure until all the nodes are exhausted.

Now, we can propose our greedy heuristic (GH), which iterates between solving the master problem (with fixed SO actions) and the subproblem (with fixed attacker actions), with successively increasing maximin values of post-contingency losses. In the first iteration, fix the SO response to the pre-contingency values, i.e. $sg^c = sg^n, \beta^c = \beta^n$, and compute the optimal attacker strategy as the solution of [Maxmin-a] by implementing the pivot node algorithm. Then, consider this attacker strategy as fixed, and compute an optimal SO response as well as the post-contingency cost by solving [Maxmin-d]. In the next iteration, consider the new SO response as fixed, and again compute the optimal attacker strategy. Then, fixing the new attacker strategy, compute the optimal post-contingency cost. If this cost is smaller than the previously computed post-contingency cost, we terminate the heuristic. Otherwise, we continue to iterate between the master- and the sub-problems until we get some attacker strategy twice. Since, the number of optimal attacker strategies is finite, the greedy heuristic is bound to terminate. However, we observe that the heuristic converges to optimality in few iterations. Indeed, we observed that our heuristic provides optimal solutions in less than 5 iterations for medium sized networks of size 37.

[6] A similar pivot node algorithm is presented in [74].

4.2.3 Evaluation of the greedy heuristic

We describe a set of computational experiments to evaluate the performance of the greedy heuristic (GH) in solving the 2-stage subgame. Specifically, we compare the GH solution against the solutions obtained by the KKT approach mentioned at the beginning of this section and also brute force (BF). We also evaluate the effect of weights on post-contingency costs for a range of k values; see attacker's resource constraint (4.9).

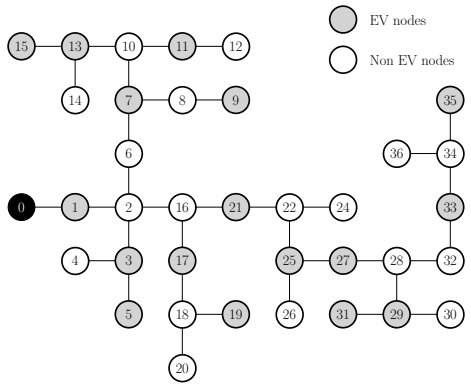


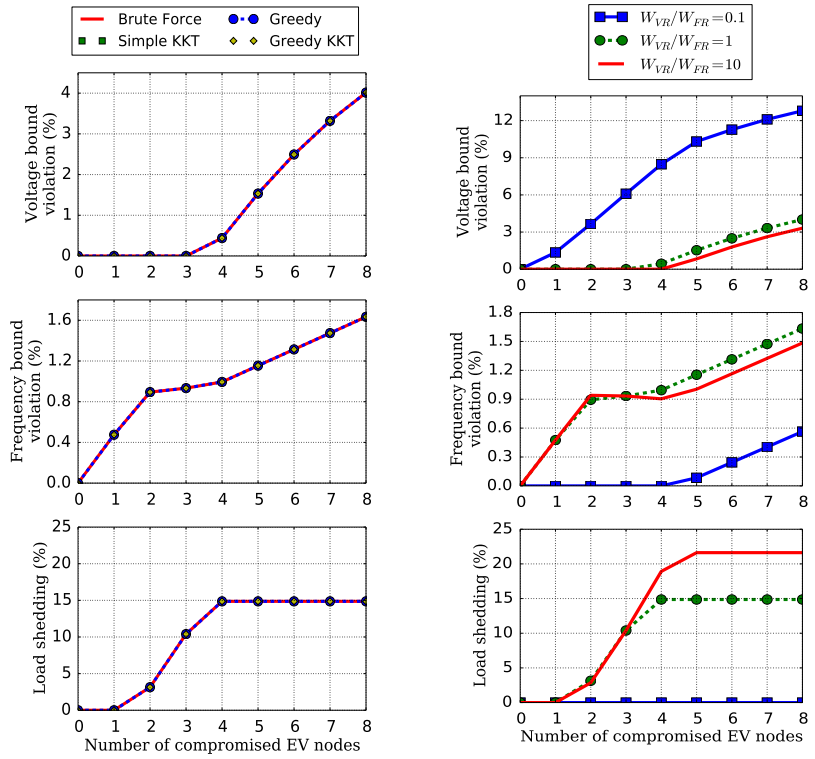
Figure 4-3: Modified IEEE 37 Node Network.

Network Setup. Our simulation setup is as follows: We consider a modified IEEE 37 node network as shown in Figure 4-3. Each line has an identical impedance of $\mathbf{z}_j = 0.01 + 0.02\mathbf{j}$, and each node has one DER and one non-EV load. The set of feasible DER setpoints is given by:

$$\mathcal{S}_i^{poly} = \{p + \mathbf{j}q \mid p \geqslant 0,\ -a \leqslant q \leqslant a,\ 4p + 3q \leqslant 5a,\ 4p - 3q \leqslant 5a\},$$

where $a = 0.04$ is a parameter; see (4.5). In the slow-charging mode, each EV load is $se_i^n = 2(1 + 0.33\mathbf{j})a$. In the fast-charging mode, each EV draws twice the power drawn in slow-charging mode: $se_i^a = 4(1 + 0.33\mathbf{j})a$. The non-EV demand at each node is $\overline{\mathbf{sn}}_i = 0.03 + 0.01\mathbf{j}$, and the maximum load control parameter is $\overline{\beta}_i = 0.5$, i.e. 50% of the non-EV load can be shed at each node. For the sake of simplicity, we assume that all DERs, non-EV loads and EVs are homogeneous. Furthermore, the black node in Figure 4-3 is the substation node, the grey colored nodes are the nodes with EVs, and the remaining nodes do not have EVs.

We assume the following cost parameters: the cost of per unit load shedding, per unit voltage bound violation, and per unit frequency bound violation is chosen to be $\mathrm{W}^{\mathrm{LC}} = 1, \mathrm{W}_{\mathrm{VR}} = 250, \mathrm{W}_{\mathrm{FR}} = 250$, respectively; see (4.12). The voltage and frequency regulation constants in (4.2) are chosen as $\boldsymbol{V}^{reg} = 0.01$ and $\boldsymbol{f}^{reg} = 0.02$.



(a) Comparison of algorithms - 37 node network.

(b) Post-contingency losses for different weights of regulation objectives.

Figure 4-4: Evaluation of the greedy heuristic.

GH *vs.* KKT *vs.* BF. Figure 4-4a shows percentage voltage bound violation $\left(100 \max_i \max\left(\frac{\underline{\mathbf{V}}_i - V_i^c}{V_0}, \frac{V_i^c - \overline{\mathbf{V}}_i}{V_0}, 0\right)\right)$, percentage frequency bound violation $\left(100 \max\left(\frac{\underline{\mathbf{f}} - f^c}{f_0}, \frac{f^c - \overline{\mathbf{f}}}{f_0}, 0\right)\right)$, and percentage load shedding $\left(\frac{100}{N}\sum_i \beta_i^c\right)$ as the number of EV nodes compromised increases. The pre-contingency setpoints are chosen to be $sg_i^n = (0.9 + 0.33\mathbf{j})a$. Note that the GH provides an optimal solution in this setting. Also note that, for the chosen weight parameters and $\mathrm{k} = 1$, C_{VR} and L_{LC} are both zero, but C_{FR} is positive, which implies that SO tolerates some frequency bound violation to maintain voltage regulation and full demand satisfaction. This shows that SO tolerates some frequency bound violation at the expense of no load control. For slightly higher intensity

attacks ($\mathrm{k} = 2, 3$) the SO starts imposing load control. However, as k increases further, the load control saturates at 15% for $\mathrm{k} \geqslant 4$, although the total load control capability is 50%. This observation has been detailed in the previous work; see Chapter 3. Intuitively, initial shedding of downstream loads reduces the post-contingency cost because the active and reactive power reduction contributes to reduction in both C_{FR} and C_{VR}. Indeed, when the SO exhausts the load control capability of the downstream nodes, control of nodes that are upstream is not as beneficial in reducing C_{VR}. Hence, the saturation in cost of load control.

In Figure 4-4b, we fixed the W^{LC} and varied the $\mathrm{W}_{\mathrm{VR}}/\mathrm{W}_{\mathrm{FR}}$ ratio. The different $\mathrm{W}_{\mathrm{VR}}/\mathrm{W}_{\mathrm{FR}}$ ratios correspond to different weights given to voltage and frequency regulation objectives. Note that for $\mathrm{W}_{\mathrm{VR}}/\mathrm{W}_{\mathrm{FR}} = 0.1$, the SO exerts no load control, but for higher $\mathrm{W}_{\mathrm{VR}}/\mathrm{W}_{\mathrm{FR}}$, there is load control. This indicates that the load control is more effective in reducing C_{VR} than in reducing C_{FR}. Indeed, a reduction in the load reduces both active and reactive power demand. However, the C_{FR} is affected only by active power reduction (see (4.2a)), whereas the C_{VR} is affected by both active and reactive power reduction (see (4.1c)). Hence, load control directly reduces C_{VR}, and also indirectly reduces C_{FR}. Again, the L_{LC} reaches a saturation level after the downstream nodes' capability of load control is exhausted. Additionally, as the $\mathrm{W}_{\mathrm{VR}}/\mathrm{W}_{\mathrm{FR}}$ ratio increases, the saturation level is reached for a higher intensity attack; and also attains a higher saturation value.

4.3 Trilevel optimization problem

In this section, we extend the [Maxmin] bilevel formulation to a tri-level framework with the outermost level denoting the resource allocation stage. We call this extended formulation the RAOPF problem:

$$
\begin{aligned}
[\text{RAOPF}]\ \mathcal{L} \ :=\ & \min_{\mathrm{x}^n \in \mathcal{X}^n} C_{\text{alloc}}(\mathrm{x}^n) + C_{\text{loss}}(\mathrm{x}^n(a), \mathrm{x}^c(\delta^{a\star}, u^\star)) \\
& \text{s.t.}\ \ (4.3), (4.6)\text{ - }(4.8) \\
& (\delta^{a\star}, u^\star) \in \arg\max_{\delta^a \in \mathcal{D}_{\mathrm{k}}} \min_{u \in \mathcal{U}}\ C_{\text{loss}}(\mathrm{x}^n(a), \mathrm{x}^c(\delta^a, u)) \\
& \qquad \text{s.t. } \mathrm{x}^c \in \mathcal{X}^c, (4.2), (4.6)\text{ - }(4.8), (4.10)
\end{aligned}
\tag{4.13}
$$

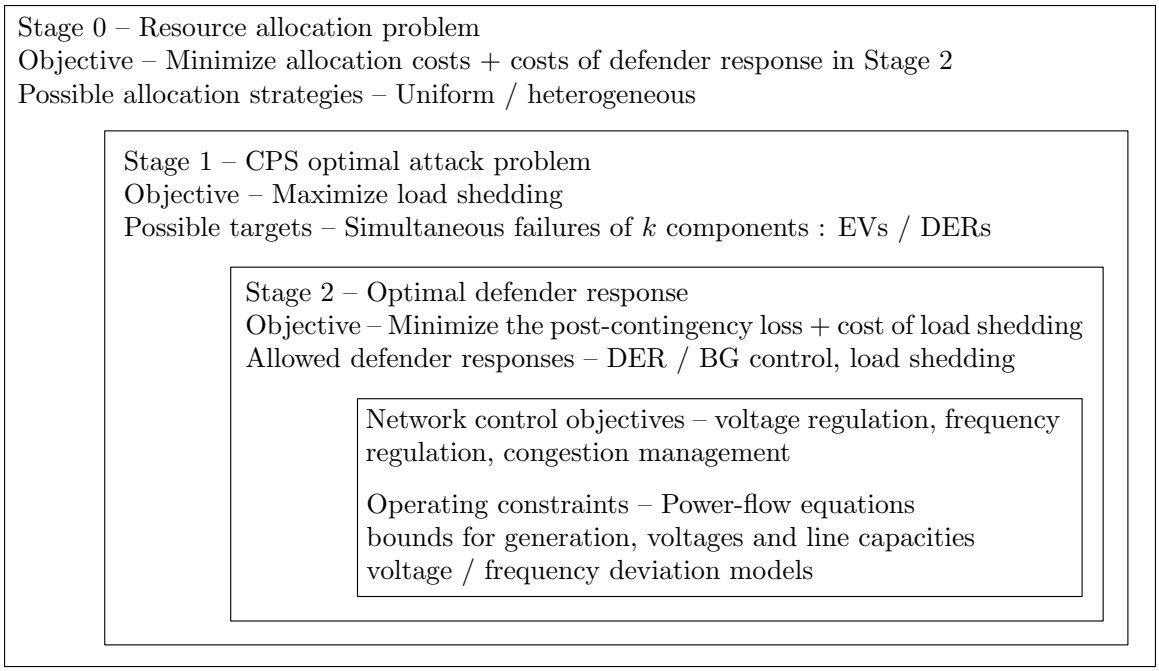


Figure 4-5: Modeling framework.

The overall framework of the trilevel RAOPF problem can be summarized as in Figure 4-5. The [RAOPF] game is a sequential game of perfect information, i.e. each player is perfectly informed about the actions that have been chosen by the previous players. The attacker's (resp. SO's) objective in the last two stages of the game is to maximize (resp. minimize) the post-contingency cost (sum of attacker-induced network costs and forced /load shedding).

As mentioned in Figure 4-5, the SO's objective in Stage 0 is to determine the resource allocation (i.e., output of the generators sg^n) that minimizes the total cost of resource allocation (C_{alloc}) and the maximin post-contingency loss incurred in the last two stages of the game.

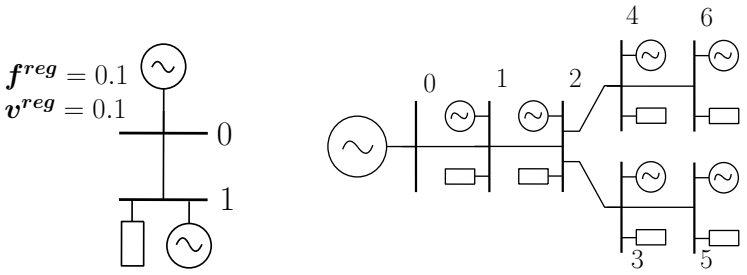
The RAOPF problem (4.13) belongs to a class of mixed-integer non-convex trilevel problems which are typically computationally hard to solve. However, after the MILP reformulation of the last two stages ([Maxmin]), the overall RAOPF can be shown to be a Mixed-Integer Bilevel Non-Linear Program (MIBNLP). Although MIBNLP are NP-hard problems, few computational approaches have been proposed in the literature for solving of MIBNLP problems based on branch and bound techniques [145]. We do not focus on implementing these techniques here, but instead focus on simple examples which

provide us interesting and practically relevant insights on the SO's allocation/dispatch and attacker's strategy.

By way of simple examples, we first illustrate the key tradeoffs faced by the SO in maintaining regulation objectives (Sec. 4.3.1). Next, we describe the structure of optimal attack in two cases: with and without adequate resources (Sec. 4.3.2). Finally, we present some insights about resource allocation strategies (Sec. 4.3.3), and compare two qualitatively different resource allocation strategies (Sec. 4.3.4).

4.3.1 Insights on optimal SO response

The fact that the regulation objectives VR, FR, and CM are not aligned with each other can be seen by considering a simple 2 node network in Figure 4-6. It has a BG with $\boldsymbol{f}^{\boldsymbol{reg}} = 0.1$ and $\boldsymbol{V}^{\boldsymbol{reg}} = 0.1$. Node 1 has a load with $pc_1^n = 0.4$ pu and $qc_1^n = 0.2$ pu. Node 1 also has a DER which can be modeled according to the in Figure 4-7a with apparent power capability of $\overline{\mathbf{sg}} = 0.4$ pu. The pre-contingency output of the DER is set to $pg_1^n = 0.2$ pu, $qg_1^n = 0.2$ pu. The line parameters are $\mathbf{r}_1 = 0.2$ pu and $\mathbf{x}_1 = 0.4$ pu.

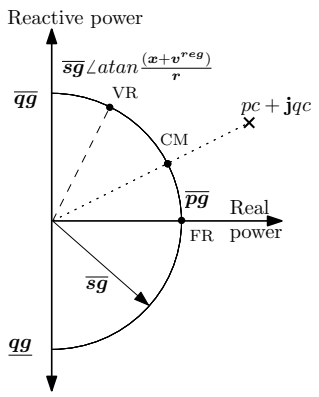


(a) 2 node network. (b) 6 node network.

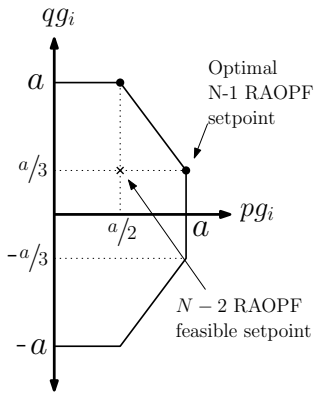
Figure 4-6: DN topologies

Now, consider the contingency created by a sudden change of load to twice its pre-contingency value, i.e. $pc_1^c + \mathbf{j}qc_1^c = 0.8 + 0.4\mathbf{j}$. This trade-off in maintaining the regulation objectives (FR, VR, and CM) is apparent from the difference in optimal DER outputs needed to address each of these objectives individually. Indeed, the DERs alone may not be able to completely resolve the contingency; under our assumptions, the remaining supply-demand imbalance is eventually covered by the BG.

Let $\Delta p := (pc_1^c - pg_1^c) - (pc_1^n - pg_1^n)$ be the net change in active power consumed



(a) SO response for each of the three regulation objectives in 2 node example network.



(b) Resource allocation strategies considered for the 6 node network.

Figure 4-7: Trade-offs in in maintaining regulation objectives and DER setpoints for reserve allocation.

at node 1. Similarly, let $\Delta q := (qc_1^c - qg_1^c) - (qc_1^n - qg_1^n)$ be the net change in reactive power consumed at node 1. Now, consider the following cases which correspond to the SO addressing each regulation objective individually (again, see Figure 4-7a for the corresponding DER setpoints):

- Using (4.2a), the drop in system frequency can be approximated as $\boldsymbol{f^{reg}}\Delta p$. Thus, to achieve maximum FR, the SO should minimize $\boldsymbol{f^{reg}}\Delta p$.

- Using (4.1) and (4.2b), the voltage drop at node 1 can be approximated as $\mathbf{r}\Delta p + (\mathbf{x} + \boldsymbol{V^{reg}})\Delta q$. Thus, to best maintain VR, the SO should minimize this quantity.

- Finally, the power flow on line (0,1) can be expressed as $(pc_1^c - pg_1^c) + \mathbf{j}\,(qc_1^c - qg_1^c)$. Thus, for CM, the SO should minimize $\mathbf{r}\,((pc_1^c - pg_1^c)^2 + (qc_1^c - qg_1^c)^2)$.

The optimal DER setpoint for each of the abovementioned cases can be expressed in closed form and are given below (these setpoints are illustrated in Figure 4-7a):

$$pg_1^{c\star} + \mathbf{j}qg_1^{c\star} = \begin{cases} \overline{\mathbf{sg}}\angle \arctan 0 & \text{for maximum FR} \\ \overline{\mathbf{sg}}\angle \arctan\left(\frac{(\mathbf{x}+\boldsymbol{V^{reg}})}{\mathbf{r}}\right) & \text{for maximum VR} \\ \overline{\mathbf{sg}}\angle \arctan\left(\frac{qc_1^c}{pc_1^c}\right) & \text{for maximum CM} \end{cases}$$

Clearly, the optimal response DER setpoints for FR, VR and CM are distinct. Thus, the optimal DER setpoints depends on weight of each regulation objective in the post-contingency cost; see (4.12). For the chosen parameters in the 2-node network, the DER setpoints and their corresponding impact on regulation objectives are summarized in Table 4.1.

Network objectives	Post-contingency $\mathbf{x}_1$ qg_1/pg_1	Objective Values Δf	ΔV_1	$\mathbf{r}_1 (P_1^2 + Q_1^2)$
FR	0	0.01	0.22	0.05
VR	$(\mathbf{x} + \boldsymbol{V}^{\boldsymbol{reg}})/\mathbf{r}$	0.041	0.051	0.076
CM	qc^c/pc^c	0.015	0.119	0.031

Table 4.1: Trade-offs between FR, VR and CM.

4.3.2 Insights on optimal attacker strategy

Now let us study the structure of optimal attack under no DER response by considering a 6 node example network as shown in Figure 4-6b. We will define the load and DER parameters in terms of a constant scalar $a = 0.1$ pu. Let $b = a/3$. Assume that each line has identical impedance $\mathbf{z} = \mathbf{r} + \mathbf{j}\mathbf{x}$, where $\mathbf{r} = 0.03$ pu and $\mathbf{x} = 0.06$ pu. At each node $i \in \mathcal{N}$, we assume the non-EV load $sn_i^n = a + \mathbf{j}b$. Consider the EV load $se_i^n = a + \mathbf{j}b$ for $i \in \{3, 4, 5, 6\}$, and the EV load as $se_i^n = 1.4(a+\mathbf{j}b)$ for $i \in \{1, 2\}$. We assume that if the EVs are compromised, then their load becomes twice of that of their pre-contingency demand, i.e., $\overline{\mathbf{se}}_i = 2\underline{\mathbf{se}}_i$. Let's consider the pre-contingency DER setpoints to be $sg_i^n = a + \mathbf{j}b$. The frequency regulation constant $\boldsymbol{f}^{\boldsymbol{reg}}$ is 1 Hz/pu, i.e. the frequency drops by 1 Hz if the supply-demand deficit suddenly increases by 1 pu, and the voltage regulation constant $\boldsymbol{V}^{\boldsymbol{reg}}$ is 0 pu. The frequency bounds are $\underline{\mathbf{f}} = 59.8, \overline{\mathbf{f}} = 60.2$ Hz. The voltage bounds are $\underline{\mathbf{V}}_i = 0.9, \overline{\mathbf{V}}_i = 1.1$.

Recursively using the voltage-drop equation (4.1c), we can compute the voltage profile as follows:

$$\forall\, i \in \mathcal{N}, \eta \in \{o, c\}, \quad V_i^\eta = V_0^\eta \mathbf{1}_N - \sum_{j \in \mathcal{N}} \boldsymbol{R}_{\boldsymbol{ij}}(pc_j^\eta - pg_j^\eta) - \boldsymbol{X}_{\boldsymbol{ij}}(qc_j^\eta - qg_j^\eta). \tag{4.14}$$

Using (4.14), we can compute the pre-contingency voltage profile:

$$V^n = \begin{bmatrix} 0.965 & 0.938 & 0.928 & 0.928 & 0.923 & 0.923 \end{bmatrix}.$$

We can check that this 6-node DN satisfies regulation objectives under any single EV node attack. For example, when the EV at node 1 or 2 is compromised, the net active power demand increases by $1.5a$ pu. Hence, the frequency only drops to 59.85 Hz, which is above frequency lower bound. Similarly, if node 5 or node 6 is compromised then the minimum voltage in the DN is 0.907, which is above the voltage lower bound. In case of compromise of an EV at an intermediate node 3 or 4, we can similarly ensure that the regulation objectives are fulfilled, as these nodes are smaller in size than nodes 1 or 2, and are located upstream to the nodes 5 and 6. Consequently, the impact of EV compromise at node 3 or 4 will be smaller than nodes 1 or 2 (resp. nodes 5 or 6) in terms of frequency (resp. voltage) drop. Thus, in the terminology of classical SCOPF problem, this network is resilient to the N-1 contingencies, each concerning the compromise of a single EV node.

Now, we consider the case when the attacker compromises $\mathrm{k} = 2$ EV nodes. Let's consider three different subcases.

(a) $\mathbf{W}_{\mathrm{VR}} = 0, \mathbf{W}_{\mathrm{FR}} > 0$**:** In this case, the attacker's goal is to maximize C_{FR}. Then, by Claim 1, the attacker's optimal strategy will be to compromise EVs at nodes 1 and 2 because nodes 1 and 2 have the largest EVs. In this case, the location of EVs in the DN does not matter from the attacker's perspective.

(b) $\mathbf{W}_{\mathrm{VR}} > 0, \mathbf{W}_{\mathrm{FR}} = 0$**:** Now, the attacker's goal is to maximize C_{VR}. Following Claim 2, the attacker's optimal strategy is to compromise EVs at nodes 4 and 6. Since, the net demand at each node is positive, power only flows from the substation to the downstream nodes. As a result, node 6 has the lowest voltage in the DN. Voltages at all nodes will reduce if EVs are compromised, but the voltage at node 6 will reduce the most if nodes 4 and 6 are compromised (by Claims 2 and 3). Therefore, we observe that the attacker chooses to compromise downstream EVs. Note that due to symmetric nature of the DN, compromising EVs at nodes 3 and 5 is also an optimal attack strategy for this case.

(c) $\mathbf{W}_{\mathrm{VR}} > 0, \mathbf{W}_{\mathrm{FR}} > 0$**:** In this case, the attacker's goal is to maximize weighted sum

of C_{FR} and C_{VR}. We observe that for a certain range of values for $\frac{\mathrm{W_{VR}}}{\mathrm{W_{FR}}}$ ratio, the optimal attack strategy is to compromise nodes 2 and 6. The attacker compromises an upstream node 2 instead of a downstream node 4 to increase the loss of FR even though the loss in VR may reduce. Additionally, we see that although nodes 1 and 2 have identical EVs, attacker will choose to compromise node 2 because of his preference for downstream EV nodes maximizes loss of VR.

Thus, we observe that when the $\frac{\mathrm{W_{VR}}}{\mathrm{W_{FR}}}$ ratio is small, the attacker chooses to compromise large EV nodes which may or may not be spatially co-located. However, as the $\frac{\mathrm{W_{VR}}}{\mathrm{W_{FR}}}$ ratio increases the optimal attack starts to target downstream nodes in a clustered manner.

4.3.3 Insights on resource allocation

Next, among the optimal attacker strategies determined in Sec. 4.3.2, we consider the following attack scenarios each involving simultaneous compromise of k $= 2$ EV nodes: (a) nodes 1 and 2 are compromised (i.e. $\delta = [1, 1, 0, 0, 0, 0]$), (b) nodes 4 and 6 are compromised ($\delta = [0, 0, 0, 1, 0, 1]$). For each of these two scenarios, we evaluate the costs due to loss in VR and FR components of the total post-contingency cost when DER reserves are not present, and compare these costs with the case when DER reserves are available.

(i) Network with no DER resources

Assume that all the DERs are operating at $sg_i^n = a + b$**j**pu. At this initial setpoint, there is no available active or reactive power reserve from the DERs.

Attack scenario (a):

The net increase in active power load is $3a = 0.3$ pu. This change results in $f^c = 59.7$ Hz. Hence, some amount of load shedding will be required to bring the frequency back to the acceptable range.

Attack scenario (b):

Under this attack, if the SO does not respond, then the post-contingency voltages will be:

$$V^c = \begin{bmatrix} 0.952 & 0.912 & 0.902 & 0.898 & 0.898 & 0.888 \end{bmatrix}.$$

Clearly, the voltage bounds will be violated at nodes 4 and 6, and some load shedding is required to bring voltages back to acceptable range. Note that, the voltages at nodes 4 and 6 are smaller than the voltages at nodes 3 and 5. This is due to the proximity of load compromises to nodes 4 and 6.

(ii) Network with DER reserves

Now assume that the pre-contingency DER setpoints are $sg_i^n = 0.5a + b\mathbf{j}$ pu. This gives us active and reactive power reserves of $0.5a + 2b\mathbf{j}$; see Figure 4-7b. Note that this is an overestimate of actually available reserves, because if active power reserves are fully used, then reactive power reserves cannot be used at all and vice versa. We chose this DER setpoint only for the ease of calculation; it is certainly not an optimal reserve allocation in the face of 2-sized EV attacks. Under this resource allocation, the pre-contingency voltage profile will be:

$$V^n = \begin{bmatrix} 0.956 & 0.921 & 0.908 & 0.908 & 0.902 & 0.902 \end{bmatrix},$$

which also satisfies the voltage bounds.

Attack scenario (a):

Again, the total load suddenly increases as a result of EV attacks to nodes 1 and 2. Now, each DER can rapidly respond to the contingency, and if the SO increases their generation from the initial setpoint $sg_i^n = 0.5a + b\mathbf{j}$ to final setpoint $sg_i^c = a + bj$, then the additional active power injected from the DERs is $6(a - a/2) = 3a$ pu. Hence, the net change in active power between pre- and post-contingency situation is 0. As a result, there is no change in frequency despite two EVs being compromised. Although there is a drop in voltage because of a net increase in reactive power demand, the voltage bounds are also satisfied. Hence, load shedding is not required.

Attack scenario (b):

Due to the compromise of downstream EV nodes, the minimum voltage in DN will violate the bounds in the absence of a DER response. Fortunately, this situation can be avoided if the reactive power supply is increased and the setpoints of all DERs are changed to

$0.5a + a\mathbf{j}$. The resulting post-contingency voltage profile will be as follows:

$$V^c = \begin{bmatrix} 0.97 & 0.945 & 0.94 & 0.93 & 0.938 & 0.922 \end{bmatrix}.$$

Thus, all voltage bounds are met with this DER reserve.

Using this illustrative example, we have tried to argue that with sufficient reserves as well as appropriate SO response, the DN can withstand contingencies resulting from compromise of mutiple (k $= 2$) EV nodes. In this example, we see that both frequency and voltage regulation objectives can be maintained without any load control because the DER reserves were sufficient to provide the active and reactive power supply needed to avoid the frequency and voltage bound violations.

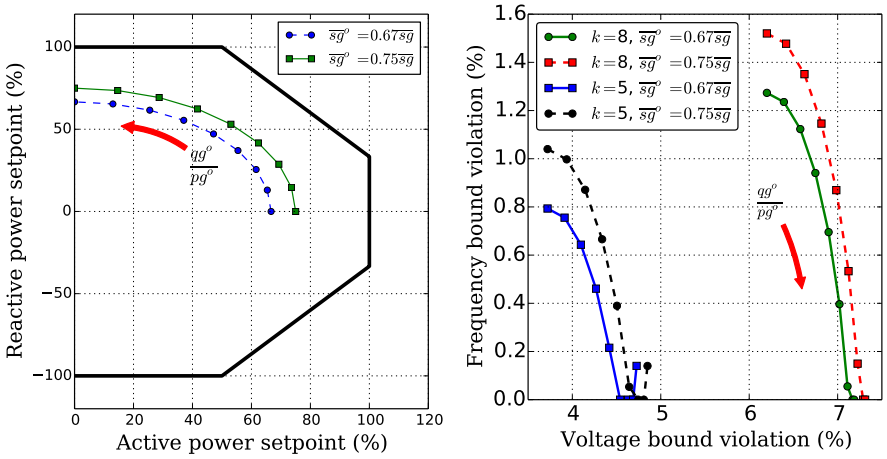
4.3.4 Further insights on resource allocation stage (Stage 0)

Finally, we study two possible SO strategies for optimal resource allocation in Stage 0. We retain the same network setup as in Sec. 4.2. First, we focus on "uniform" resource allocation, i.e., all DERs have identical pre-contingency setpoints. For this resource allocation, we use the greedy heuristic to compute optimal attacker strategy and the SO response. Secondly, based on our observations regarding the SO response, we suggest a feasible "heterogeneous" resource allocation, i.e. DERs having different pre-contingency setpoints, while keeping the total DER output identical to that of the former case. Finally, we compare the worst-case post-contingency losses for the two resource allocation strategies.

Trade-off between active and reactive power allocation. First, we show that there exists a trade-off between active and reactive power resource allocation to meet the objectives of FR and VR. We assume no load control, i.e. $\overline{\beta} = 0$, and vary the initial DER resource allocation as shown in Figure 4-8a. Two different values of $\overline{\mathbf{sg}}^o$ are chosen, and the resource allocation is varied in the increasing order of $\frac{qg_i^n}{pg_i^n}$ (see Figure 4-8a). For each combination of $\overline{\mathbf{sg}}^o$ and $\frac{qg_i^n}{pg_i^n}$ ratio, the optimum maximin post-contingency losses are computed for two attack intensities; see Figure 4-8b.

We can draw some useful observations from this figure: as the intensity of the attack

k (i.e., number of compromised EV nodes) increases or the apparent reserves allocated decrease (i.e., $\overline{\text{sg}}^o$ increases), the post-contingency voltage bound violation increases. Note that for both $\text{k} = 5$ and $\text{k} = 8$, as $\frac{qg_i^n}{pg_i^n}$ ratio increases, the voltage bound violation increases since the reactive power reserves are reduced. The frequency bound violation decreases initially for higher allocation of active power reserves. Interestingly enough, for $\text{k} = 5$, and for large enough $\frac{qg_i^n}{pg_i^n}$ ratio, we can see the frequency bound violation increases again. This can be explained as follows: For large enough $\frac{qg_i^n}{pg_i^n}$ ratio, the reactive power reserve reduces. Hence, to do VR, the SO increases both active and reactive power output of the DERs. However, since the attack intensity is small, the net change in active power after the attack becomes positive and large enough to cause violation of upper frequency bound.



(a) DER resource allocation.

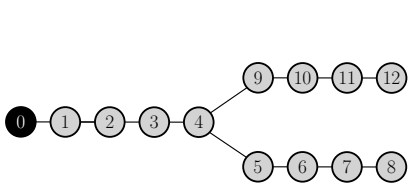
(b) Trade-off between frequency and voltage bound violations.

Figure 4-8: Post-contingency losses for different weights of regulation objectives.

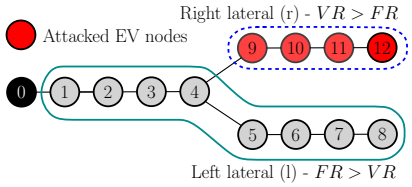
4.4 Optimal operator response and allocation

Diversification in SO response. Secondly, we show the optimal SO response admits a diversification strategy, where some DERs supply more active power than reactive power (i.e. their contribution to FR is more than that to VR), while other DERs supply more reactive power than active power (i.e. their contribution to VR is more than that to FR).

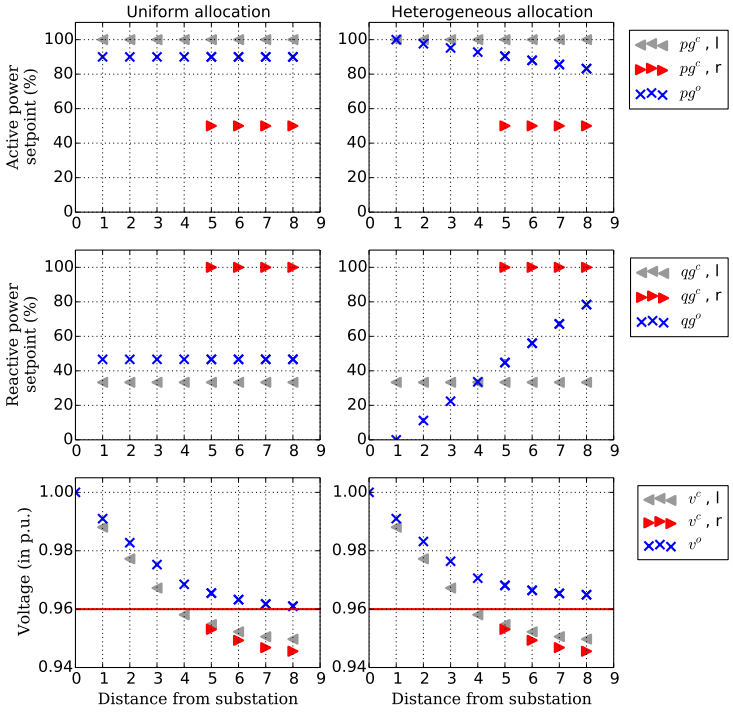
Consider the 13 node network as shown in Figure 4-9a. For $\text{k} = 4$, the optimal attacker



(a) 13 node network.



(b) Diversification of SO response.



(c) Uniform vs. heterogeneous resource allocation.

Figure 4-9: Diversification of nodes for voltage vs. frequency regulation.

strategy is to compromise EV nodes $\{5, 6, 7, 8\}$ or $\{9, 10, 11, 12\}$. Due to symmetricity, assume that the latter EV node set is compromised. These 4 nodes form the right lateral, denoted by (r), and the remaining nodes form the left lateral, denoted by (l). Consider uniform resource allocation, as shown in Figure 4-9c. The pre-contingency output of the DERs is 90% and 47% of the maximum active and the maximum reactive power output, i.e., $sg_i^n = 0.9\overline{\mathbf{pg}}_i + 0.47\overline{\mathbf{qg}}_i$. Before the attack, the voltages of the nodes in the left lateral are equal to the corresponding nodes in the right lateral. After the attack, the voltages in the right lateral fall below that of the left lateral. Hence, the DERs in the right lateral start contributing to VR, by generating $sg_i^c = (0.5 + \mathbf{j})\overline{\mathbf{sg}}_i$. However, rest of the DERs contribute more to the FR by generating $sg_i^c = (1 + 0.33\mathbf{j})\overline{\mathbf{sg}}_i$. This shows that the DERs diversify in their roles to contribute to different objectives.

Diversification in DER resource allocation. Finally, we evaluate the pre-contingency state vector and post-contingency cost for a heterogeneous resource allocation strategy and compare with the uniform allocation strategy. Recall from our experiment above that the downstream DERs are likely to contribute more to VR than to FR. Therefore, we may choose the initial DER setpoints as shown in Figure 4-9c, such that downstream DERs contribute more reactive power as compared to upstream DERs. Now, consider the following heterogeneous allocation strategy: as the distance of the node from the substation increases, let us choose a higher reactive power setpoint, and lower active power setpoint. Note that, we keep the sum total of active and reactive power output of the DERs to be the same as in the case of uniform allocation. Interestingly, we observe that the post-contingency losses are identical for both uniform and heterogeneous resource allocation. However, the pre-contingency voltage profile is better for the heterogeneous resource allocation as opposed to uniform resource allocation. We expect that a better voltage profile will allow the SO to incur lesser costs regulation cost in the pre-contingency state.

Chapter 5

Leveraging Substation Automation Systems for Network Resilience

In Chapters 3 and 4, we evaluated the impact of DN-side disruptions on the extent of loss of voltage and frequency regulation. Consequently, the operator response problem consisted only of continuous variables. However, the components at DN nodes cannot continue to operate for too long if the voltage and frequency bound violations are not quickly addressed. In this chapter, we extend our operator response models to allow for component disconnections. This can be achieved by either autonomous disconnects due to activation of local protection mechanisms or by a centralized response by the operator.

5.1 Value of timely disconnects

Despite the recent trends in modernization of electricity Distribution Networks (DNs), many Distribution System Operators (DSOs) continue to face both strategic and operational challenges in ensuring a reliable and secure service to their customers. On one hand, the integration of new supply sources such as Distributed Generators (DGs) and new monitoring and control capabilities enable flexible DN operations [52, 106, 110, 130]. On the other hand, these capabilities also expose the vulnerabilities of DNs to remote adversaries [77, 97, 98, 109], which can include criminal organizations, terrorist groups, and even nation states.

Security threats to DNs can escalate in the presence of intermittent disturbances in

the Transmission Network (TN), or during conditions when the power system is close to an emergency state [24, 103, 121]. It is well-recognized that significant cyber-physical failures in TN/DN – individually or in combination – can result in a sudden disruption, potentially leading to contingencies such as violations in the operating bounds of system states and/or loss in the functionality of network components. This paper is motivated by the DSOs' need for responding to such contingencies in a timely manner to prevent (or at least delay) the automatic protection mechanisms from triggering and causing extensive uncontrolled load/DG disconnects (outage). Our main hypothesis is that the operational flexibility of modern DNs can be exploited to generate a timely response to cyber-physical failures. We show that such a response can lead to significant reduction in the post-contingency losses. This capability becomes especially important for DNs facing risk of correlated failures under which the traditional protection mechanisms may no longer be adequate or not trigger at all.

More broadly, we contribute to a systematic framework for evaluating DN resilience. Generically, resilience of a system is defined as "its ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events" [93]. Indeed, previous literature has dealt with issues related to resiliency of power systems [77, 103, 121]. However, these approaches do not explicitly model the combined effects of TN- and DN-side failure scenarios on the losses faced by the DSO, and hence cannot be directly used to evaluate the effectiveness of available response strategies. In this paper and its companion paper [115], we develop a simple yet generic approach to address this gap in the literature.

We say that a DN with an operational response capability is *more resilient* to a class of cyber-physical failures if the DSO incurs a *lesser* post-contingency loss when subjected to these failures, relative to the loss under classical protection mechanisms (e.g. autonomous disconnections). Indeed, defining a relevant class of failure scenarios, DSO response, and acceptable extent of post-contingency loss are all important aspects of the problem. Also important is a computationally tractable approach to evaluate "worst-case" post-contingency loss.

We fully address these aspects in the context of a linear power flow model. We first introduce an attack model to capture DN-side failure scenarios that are relevant to cyber-

physical security of DNs [98]. We argue that the impact of such security failures may be aggravated under TN-side reliability failures. To begin with, we model the impact of TN-side failure as a voltage sag (drop in the substation voltage), and that of DN-side security failures as supply-demand disturbances at the DN nodes. A plausible attack scenario that can be studied using this model is one in which a remote control functionality (e.g. DG management system, DGMS) is compromised by an external attack [98].

To model DSO's response capability, we consider different operations supported by modern DNs: remote control by the control center, autonomous disconnects of components due to activation of local protection systems, and emergency control by the Substation Automation (SA) systems (Sec. 5.1). We pose a bilevel optimization problem for evaluating the maximum post-contingency loss when the DSO optimally responds to the attack, and present a computational approach to solve it. We formulate this problem as a Bilevel Mixed Integer Problem (BiMIP). In principle, the Benders Decomposition (BD) algorithm can be applied to solve such formulations. However, it is shown in Sec. 5.2 that in our problem, only binary variables enter in the coupling constraints. It turns out that, in such cases, a straightforward application of the BD algorithm does not generate useful Benders cuts. Our solution approach addresses this issue by formulating an equivalent min-cardinality disruption problem, and reformulating the coupling constraints to ensure that the set of attacks are progressively refined in each iteration of the BD algorithm (Sec. 5.4).

Several papers have used bilevel optimization formulations for vulnerability assessment of TNs to adversarial disruptions [24, 97, 103, 121]. A notable application is the generalization of the classical N-1 security problem to an N-k problem [24, 121]. These formulations typically assume the DC power flow approximation, which enables a KKT-based reformulation, and leads to single-level Mixed-Integer Program (MIP). In our past work, we used a similar formulation to assess the security of DNs to remotely induced DG disruptions [109, 110]. However, that formulation did not consider preemptive tripping of loads/DGs as a part of the operator's response strategy, and thus it did not require the inner problem of the bilevel program to have integer variables. A relatively simple greedy heuristic gave reasonable performance in that case. In this paper, we deal with a bilevel

program with mixed-integer variables in the inner problem.

Our main contributions include:

(⋆) An approach to evaluate the resilience of DNs based on post-contingency losses (Sec. 5.1) by modeling the physical impact on a DN due to a class of cyberphysical failures which consists of disruptions due to DN-side security failures as well as TN-side reliability failures (Sec. 5.2), and

(⋆) an extended Benders Decomposition approach for solving BiMIPs in which the coupling constraints consist only of binary variables (Sec. 5.4), and using this approach for computing post-contingency losses under different operator response capabilities (Sec. 5.3).

Broadly speaking, the response capabilities of modern DN systems can be classified as follows: (a) Remote control of nodal demand and/or supply sources by the DSO/control center; (b) autonomous disconnect operation of individual components; for example, tripping of DGs or loads under nodal violations in operating conditions; and (c) emergency control at the substation level which is executed by the Substation Automation (SA) system, and includes preemptive response actions such as load control and/or disconnection of components. Please refer to Figure 5-1 for an illustration of these control capabilities. The autonomous disconnect operation is based on local checks of operating bounds at the DN nodes. On the other hand, the operator response via the control center or the SA system utilizes the information from the meters in the DN about node-level consumption, distributed generation, and nodal voltages.

To describe our modeling approach, we focus on a specific attack model: the compromise of remote control capabilities of the control center. Hence, (a) is no longer a viable response, but (b) and (c) can be used to respond to the attack-induced disturbance. Thus, it becomes imperative to clearly distinguish these response capabilities and model the resulting network state.

In our model, the DSO response (c) is comprised of load control and preemptive tripping of components (loads and/or DGs), and can be operationalized via the SA system (refer to (c) in Figure 5-1). The SA systems were recently provided cyber-security reperime-

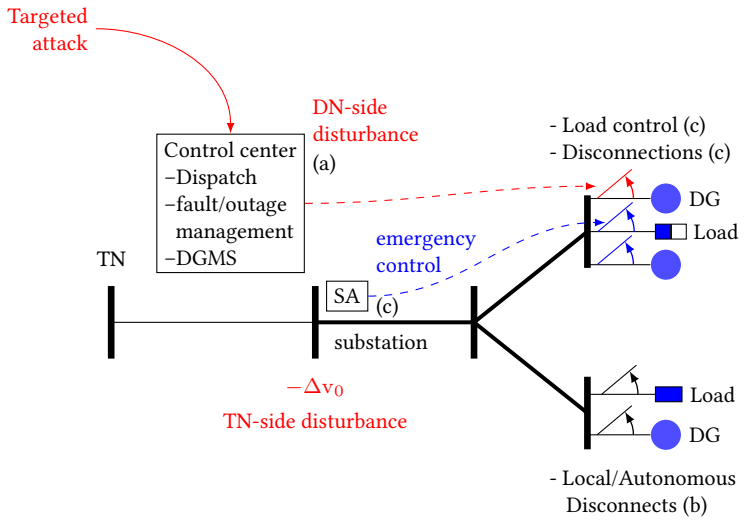


Figure 5-1: Attacker-operator interaction.

terisation by the NERC regulations [94]. In comparison, the newer control center operations such as DGMS are prone to back channel attacks by remote third parties, as evident from the recent incidents [75]. By evaluating the reduction in loss due to a timely DSO response, and comparing it with the loss under the autonomous disconnections, we can estimate the *value* of the timely response toward improving the DN's resilience.

We formulate a bilevel problem to model the sequential interaction between the strategic attacker and operator; see [24, 72, 110, 148] for similar formulations. Our problem can be stated as follows:

$$\mathcal{L}_{\text{Mm}} \coloneqq \max_{d \in \mathcal{D}_{\text{k}}} \min_{u \in \mathcal{U}(d)} L(u, \text{x}) \qquad \text{s.t.} \quad \text{x} \in \mathcal{X}(u)\,, \tag{P1}$$

where $\mathcal{L}_{\text{Mm}}$ denotes the Max-min (Mm) post-contingency loss used for evaluating DN's resilience; d an attacker-induced failure; k the attacker's resource constraint; $\mathcal{D}_{\text{k}}$ the set of attacker's strategies; u an operator response; $\mathcal{U}(d)$ the *coupling* constraints that define the set of feasible operator responses under the impact of attack-induced failures; x the post-contingency network state, i.e. the state after the attacker-operator interaction is completed; $\mathcal{X}$ the set of constraints that model physical constraints (power flows), component constraints (loads and DGs), and nodal voltage constraints (Sec. 5.1). For a given disruption $d \in \mathcal{D}_{\text{k}}$, the operator's objective is to minimize the post-contingency

loss $L(u, \mathrm{x})$, and the attacker's objective is to choose an attack that maximizes the post-contingency loss assuming an optimal response by the operator. Suppose that $(d^\star, u^\star)$ is an optimal solution to this maximin problem which results in the network state $\mathrm{x}^\star$. Then $\mathcal{L}_{\mathrm{Mm}} = L(u^\star, \mathrm{x}^\star)$ is the post-contingency loss that is incurred by the operator when he implements $u^\star$ in response to the attack $d^\star$ (Sec. 5.4).

Note that the post-contingency loss $\mathcal{L}_{\mathrm{Mm}}$ is a measure of the maximum reduction in system performance under the class of disruptions in the set $\mathcal{D}_{\mathrm{k}}$; see Figure 5-2. For the sake of normalization, we denote by $\mathcal{L}_{\max}$ the loss incurred when all loads and DGs are disconnected. Then, $\mathcal{R}_{\mathrm{Mm}} := 100\left(1 - \frac{\mathcal{L}_{\mathrm{Mm}}}{\mathcal{L}_{\max}}\right)$ can be considered as a metric of the DN resilience under operator response (in the set of responses $\mathcal{U}$).

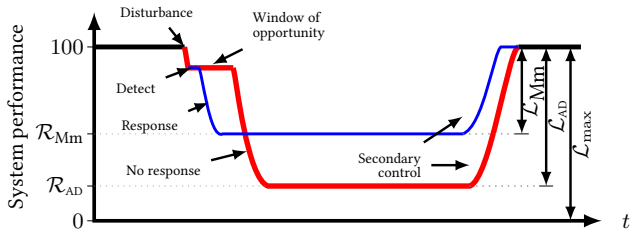


Figure 5-2: Performance under various response capabilities.

Now suppose that we want to compare the DN resilience under operator response to the case of autonomous disconnections. To do this comparison, we need to estimate the maximum loss corresponding to automatic disconnects of DN components (refer to (b) in Figure 5-1) that would be induced by a maximally disruptive attack in the set $\mathcal{D}_{\mathrm{k}}$ (due to compromise of (a) in Figure 5-1). In Sec. 5.3, we present a simple algorithm to estimate the uncontrolled cascade-like loss in load/DG connectivity due to operating voltage bound violations, and in Sec. 5.4, we present an approximate algorithm to estimate the worst-case operator loss under autonomous disconnections. Let the automatic disconnect actions be denoted by u_{nr}, resulting network state by x_{nr}, and the corresponding loss by $\mathcal{L}_{\mathrm{AD}} = L(\mathrm{x}_{\mathrm{nr}}, u_{\mathrm{nr}})$. Then, the resilience metric of the DN under autonomous disconnections can be written as $\mathcal{R}_{\mathrm{AD}} = 100(1 - \mathcal{L}_{\mathrm{AD}}/\mathcal{L}_{\max})$. Naturally, $\mathcal{R}_{\mathrm{Mm}} \geqslant \mathcal{R}_{\mathrm{AD}}$, and we can evaluate the relative value of operational response (or equivalently, the improvement in DN resilience) as $(\mathcal{R}_{\mathrm{Mm}} - \mathcal{R}_{\mathrm{AD}})$. In Sec. 5.4, we evaluate this quantity for a set of test DNs.

More generally, Figure 5-2 illustrates the evolution of system performance evolves

over time after the attacker-operator interaction. Initially, the DN is operating in nominal conditions. As a result of the TN/DN-side disturbances, the system performance degrades. If the operator fails to respond in a timely manner (in less than a few seconds), then an uncontrolled cascade can occur (resulting in a post-contingency loss $\mathcal{L}_{\text{AD}}$). However, to regain nominal operation, the operator eventually undertakes secondary control actions like changing tap settings of transformers, or switching on capacitor banks. Then, the nodal voltages recover, allowing the disconnected components to be reconnected and operate within safety bounds. In the companion paper [115], we address other aspects of DN resilience such as microgrid capabilities to further minimize the post-contingency loss, as well as reconnection of disrupted DGs to enable faster DN recovery.

Network Model

We model the DN as a tree network of node set $\mathcal{N} \bigcup \{0\}$ and line set $\mathcal{E}$; see Figure 5-3. We refer the reader to Table 5.1 for the definitions of key notations, and to references [109, 130] for further details.

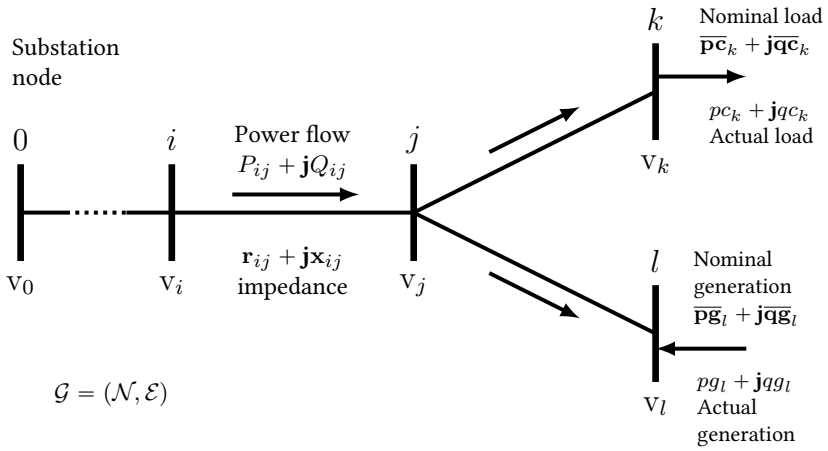


Figure 5-3: DN model.

For the sake of computational simplicity, we model the power flows using the classical

Table 5.1: Table of Notations.

DN parameters	
$\mathcal{N}$	set of nodes in DN
$\mathcal{E}$	set of edges in DN
0	substation node label
$\mathcal{G}$	radial topology of DN, $\mathcal{G} = (\mathcal{N} \bigcup \{0\}, \mathcal{E})$
$N = \lvert\mathcal{N}\rvert$	number of non-substation nodes in DN
$\mathbf{j}$	complex square root of -1, $\mathbf{j} = \sqrt{-1}$
$\mathrm{v}^{\mathbf{nom}}$	nominal squared voltage magnitude (1 pu)
v_0	squared voltage magnitude at substation node
Nodal quantities of node $i \in \mathcal{N}$	
v_i	squared voltage magnitude at node i
$\overline{\mathbf{pc}}_i + \mathbf{j}\overline{\mathbf{qc}}_i$	nominal demand at node i
$\overline{\mathbf{pg}}_i + \mathbf{j}\overline{\mathbf{qg}}_i$	nominal generation at node i
$pc_i + \mathbf{j}qc_i$	actual power consumed at node i
$pg_i + \mathbf{j}qg_i$	actual power generated at node i
$p_i + \mathbf{j}q_i$	net power consumed at node i
$\underline{\mathbf{vc}}_i, \overline{\mathbf{vc}}_i$	lower, upper voltage bounds for load at node i
$\underline{\mathbf{vg}}_i, \overline{\mathbf{vg}}_i$	lower, upper voltage bounds for DG at node i
y_i	0 if DG at node i is connected to DN; 1 otherwise
kc_i	0 if load at node i is connected to DN; 1 otherwise
β_i	fraction of demand satisfied at node i
$\underline{\beta}_i$	lower bound of load control parameter β_i
Parameters of edge $(i,j) \in \mathcal{E}$	
$P_{ij} + \mathbf{j}Q_{ij}$	power flowing from node i to node j
$\mathbf{r}_{ij}, \mathbf{x}_{ij}$	resistance and reactance of line $(i,j) \in \mathcal{E}$
Attack variables	
$d \in \{0,1\}^{\mathcal{N}}$	$d_i = 1$ if DG at node i is disrupted; 0 otherwise.
Operator response variables	
u	an operator response action

LinDistFlow model [16]:

$$P_{ij} = \sum_{k:(j,k)\in\mathcal{E}} P_{jk} + p_j \qquad \forall\,(i,j)\in\mathcal{E} \tag{5.1}$$

$$Q_{ij} = \sum_{k:(j,k)\in\mathcal{E}} Q_{jk} + q_j \qquad \forall\,(i,j)\in\mathcal{E} \tag{5.2}$$

$$\mathrm{v}_j = \mathrm{v}_i - 2\left(\mathbf{r}_{ij}P_{ij} + \mathbf{x}_{ij}Q_{ij}\right) \qquad \forall\,(i,j)\in\mathcal{E}, \tag{5.3}$$

where eqs. (5.1) to (5.2) are the power conservation equations and (5.3) is the voltage drop equation.

Without loss of generality, we assume that each node of the DN has a load and a DG. Furthermore, we consider the constant power model for both loads and DGs.[1]

DG model

We assume that each DG is connected to the DN via an inverter. Let $\overline{\mathbf{sg}}_i := \overline{\mathbf{pg}}_i + \mathbf{j}\overline{\mathbf{qg}}_i$ denote the nominal complex power supplied at node $i \in \mathcal{G}$, where $\overline{\mathbf{pg}}_i$ is the active power supplied by the DG and $\overline{\mathbf{qg}}_i$ is the reactive power supplied by its inverter. For the sake of simplicity, we refer to the DG-inverter assembly as simply DG. Now, depending on whether a DG is connected to the network or not, its actual output is related to its nominal output as follows:

$$pg_i = (1-y_i)\,\overline{\mathbf{pg}}_i, \quad qg_i = (1-y_i)\,\overline{\mathbf{qg}}_i. \tag{5.4}$$

According to the IEEE standard rules for interconnection of DGs [70], to ensure safety as well as proper functioning of the components, DGs are required to disconnect from the DN if voltage bound violations occur.[2] We model this constraint as follows:

$$y_i \geqslant \underline{\mathbf{vg}}_i - \mathrm{v}_i, \qquad y_i \geqslant \mathrm{v}_i - \overline{\mathbf{vg}}_i \qquad \forall\, i \in \mathcal{N}. \tag{5.5}$$

[1] More generally, loads can be modeled using the constant impedance (Z), constant current (I), constant power (P) or a general ZIP model, or even voltage dependent loads as the load power consumption can also change due to voltage deviations. Our network model can be extended to include more general load models.

[2] Note that the tripping of DGs may also happen for other reasons such as frequency bound violations, which we consider in the companion paper [115].

Load model

In many smart DNs, the operator can change the actual consumption of a connected load to a fraction of its nominal demand via direct load control in response to supply-demand disturbances [106]. We model this flexibility as the choice of load control parameter $\beta_i \in [\underline{\beta}_i, 1]$ when $kc_i = 0$, and $\beta_i = 0$ when $kc_i = 1$. Here $\underline{\beta}_i \in [0, 1]$ denotes the minimum fraction of the load's nominal demand that should be satisfied provided the load is connected. This load control capability can be represented as the mixed-integer linear constraints:

$$pc_i = \beta_i \overline{\mathbf{pc}}_i, \quad qc_i = \beta_i \overline{\mathbf{qc}}_i \qquad \forall\, i \in \mathcal{N}, \tag{5.6}$$

where

$$(1 - kc_i)\, \underline{\beta}_i \leqslant \beta_i \leqslant (1 - kc_i) \qquad \forall\, i \in \mathcal{N}. \tag{5.7}$$

Similar to DGs, the connectivity of loads also depends on the nodal voltages which can be modeled as follows:

$$kc_i \geqslant \underline{\mathbf{vc}}_i - \mathrm{v}_i, \qquad kc_i \geqslant \mathrm{v}_i - \overline{\mathbf{vc}}_i \qquad \forall\, i \in \mathcal{N}. \tag{5.8}$$

Then, the net actual consumption at nodes is given by:

$$p_i = pc_i - pg_i, \qquad q_i = qc_i - qg_i \qquad \forall\, i \in \mathcal{N}. \tag{5.9}$$

We define the network state $\mathrm{x} \in \mathbb{R}^{5N}$ as $\mathrm{x} := (p, q, P, Q, \mathrm{v})$, where p, q, P, Q, v are vectors of appropriate dimensions.

5.2 Disruption model

We now discuss a generic cyber-physical failure model that captures the effects of DN-side component disruptions caused by security failures as well as effects of disturbances from the TN.

Our attack model is motivated by the security failure scenarios discussed in [98]. These

scenarios capture the capabilities of the following threat actors: (i) cyber-hackers of an enemy nation motivated to disrupt supply to critical facilities, (ii) a malicious adversary looking to extort ransom money from the utility, or (iii) a disgruntled internal employee motivated by revenge. In this paper, we are concerned with type (i) actors. Such actors can leverage existing vulnerabilities in DN cyber architecture such as non-confidentiality of control commands, lack of multi-factor authentication, and incorrect firewall rules that allow unauthorized access. Particularly, a threat actor can exploit these vulnerabilities to launch replay attacks [150], or a server-side attack at the control center, or hack operator credentials, any of which could allow him to perform malicious activities such as mass remote disconnect of components. We model the DN-side disruptions as nodal supply-demand disturbances. For example, mass disconnects of DGs (resp. loads) can cause loss of supply (resp. demand). Additionally, a threat actor could program his attack to be launched simultaneously with a TN-side disruption. A high-level framework for modeling impact of cyber-physical disruptions to DN is illustrated in Figure 5-4.

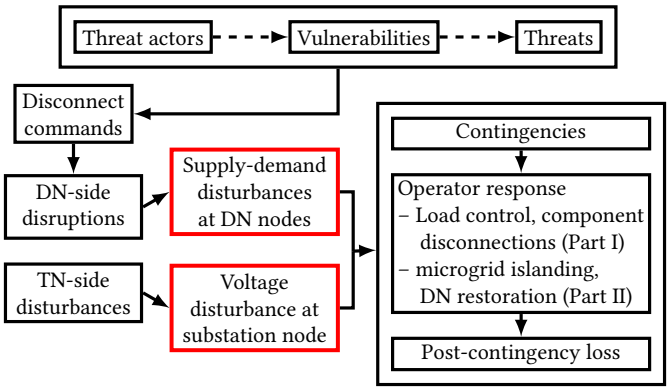


Figure 5-4: Framework for modeling impact of cyber-physical failures on DNs.

DN-side disruption

Our attack model is relevant in the context of smart DNs, with a hierarchical control architecture as illustrated in Figure 5-1; for further details we refer the reader to [147]. In this architecture, the main controller resides in the DN control center and performs the traditional tasks such as the optimization of DN operations and VoltVAR control during nominal operations. Besides, it also provides flexibility to implement new functionalities such as DGMS. An attack on the DN control center server can affect one or more of these

functionalities. For the sake of concreteness, we limit our attention to a specific attack scenario in which the attacker targets the DGMS server, with the aim to simultaneously disrupt multiple DGs connected to the DN. However, our modeling approach is general in that it can also accommodate other important attack scenarios such as mass remote disconnects of loads or invalid load control commands [98].[3]

Let $d \in \{0,1\}^{\mathcal{N}}$ be a vector denoting the disrupted nodes, where $d_i = 1$ if node i is disrupted, otherwise $d_i = 0$. Let k be the maximum number of nodes that the attacker can disrupt (i.e. resource constraint), and let $\mathcal{D}_{\mathrm{k}} := \{d \in \{0,1\}^{\mathcal{N}} \mid \sum_{i \in \mathcal{N}} d_i \leqslant \mathrm{k}\}$ denote the set of feasible attacker strategies. This constraint limits the attacker's ability to disrupt an arbitrary number of nodes, and a particular choice of k needs adequate justification. For the purpose of evaluating a DN's resilience to security attacks, one can consider that the existing fail-safe mechanisms employed by the operator (including the in-built "hard" security checks within the DGMS software) do not permit simultaneous disruption of DG nodes beyond a certain limit. This limit can be taken as the choice of k.

It is also reasonable to assume that by compromising the DGMS, the attacker can access information needed to strategically choose the disruption vector d. This includes DN topology, line resistances and reactances, nominal nodal demands and DG outputs, and the value of substation voltage deviation due to TN-side disturbance. Note that this data is already collected by the DGMS to control DG output (e.g. for Volt-VAr regulation).

Furthermore, our attack model considers that the control center functionalities such as DGMS are more viable targets for remote external attackers than local substation automation (SA) systems. Indeed, recent incidents [75] have confirmed that control center/DGMS servers can be targets of sophisticated phishing attacks (e.g. through a download of infected email attachments by the human operators who manage these servers). In contrast, a growing number of distribution utilities are regulated under NERC CIP standards which secure the substations against remote attacks via reperimetrisation of the substation cyber architecture [57, 94]. In addition, SA is typically not prone to insecure actions by human insiders.

[3] An attack on a DN control center can also be used to open circuit breakers. We consider this attack in the companion paper [115].

Now we model the impact of an attacker's actions on the DN state. If the attacker disrupts a DG at node i, then that DG becomes non-operational, and is *effectively disconnected* from the DN, i.e

$$y_i \geqslant d_i \quad \forall \quad i \in \mathcal{N}. \tag{5.10}$$

The disconnections of DGs and their inverters lead to a sudden drop in active as well as reactive power supply. Under heavy loading (high demand) conditions, reactive power often cannot be supplied from the bulk supply sources through the transmission lines. The reactive power shortfall may be exacerbated by a voltage dip resulting from a TN-side disturbance, as discussed below. This may result in sustained low-voltage conditions, e.g. a fault-induced delayed voltage recovery (FIDVR) event [17, 95] and/or result in voltage collapse.

TN-side disturbance

Our model of TN-side disturbances is motivated by situations such as failure of a transmission line or a bulk generator, which result in low voltage conditions that last for a prolonged period (several minutes). We model its impact as a sudden drop in the substation node's voltage by $\Delta \mathrm{v}_0$, which we assume to be exogenously given (and fixed). Thus, the substation voltage in the presence of a TN-side disturbance can be written as follows:

$$\mathrm{v}_0 = \mathrm{v}^{\mathbf{nom}} - \Delta \mathrm{v}_0. \tag{5.11}$$

Indeed, $\Delta \mathrm{v}_0 = 0$ indicates no TN-side disturbance.

Note that a TN-side disturbance can also result in a change in frequency away from the nominal operating frequency of the network. We extend our model to include frequency disturbances in [115]. Finally, we emphasize that the impact of attack-induced disruptions on a DN can be quite severe when the DN is simultaneously facing such a TN-side disturbance. For instance, the attacker can program the DN-side attack to be launched when a substation voltage drops at least by $\Delta \mathrm{v}_0$.

5.3 Substation Automation system capabilities

Recall from Sec. 5.1 that two operator response capabilities that we consider are the autonomous disconnect operations and emergency control by substation automation. Now, we describe these response capabilities in detail.

Autonomous Component Disconnections

The autonomous disconnect operation is based on local checks of operating bounds at the DN nodes. This is typically the case for legacy DN management systems where the operator does not have access to node-level data. Consequently, an operator relying solely on this response capability does not have the ability to timely detect, accurately identify, and promptly respond to coordinated supply-demand disturbances in the DN induced by the attack in our model.

To model the network state under response (b), we adopt and refine the *cascade algorithm* used in [23]. This algorithm is well-suited for modeling forced tripping of network components under operating bound violations. Specifically, Algorithm 8 takes the initial network state at the start of an attack-induced contingency (denoted x_{nr}), and generates automatic disconnect actions for one or more components, as the state evolves over multiple rounds of an uncontrolled cascade. Let the vector of variables representing the automatic disconnect actions be denoted by $u_{\mathrm{nr}} = (\beta^{\mathrm{nr}}, kc^{\mathrm{nr}}, y^{\mathrm{nr}})$. In each round of the cascade, u_{nr} is updated based on disconnect actions of the DGs that violate the voltage bounds in that round. These actions are determined by checking (5.5). Then, new power flows are computed after each round of disconnection by recomputing x_{nr}. Next, the set of all loads which violate the voltage bounds in (7.25) is computed, and all the loads in this set are disconnected. Note that the load control parameter $\beta_i^{\mathrm{nr}} = 1$ throughout the cascading disconnects of DGs, unless the load becomes fully disconnected, in which case it switches to $\beta_i^{\mathrm{nr}} = 0$. Since at least one DG disconnect happens in each round, the algorithm terminates in at most N+1 rounds, where the last round corresponds to load disconnects. The final connectivity vector u_{nr} corresponds to a situation where all the connected components satisfy voltage bounds, and can be used to compute the post-contingency state and

the corresponding loss.

Algorithm 8 Uncontrolled cascade under response (b)

Input: attacker action d (initial contingency)

$u_{\text{nr}}, \mathrm{x}_{\text{nr}} \leftarrow$ GetCascadeFinalState(d)
function GetCascadeFinalState(d)
  Initialize $u_{\text{nr}} = (\beta^{\text{nr}}, kc^{\text{nr}}, y^{\text{nr}}) = (\mathbf{1}_N, \mathbf{0}, d)$
  Compute state x_{nr} using eqs. (5.1) to (5.4), (5.6), (7.24), and (5.9)
  while $\exists\, i$ such that (5.5) is violated **do**
    Set $y_i^{\text{nr}} = 1$, update u_{nr}
    Recompute x_{nr} using eqs. (5.1) to (5.4), (5.6), (7.24), and (5.9)
  end while
  Compute $\mathcal{I} = \{i \in \mathcal{N} \mid \text{such that (7.25) is violated}\}$
  for each $i \in \mathcal{I}$ **do**
    Set $\beta_i^{\text{nr}} = 0, kc_i^{\text{nr}} = 1$
  end for
  Update u_{nr}, recompute x_{nr}
  return $u_{\text{nr}}, \mathrm{x}_{\text{nr}}$
end function

Now we explain the reason as to why, in Algorithm 8, we consider the disconnection of DGs before the load disconnects. A sudden voltage drop can be indicative of a fault within the DN, and therefore DGs supplying power to a fault can be potentially dangerous. Therefore, according to [70], when voltage bound violations occur, the DGs are supposed to disconnect within two seconds or less, depending on the extent of voltage drop. On the other hand, the loads can continue to operate even a minute after mild or moderate voltage bound violation occurs. Indeed, we can infer this from the fact that the response time of voltage regulators along the DN feeders is typically around 15 or 30 seconds [17, 136]. However, the disconnect actions of loads happen due to activation of protection devices which operate based on local measurements, i.e. they operate independent of each other. Therefore, in the worst-case all loads experiencing voltage bound violations can disconnect together. Hence, our choice to consider the disconnects of all the loads in set $\mathcal{I}$ within one round is reasonable.

Emergency Response by System Automation

The emergency response capability (refer (c) in Figure 5-1) of modern SA systems is enabled by fine-grained data collection of node-level consumption, distributed generation,

and nodal voltages. Many of the newer installations of smart meters are already equipped with data logging and communication capabilities. As a side note, the temporal frequency of data collected by low-voltage residential meters can vary from 15 minute to 24 hour intervals, depending on the desired control functionalities, customer privacy levels provided by the operator as well as the available communication bandwidth between DN nodes and the SA. However, for the purpose of emergency response, meters installed at medium voltage to low voltage transformers at DN nodes can be utilized to provide aggregated node-level data from the customer meters in real-time (every second). With this capability, sudden changes in local DG output can also be detected by the SA, thereby enabling the operator to identify the attack vector d. This level of monitoring does not involve individual customer meter readings, and hence, does not violate privacy regulations.

Thus, the currently available capabilities of collection and processing of node-level data can be exploited by the operator to implement fast response strategies through SA. In particular, we consider that node-level data can be used to determine the required load control (β) and intentional *preemptive* disconnects (kc, y), and that this response is exercised through the SA. Let the set of allowable load control vectors be defined as $\mathcal{B} := \prod_{i\in\mathcal{N}}(\{0\}\bigcup[\underline{\beta}_i, 1])$. Then, we can denote an operator response strategy as $u = (\beta, kc, y) \in \mathcal{U}$, where $\mathcal{U} := \mathcal{B} \times \{0,1\}^{\mathcal{N}} \times \{0,1\}^{\mathcal{N}}$. Finally, we can denote the set of response strategies feasible after an attack d by $\mathcal{U}(d) := \{u \in \mathcal{U} \mid \text{such that (5.10) holds}\}$.

Traditional response to voltage regulation

Indeed, other types of classical actions implemented through control of voltage regulators and capacitors as well as network reconfiguration can also form part of the operator response. However, we chose load control and intentional disconnects due to timing requirements. The time-scale of disturbance created by the attack can be very small (few seconds), and can trigger an immediate cascade of component disconnects due to operating bound violations. Typically, voltage regulators and capacitor banks require a larger response time; in fact, frequent activation of these devices is not preferred as they are subject to mechanical wear and tear [3]. On the other hand, thanks to advancements in

SA and power electronics based control of loads/DGs, our response strategy can be implemented within a few milliseconds after the information about the timing and extent of disruption is obtained by the SA. Our modeling approach can be extended to situations where appropriate changes in the settings of voltage regulators and capacitor banks are deemed as desirable aspects of operator response; these can be incorporated as integer decision variables in the inner problem of (P1).

Post-contingency loss

Let L denote the post-contingency loss incurred by the operator. We define it as the sum of following costs: (i) cost due to loss of voltage regulation, (ii) cost of load control, and (iii) cost of load shedding:

$$\begin{aligned} L(u, \mathrm{x}) = \mathrm{W}_{\mathrm{VR}} \left\| \mathrm{v}^{\mathbf{nom}} - \mathrm{v} \right\|_{\infty} + \mathrm{W}^{\mathrm{LC}} \textstyle\sum_{i \in \mathcal{N}} \left(\mathbf{1}_N - \beta_i \right) \overline{\mathbf{pc}}_i \\ + \left(\mathrm{W}^{\mathrm{LS}} - \mathrm{W}^{\mathrm{LC}} \right) \textstyle\sum_{i \in \mathcal{N}} kc_i \overline{\mathbf{pc}}_i, \end{aligned} \tag{5.12}$$

where $\mathrm{W}^{\mathrm{LC}} \in \mathbb{R}_+$ denotes the cost of per unit load controlled, $\mathrm{W}^{\mathrm{LS}} \in \mathbb{R}_+$ and $\mathrm{W}^{\mathrm{LS}} \geqslant \mathrm{W}^{\mathrm{LC}}$ is the cost in dollars of per unit load shed, and $\mathrm{W}_{\mathrm{VR}} \in \mathbb{R}_+$ is the cost of unit absolute deviation of nodal voltage from the nominal value $\mathrm{v}^{\mathbf{nom}} = 1$ pu. The weight $\mathrm{W}^{\mathrm{LS}} - \mathrm{W}^{\mathrm{LC}}$ is chosen to enable proper counting of the cost of load control when the load is disconnected. The typical values for the parameters in (5.12) of the cost terms are listed in Table 5.2.

Weights	Typical values
W^{LC}	$\frac{1}{4}\times$ 11 cents per kilowatt hour
W_{VR}	$\frac{2}{100}\times$ 11 cents per kilowatt hour
W^{LS}	3 dollars per kilowatt hour

Table 5.2: Typical values of cost parameters.

Remark 6. We have included the cost of load shedding, but not the cost of disconnection of customer-owned DGs because the customers are likely to face more inconvenience if there is load shedding, in comparison to DG disconnections during a contingency. However, we can easily account for the cost of DG disconnections in our formulation.

We say that if no components are disconnected after the attacker-operator interaction,

the DN is in the *No-Disconnect* (ND) regime; otherwise, it's in the *Component-Disconnected* (CD) regime. In the CD regime, the operator incurs an additional cost over the ND regime in the form of compensation to the consumers whose loads are completely disconnected; see (5.12). Note that, in our model, the CD regime can result from an uncontrolled cascade under autonomous disconnections, or from emergency response by the SA system.

5.4 Bilevel mixed-binary optimization problem

Let $\mathcal{X}$ denote the set of post-contingency states x that satisfy the constraints (5.1)-(5.9). Then, we can model the attacker-operator interaction in the presence of TN-side disturbance by refining (P1) as follows:

$$\begin{aligned} \mathcal{L}_{\mathrm{Mm}} \coloneqq \quad & \max_{d \in \mathcal{D}_{\mathrm{k}}} \ \min_{u \in \mathcal{U}(d)} \ L\left(u, \mathrm{x}\right) \\ & \text{s.t. } \mathrm{x} \in \mathcal{X}(u)\,, (5.11). \end{aligned} \tag{Mm}$$

Thus, the attacker's (resp. operator's) objective is to maximize (resp. minimize) the loss L subject to LinDistFlow (5.1)-(5.3), DG and load models (5.4)-(5.9), and the failure impact captured by $u \in \mathcal{U}(d)$ and (5.11). We refer the problem (Mm) as the *Budget-k-max-loss* problem, where k is the budget of the attacker and determines $\mathcal{D}_{\mathrm{k}}$.

In the case of autonomous disconnections, for a given attacker action d, Algorithm 8 allows us to compute the final state of operator variables u_{nr} and network state x_{nr}. We can then evaluate the post-contingency loss $L\left(u_{\mathrm{nr}}, \mathrm{x}_{\mathrm{nr}}\right)$ for an attack-induced DG disruption vector $d \in \mathcal{D}_{\mathrm{k}}$ in the autonomous disconnections case by using (5.12). For any given attack cardinality k, we denote the maximum over no-response post-contingency losses of all attacks by $\mathcal{L}_{\text{AD}}$. The optimal attack vector can be computed by simple enumeration over attacks of cardinality k. However, we will present an algorithm in Sec. 5.4 to estimate $\mathcal{L}_{\text{AD}}$.

Solution Approach

To evaluate the post-contingency loss in the case of emergency response by the SA, we need to solve the bilevel problem (Mm), which has binary variables in both inner and

outer problems. In general, such BiMIP problems are NP-hard and are computationally challenging to solve [23, 72]. Our solution approach relies on using the Benders Decomposition (BD) algorithm to approximately solve (Mm) on a reformulated problem. The overall approach can be described as follows. First, we argue that $\mathcal{L}_{\text{Mm}}$ can be obtained by solving an equivalent *Min-cardinality disruption* problem instead. Then, we apply the BD algorithm, which decomposes the min-cardinality problem into a master (attacker) problem (an integer program) and an operator subproblem (a mixed-integer program), and then solves these two problems in an iterative manner, until either an optimal min-cardinality attack is obtained or all the attacks are exhausted.

Min-cardinality disruption problem

Recall that in problem (Mm), the attacker's goal is to determine an optimal attack of size at most k (attack resource). On the other hand, in the min-cardinality problem, the attacker computes a disruption with as few attacked DN nodes as possible to induce a loss to the operator greater than a pre-specified threshold target post-contingency loss, denoted $\mathcal{L}_{\text{target}}$. These two problems are equivalent to each other in the following sense. The loss $\mathcal{L}_{\text{Mm}}$ in (Mm) is non-decreasing in k (due to the inequality constraint $\sum_{i\in\mathcal{N}} d_i \leqslant$ k). Therefore, if the parameter $\mathcal{L}_{\text{target}}$ is gradually increased then the minimum attack cardinality computed by min-cardinality problem will be non-decreasing in $\mathcal{L}_{\text{target}}$. Thus, for a fixed budget k, the smallest $\mathcal{L}_{\text{target}}$ value at which the minimum attack cardinality changes from k to k $+ 1$ will be the optimal value of problem (Mm). By implementing a binary search on the parameter $\frac{100\mathcal{L}_{\text{target}}}{\mathcal{L}_{\max}}$ between $0-100\%$, we can determine the smallest $\mathcal{L}_{\text{target}}$ at which the minimum attack cardinality changes from k to k $+ 1$. Conversely, if we can solve (Mm), then by implementing a binary search on the parameter k between 0 and N, we can determine the minimum attack cardinality whose optimal loss exceeds $\mathcal{L}_{\text{target}}$.

It turns out that application of the BD algorithm to the min-cardinality problem decomposes the min-cardinality problem into two single-level MIPs, namely the master (attacker) problem and the operator subproblem. The master problem only has the attack variables, integrality constraints, and the Benders cuts; and its objective function is

bounded. If the BD algorithm were applied to the budget-k-max-loss problem instead, the corresponding master problem will have variables d and u and eqs. (5.1) to (5.11) as constraints. Besides the computational advantage in solving the min-cardinality problem, the quantity $\frac{100\mathcal{L}_{\text{target}}}{\mathcal{L}_{\max}}$ is relevant from the viewpoint of DN resilience. For example, if we want to evaluate whether or not a DN is 80% resilient to a k cardinality attack, we can set $\mathcal{L}_{\text{target}} = 0.2\mathcal{L}_{\max}$, and then check if the optimal value of the min-cardinality problem is smaller than or equal k.

Now, we detail an approach to solve the min-cardinality problem. For given load and DG connectivity vectors kc and y, we define a **configuration** vector as $\kappa := (kc, y)$. Given an attack vector d, let $\mathcal{K}(d) := \{(kc, y) \in \{0,1\}^{\mathcal{N}} \times \{0,1\}^{\mathcal{N}}$ such that (5.10) holds$\}$, i.e. $\mathcal{K}(d)$ denotes the set of all possible post-disruption configuration vectors that the operator can choose from. Then, for a fixed attack d and a fixed configuration vector $\kappa \in \mathcal{K}(d)$, consider the following linear program:

$$\begin{aligned} \mathcal{P}(d, \kappa) \;:=\; & \min_{\beta \in \mathcal{B}} \; L(u, \mathrm{x}) \\ & \text{s.t. } u = (\beta, \kappa), \mathrm{x} \in \mathcal{X}(u), (5.11). \end{aligned} \tag{O-LP}$$

Note that (O-LP) may not have feasible solutions as the chosen configuration vector κ may violate (5.5) or (7.25) in the set of constraints $\mathcal{X}(u)$. In this case, the value of $\mathcal{P}(d, \kappa)$ is set to ∞.

Suppose that, for a given DN, we are concerned with a TN-side disturbance $\Delta \mathrm{v}_0$ and a target $\mathcal{L}_{\text{target}}$ post-contingency loss. We say that an attack-induced disruption $d \in \mathcal{D}_{\mathrm{k}}$ *defeats* a configuration $\kappa \in \mathcal{K}(d)$ if $\mathcal{P}(d, \kappa) \geqslant \mathcal{L}_{\text{target}}$, and is *successful* if it defeats *every* $\kappa \in \mathcal{K}(d)$. The above definition is analogous to the definition of successful attack considered in [24]. We can now state the *Min-cardinality disruption* problem as follows:

$$\begin{aligned} \min_{d \in \{0,1\}^{\mathcal{N}}} \quad & \sum_{i \in \mathcal{N}} d_i \\ \text{s.t.} \quad & \mathcal{P}(d, \kappa) \geqslant \mathcal{L}_{\text{target}} \quad \forall\, \kappa \in \mathcal{K}(d). \end{aligned} \tag{MCP}$$

If there exists an optimal solution of the problem (MCP), say $d^\star$, then it is a *min-cardinality disruption* corresponding to $\mathcal{L}_{\text{target}}$ because it is successful and has minimum number of

attacked nodes.

However, problem (MCP) is not tractable in its current form because the number of constraints are equal to the cardinality of set $\mathcal{K}(d)$ which can be exponential in $|\mathcal{N}|$, and verifying each constraint $\left(\mathcal{P}\left(d,\kappa\right) \geqslant \mathcal{L}_{\text{target}}\right)$ is itself a linear optimization problem. Fortunately, the BD algorithm can be applied to address this issue.

Benders Decomposition

The algorithm decomposes (MCP) into two relatively simpler mixed-integer (MIP) subproblems: attacker subproblem (A-MIP) and operator subproblem (O-MIP). Both these problems are then solved in an iterative manner. In fact, in each iteration, one needs to solve (A-MIP), (O-MIP), and the dual of the problem in (O-LP), as discussed below. Figure 5-5 summarizes the overall approach.

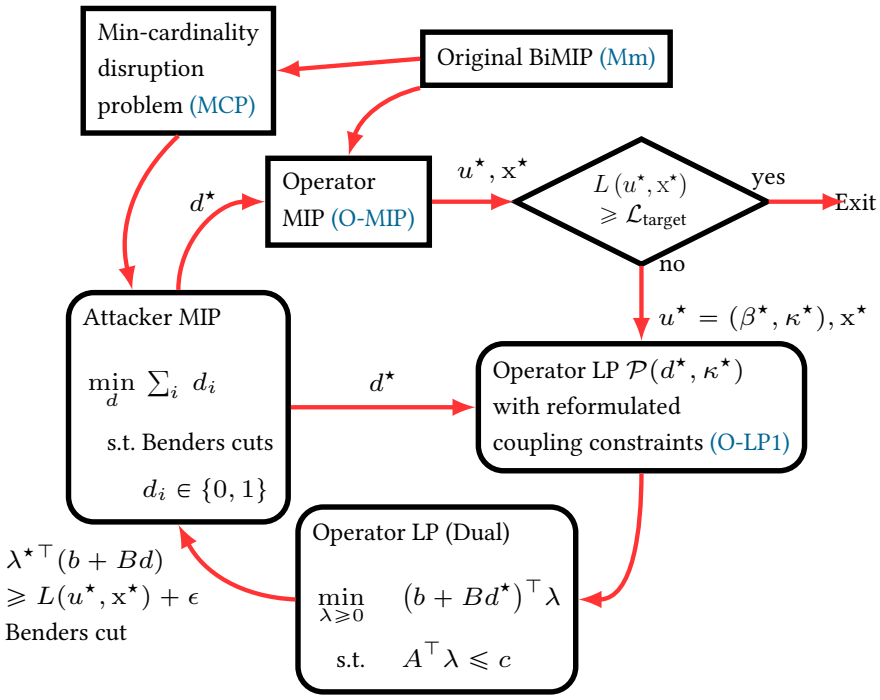


Figure 5-5: Computational approach to solve (Mm).

The attacker MIP can be written as follows:

$$\begin{aligned} \min_{d \in \{0,1\}^{\mathcal{N}}} \quad & \textstyle\sum_{i \in \mathcal{N}} d_i \\ \text{s.t.} \quad & \text{set of Benders cuts,} \end{aligned} \tag{A-MIP}$$

The master problem is initialized with only the integrality and budget constraints on the attack variables, and without any Benders cut. In each iteration, solving the master problem (A-MIP), which is a bounded MIP, if feasible, yields an attack $d^\star$. Then, this attack vector is used as an input parameter for the operator subproblem (O-MIP). For a fixed disruption $d^\star$, the operator subproblem is the same as the inner problem of (Mm):

$$\begin{aligned} \min_{u \in \mathcal{U}(d^\star)} \quad & L(u, \mathrm{x}) \\ \text{s.t.} \quad & \mathrm{x} \in \mathcal{X}(u), (5.11). \end{aligned} \tag{O-MIP}$$

The problem (O-MIP) is also a bounded MIP because the load and DGs have bounded feasible space. If (O-MIP) is feasible, it yields an optimal operator response $u^\star$ and network state $\mathrm{x}^\star$ for the disruption $d^\star$. If the operator's loss $L(u^\star, \mathrm{x}^\star)$ exceeds the target loss $\mathcal{L}_{\text{target}}$, the algorithm terminates having successfully determined an optimal min-cardinality attack. Otherwise, $L(u^\star, \mathrm{x}^\star) < \mathcal{L}_{\text{target}}$ which implies that $d^\star$ is not a successful disruption. In this case, we need to generate a Benders cut to eliminate $d^\star$ from the feasible space of (A-MIP).

To obtain a Benders cut, we select integer variables from the operator response $u^\star = (\beta^\star, \kappa^\star)$; i.e. select the configuration vector $\kappa^\star$, and consider the LP in (O-LP). However, we encounter an algorithmic issue which is as follows. Recall that in problem (Mm), the constraints (5.10) involve only the attack variables and operator binary variables. These constraints model the fact that, in our formulation, the DGs can get disconnected due to attacker actions as well as the operator response. When we fix these attack variables and inner binary variables in (5.10), the resulting linear program (O-LP) has constraints of the form $0 \geqslant 0$, $1 \geqslant 0$ or $1 \geqslant 1$. The values of the optimal dual variables ($\lambda^\star$) corresponding to these constraints (5.10) turn out to be 0, which are not useful in forming good Benders cuts. To address this issue, we modify the constraints of (O-LP) to ensure that the reformulated coupling constraints are such that coefficients of the attack variables (d) and the coefficients of inner continuous variables (pg, qg) are not simultaneously zero. One way

to achieve this is to replace (5.4) and (5.10) by the following constraints:

$$y_i \geqslant d_i, \tag{5.13a}$$

$$pg_i \leqslant (1 - d_i)\,\overline{\mathbf{pg}}_i, \qquad qg_i \leqslant (1 - d_i)\,\overline{\mathbf{qg}}_i, \tag{5.13b}$$

$$pg_i \leqslant (1 - y_i)\,\overline{\mathbf{pg}}_i, \qquad qg_i \leqslant (1 - y_i)\,\overline{\mathbf{qg}}_i, \tag{5.13c}$$

$$pg_i \geqslant (1 - y_i)\,\overline{\mathbf{pg}}_i, \qquad qg_i \geqslant (1 - y_i)\,\overline{\mathbf{qg}}_i, \tag{5.13d}$$

Note that (5.13a)-(5.13d) are equivalent to (5.4) and (5.10).[4][5] With this replacement, the values of the optimal dual variables ($\lambda^\star$) corresponding to the constraints (5.13b) will be non-zero, which ensures that useful Benders cuts will be generated in each iteration of the BD algorithm. Thus, we reformulate $\mathcal{P}(d, \kappa)$ as follows:

$$\begin{aligned} \mathcal{P}(d,\kappa) \;=\; \min_{\beta \in \mathcal{B}} \quad & L(u, \mathrm{x}) \\ \text{s.t.} \quad & u = (\beta, \kappa), (5.1) - (5.3), \\ & (5.5) - (5.11), (5.13). \end{aligned} \tag{O-LP1}$$

Note that problem (O-LP1) with parameters ($d^\star$, $\kappa^\star$) can be simplified and rewritten as the following problem whose dual is written alongside:

$$\begin{aligned} & \overbrace{\min_{w} \; c^\top w}^{\text{Primal}} && \overbrace{\max_{\lambda \geqslant \mathbf{0}} \; (b + Bd^\star)^\top \lambda}^{\textit{Dual}} \\ & \text{s.t. } A_{eq} w = b_{eq} + B_{eq} d^\star && \text{s.t. } A^\top \lambda = c \\ & \qquad A_{in} w \geqslant b_{in} + B_{in} d^\star \end{aligned} \tag{O-LP2}$$

Here w and λ are the primal and dual decision vector variables; $A = \left[{A_{eq}}^\top {A_{in}}^\top\right]^\top$, $B = \left[{B_{eq}}^\top {B_{in}}^\top\right]^\top$ are matrices and $b = \left[{b_{eq}}^\top {b_{in}}^\top\right]^\top$ is a vector of appropriate dimensions. We

[4] Using the constraints (5.4) and (5.13a)-(5.13b) is also equivalent to using (5.4) and (5.10). However, when the former set of constraints ((5.4) and (5.13a)-(5.13b)) are used, the implementation solver (Gurobi) assigns non-zero dual variables to the equality constraints (5.4) but not to (5.13b), which results in rendering of ineffective Benders cuts. Hence, (5.4) needs to be replaced by (5.13c)-(5.13d).

[5] Although for $(d_i, y_i) = (1, 1)$, the constraints (5.13c) and (5.13d) are equivalent to (5.13b), the implementation solver assigns non-zero dual variables to the inequality constraints that come up earlier in the implementation. Hence, these two sets of inequality constraints are placed *after* (5.13b).

solve the dual problem (thanks to strong duality, the optimal values are the same) in (O-LP2) to compute $\mathcal{P}\left(d^{\star}, \kappa^{\star}\right)$ and an optimal dual solution $\lambda^{\star}$. This furnishes a Benders cut, which is added to master problem in the next iteration. In particular, if the dual problem in (O-LP2) has an optimal solution $\lambda^{\star}$, and its optimal value is $L^{\star}$, then ${\lambda^{\star}}^{\top}\left(b+Bd\right) \geqslant L^{\star}+\epsilon$ is the desired Benders cut where ϵ is a small positive number. Note that $d^{\star}$ does not satisfy this Benders cut constraint because ${\lambda^{\star}}^{\top}\left(b+Bd^{\star}\right) = \mathcal{P}\left(d^{\star}, \kappa^{\star}\right) = L^{\star} < L^{\star}+\epsilon$, where the first equality holds because of strong duality in linear programs.

In each iteration, we eliminate suboptimal attacks from the feasible space of (A-MIP). Hence, the new master problem obtained by adding a Benders cut is a stronger relaxation of (MCP). Consequently, we get a progressively tighter lower bound on the minimum cardinality of the attack as the iteration continues, until we get a successful attack. Since there are a finite number of attacks, whether successful or not, the BD algorithm is bound to terminate.[6] As we will see in Sec. 5.4, the BD algorithm takes significantly fewer number of iterations in comparison to a simple enumeration.

The choice of ϵ in the generation of a Benders cut is an important issue in our implementation of the BD algorithm. If we choose too large an ϵ then many attacks (possibly including the optimal attacks) would be eliminated from the set of feasible attacker strategies in (A-MIP). If we choose too small an ϵ, then in each iteration only the current min-cardinality attack vector is eliminated resulting in performance no better than simple enumeration over all attacks.

Remark 7. Although we have used linear power flow approximation in our formulation, our approach can be generalized to consider the Second Order Cone approximation [90]. In this case, the formulation will be a Bilevel Mixed-Integer Second Order Cone Program (BiMISOCP) where the operator (inner) problem is an MISOCP. Our solution approach can, in fact, be generalized to solve the BiMISOCP by using the Generalized Benders Decomposition method [18].

We now offer some comparative remarks about our solution approach to (Mm) which – as mentioned earlier – is a BiMIP with conflicting objectives in the inner (operator)

[6] For realistically large network sizes ($N = 118$), the BD algorithm terminates in approximately 10 minutes.

and outer (attacker) problems. In general, one can reformulate a BiMIP into single level MIP (for example, using high-point relaxation (HPR) problem [92, 140]), and use advanced branch-and-bound algorithm to solve the problem. Note, however, the HPR is a weak relaxation of the original BiMIP due to directly conflicting objectives [69, 72]. More recent work has developed intersection cuts [55, 56] and disjunction cuts [85, 134] – these approaches introduce stronger cuts for the HPR problem. However, these approaches are suitable for BiMIPs in which the inner problem has integer coefficients in the constraints. On the other hand, our problem (Mm) has fractional coefficients. A recent paper by Hua et. al [69] addresses this issue by applying Generalized Benders decomposition method but without the min-cardinality reformulation; as a result, the master problem in their approach needs to handle relatively larger number of variables and constraints. Since in our solution approach we apply the Min-cardinality reformulation, the resulting master problem has fewer number of variables and constraints. Another approach by Zeng and An [145] uses Column Constraint Generation (CCG) method, whose iterations progressively add variables and constraints (particularly, the disjuntive constraints resulting from the KKT conditions for the inner problem with fixed binary variables). While these approaches are certainly of interest in solving (Mm), we find that our proposed approach achieves desirable computational performance as discussed in Sec. 5.4.

Estimating worst-case operator loss under autonomous disconnections

For each cardinality k, we compute the worst-case operator loss under the autonomous disconnections using simple enumeration. However, that would required evaluating operator loss over combinatorially many $\binom{N}{k}$ attacks. Therefore, we present a randomized algorithm to compute worst-case operator loss under the autonomous disconnections; see Algorithm 9.

Essentially, the algorithm aims to achieve the following: for each attack cardinality, it generates random attacks, compute the operator loss due to autonomous component disconnects (using Algorithm 8), and then choose the maximum among all computed losses.

Specifically, for a given parameter Z (number of random permutations) it initializes

Algorithm 9 Random and approximate worst-case attack under response (b)

Input: Z (number of random permutations)

Initialize $Y = \mathbf{0}_{N \times Z}$ and $V = \mathbf{0}_N$
for $t = 1, \cdots, Z$ **do**
  Generate a random permutation σ of nodes $\mathcal{N}$
  Reset $d = \mathbf{0}$
  for $\mathrm{k} = 1, \cdots, N$ **do**
    Set $d_{\sigma(\mathrm{k})} = 1$ ▷ k cardinality attack
    $(u_{\mathrm{nr}}, \mathrm{x}_{\mathrm{nr}}) \leftarrow$ GetCascadeFinalState(d) ▷ Refer Algorithm 8 for GetCascadeFinalState
    $Y[i, t] \leftarrow L(u_{\mathrm{nr}}, \mathrm{x}_{\mathrm{nr}})$
  end for
end for
for $\mathrm{k} = 1, \cdots, N$ **do**
  $V[\mathrm{k}] \leftarrow \max_{t \in [T]} Y[\mathrm{k}, t]$
end for
return Y, V

the entries of a matrix $Y \in \mathbb{R}^{\mathcal{N} \times \mathbb{Z}}$ and a vector $V \in \mathbb{R}^{\mathcal{N}}$ to zero. Next, for each iteration $t = 1, \cdots, Z$, it chooses a random permutation of the DN nodes $\mathcal{N}$, and resets $d = \mathbf{0}$. Then, it incrementally disrupts a DG belonging to a DN node in the order of the chosen t^{th} permutation, thereby obtaining a random attack for each cardinality k. For each attack generated in this manner, it computes the operator loss using Algorithm 8, and stores it in $Y[\mathrm{k}, t]$. After completely computing the matrix Y, it computes for each attack cardinality k, $V[\mathrm{k}] = \max_{t \in [Z]} Y[\mathrm{k}, t]$, i.e. the maximum over the computed losses. As shown in Sec. 5.4, for any randomly chosen attack of cardinality $\mathrm{k} < N$, if we disrupt one more DG, then the loss incurred by operator under autonomous disconnections would increase. This monotonicity of increasing operator loss for increasing attack cardinality cannot be shown if we simply choose $N + 1$ random attacks of cardinalities $\mathrm{k} \in \{0, \cdots, N\}$, and plot the operator loss values *vs.* k. This is the main idea behind Algorithm 9.

Computational Study

Now, we present computational results to show: (a) the value of timely operator response compared to autonomous disconnections; (b) comparison of the solutions of our BD approach with the optimal solution (generated for small networks by pure enumeration);

and (c) the scalability of our approach to larger networks.

Setup for computational study

We consider three networks: 24 node, and modified IEEE 36 node and 118 node networks. Each line has an identical impedance of $\mathbf{r}_{ij} = 0.01, \mathbf{x}_{ij} = 0.02$. Half of the nodes have a DG and half have a load. Hence, the maximum cardinality of an attack in our computational study will be half the number of the nodes in the DN. Consider a parameter $\alpha = \frac{6}{N}$. Before the contingency, each DG has active power output of $\overline{\mathbf{pg}}_i = \alpha$, and each load has a demand of $\overline{\mathbf{pc}}_i = 1.25\alpha$. Thus, we assume 80% DG penetration since the total DG output is 80% of the total demand. The voltage bounds are $\underline{\mathbf{vc}}_i = 0.9$, $\overline{\mathbf{vc}}_i = 1.1$, $\underline{\mathbf{vg}}_i = 0.92$ and $\overline{\mathbf{vg}}_i = 1.08$. The reactive power values are chosen to be exactly one third that of the corresponding active power value, i.e. a 0.95 power factor value for each load and DG. The values are chosen such that the total net active power demand in the DN is 0.75 pu, and the lowest voltage in the network before any contingency is close to $\underline{\mathbf{vg}}$. The maximum load control parameter is $\underline{\beta}_i = 0.8$, i.e. at most 20% of each load demand can be curtailed. For the sake of simplicity, we assume that all DGs and loads are homogeneous. The values of cost coefficients are chosen to be $\mathrm{W}^{\mathrm{LC}} = \frac{100}{\overline{\mathbf{pc}}_i}$, $\mathrm{W}_{\mathrm{VR}} = 100$ and $\mathrm{W}^{\mathrm{LS}} = \frac{1000}{\overline{\mathbf{pc}}_i}$.

All experiments were performed on a 2.8 GHz Intel Core i7 with 16 GB 1600 MHz DDR3 MacBook Pro laptop.

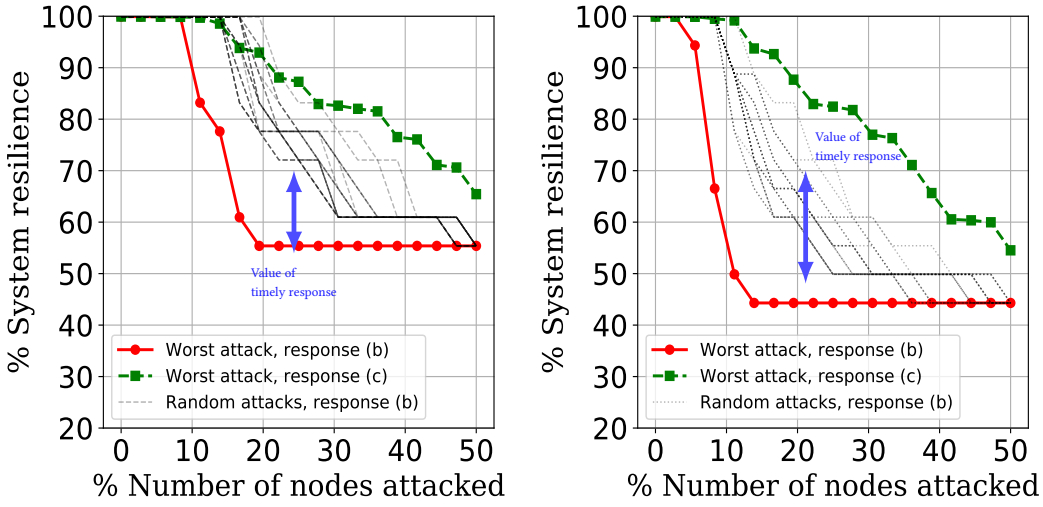
Value of timely response

Recall that in Sec. 5.1, we used post-contingency loss to define the resilience metric for operator response ($\mathcal{R}_{\text{Mm}}$) and autonomous disconnections ($\mathcal{R}_{\text{AD}}$) cases; and that $\mathcal{R}_{\text{Mm}} \geqslant \mathcal{R}_{\text{AD}}$. Figure 5-6 compares the resiliency values for the two cases (response (c) versus autonomous disconnections) for varying number of nodes attacked, where computation of $\mathcal{R}_{\text{Mm}}$ (resp. $\mathcal{R}_{\text{AD}}$) involves using BD algorithm (resp. Algorithm 8). In Figure 5-6, resiliency curve due to response (b) under random attacks is obtained by using Algorithm 9. We chose $Z = 500$, and select 10 out of Z random permutations σ (see Algorithm 9) to generate the plot. For a given cardinality k, the worst operator loss under autonomous disconnections is estimated by choosing $V[\mathrm{k}]$.

Note that, in Figure 5-6, for random attacks, the DN resilience under autonomous

disconnections monotonically decreases as the attack cardinality increases. Furthermore, the worst-case DN resilience due to compromise of less than 20% of nodes is equal to the corresponding value when all DGs are disrupted, i.e. the operator loss under autonomous disconnections quickly saturates. Therefore, the algorithmic choice of not computing the worst-case operator loss under autonomous disconnections by exhaustive enumeration over all possible attacks in Algorithm 9 is justified.

Indeed, under autonomous disconnections, we find that the voltage bound violations cause even the non-disrupted DGs to disconnect resulting in a cascade. However, under operator response, the SA detects these voltage bound violations, and *preemptively* exercises load control and/or disconnects the loads/DGs to reduce the total number of non-disrupted DGs from being disconnected, and minimize the impact of the attack. The difference between the two resiliency curves gives the value of timely response via the SA system. The intermediate curves in Figure 5-6 correspond to the DN resilience under random attacks and autonomous disconnections by the operator. Finally, when both a TN-side disturbance and a DN attack are simultaneous, the resilience metric of the DN decreases; see Figure 5-6b.

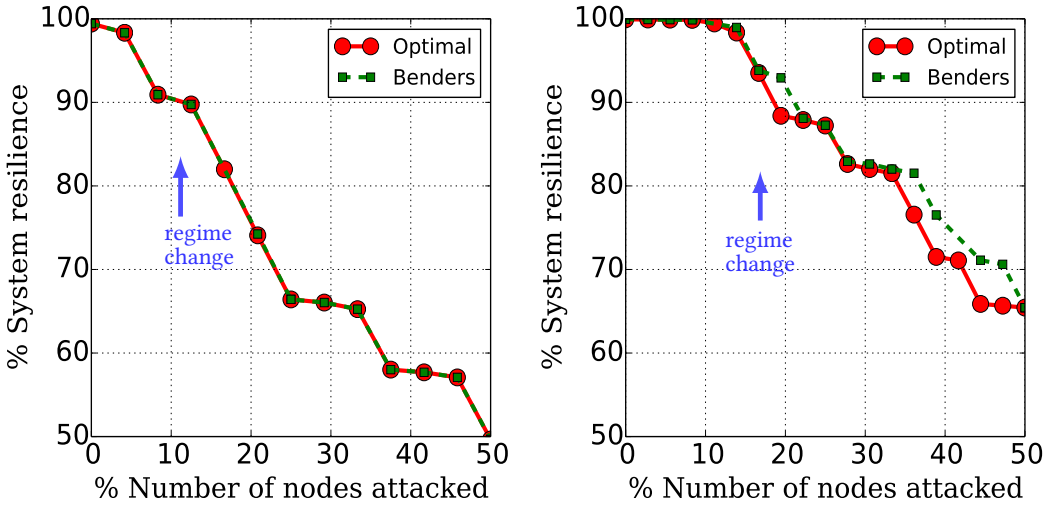


(a) $\Delta v_0 = 0$ (b) $\Delta v_0 = 0.02$

Figure 5-6: Value of timely response ($N = 36$).

Benders Decomposition method vs. Simple enumeration

For a fixed cardinality k, we compute the optimal loss $\mathcal{L}^\star$ using simple enumeration over all disruptions. Then, we use $\mathcal{L}^\star$ as the parameter $\mathcal{L}_{\text{target}}$ for the problem (MCP). If the BD algorithm applied to (MCP) computes a successful attack with the same cardinality k, then indeed we have obtained the optimal attack of cardinality k. Figure 5-7 shows that our method performs very well in computing optimal attacks. The sub-optimality results from the introduction of ϵ in the Benders cuts; see Figure 5-5.



(a) $N = 24$ (b) $N = 36$

Figure 5-7: Accuracy of BD algorithm in computing resilience metric in comparison to simple enumeration. Regime change from ND to CD is marked.

Scalability of BD algorithm

We tabulate the computational time required by the BD algorithm to compute min-cardinality attacks for different network sizes and varying values of the resilience metric $\mathcal{R}_{\text{target}} = 100\,(1 - \mathcal{L}_{\text{target}}/\mathcal{L}_{\max})$; see Table 5.3. Note that even for $N = 118$ nodes, which has 2^{118} configuration vectors, the BD algorithm finishes computations in ≈10 minutes. In comparison, for $N = 36$ node network, the simple enumeration method took ≈2 hours. The failure cases in Table 5.3 correspond to the cases where there does not exist an attack vector that exceeds the target loss values.

Table 5.3: Resiliency metric evaluated using BD algorithm. The realized resilience metric can significantly fall short of the target resilience metric ($\mathcal{R}_{\text{target}} = 100\,(1 - {}^{\mathcal{L}_{\text{target}}}/_{\mathcal{L}_{\max}})$); for example, when the attack cardinality changes from 1 to 2, the percentage resilience for 24-node network decreases sharply from 98.75% to 91.15% (which involves a change from the ND regime to the CD regime). This means that the 24-node DN is at least 90% (actual value 91.15%) resilient to k = 2 cardinality attacks.

Entries are resilience metric of DN (in percentage), number of iterations (written in brackets), time (in seconds), attack cardinality.			
$\mathcal{R}_{\text{target}}$	$N = 24$	$N = 36$	$N = 118$
99	98.75, (3), 0.04, 1	98.96, (11), 0.22, 5	98.52, (27), 1.86, 14
95	91.15, (6), 0.08, 2	93.82, (13), 0.27, 6	94.66, (39), 3.34, 17
90	89.75, (10), 0.16, 3	88.08, (15), 0.34, 8	89.94, (50), 5.44, 26
85	82.41, (11), 0.18, 4	82.93, (17), 0.4, 10	84.96, (69), 9.23, 44
80	74.38, (14), 0.26, 5	76.99, (21), 0.52, 14	79.71, (86), 613.42, 52
75	74.38, (14), 0.26, 5	71.1, (23), 0.59, 16	Failure
65	58.01, (20), 0.41, 9	Failure	
55	49.65, (23), 0.47, 12		
45	Failure		

Chapter 6

Leveraging Networked Microgrids for Distribution Network Resilience

In the previous chapter, we leveraged the capability of modern Substation Automation (SA) systems to enable preemptive load control and component disconnects in response to attacker-induced disruptions. This response capability allowed the operator to minimize the post-contingency loss. In this chapter, we consider a radial DN with one or more microgrids, and extend the operator response model to allow for dispatch of DERs as well as microgrid islanding. Furthermore, we also consider the problem of restoration of system performance by reconnection of disrupted components.

6.1 Value of microgrid operations

We model the sequential interaction between a DN operator and an external adversary as follows [114]:

$$\mathcal{L}_{\text{Mm}} := \max_{d \in \mathcal{D}_{\text{k}}} \min_{u \in \mathcal{U}(d)} L(u, \text{x}) \qquad \text{s.t.} \quad \text{x} \in \mathcal{X}(u), \tag{P1}$$

where $d \in \mathcal{D}_{\text{k}}$ denotes an attacker strategy, $u \in \mathcal{U}(d)$ an operator response strategy, $\text{x} \in \mathcal{X}$ the network state, and L the composite loss function. In [114], we argued that cyberphysical disruptions to DNs can lead to operating bound violations and cause uncontrolled or forced disconnects of DN components. Specifically, we modeled the impact of attacker-

induced disconnects of DN components as supply-demand disturbances, and the impact of TN-side disturbances as voltage deviations at the substation node. Then, we considered preemptive load control and component disconnects as operator response actions for the generic setting when the attacker's (resp. operator's) goal is to maximize (resp. minimize) the post-contingency losses. We introduced $\mathcal{R}_{\text{Mm}} := 100\left(1 - \frac{\mathcal{L}_{\text{Mm}}}{\mathcal{L}_{\max}}\right)$ as a resilience metric of the DN, where $\mathcal{L}_{\max}$ (chosen for sake of normalization) denotes the operator loss when all DN components are disconnected; see Figure 6-1. Finally, we evaluated the value of optimal response as the total reduction in post-contingency losses relative to case of autonomous disconnections, i.e. $\mathcal{R}_{\text{Mm}} - \mathcal{R}_{\text{AD}}$, where $\mathcal{R}_{\text{AD}} = 100\,(1 - {}^{\mathcal{L}_{\text{AD}}}/_{\mathcal{L}_{\max}})$.

In this article, we consider another bilevel formulation:

$$\mathcal{L}_{\text{MG}} := \max_{d \in \mathcal{D}^{\text{m}}_{\text{k}}} \min_{u \in \mathcal{U}_{\text{m}}(d)} L_{\text{m}}(u, \text{x}) \;\; \text{s.t. } \text{x} \in \mathcal{X}_{\text{m}}(u)\,, \tag{P2}$$

where the network model $\mathcal{X}_{\text{m}}$, and the loss function L_{m} are extended to capture microgrid operations (Sec. 6.2) and DER dispatch and regulation aspects; the set of attacker strategies $\mathcal{D}^{\text{m}}_{\text{k}}$ and the set of operator strategies $\mathcal{U}_{\text{m}}$ are also modified to capture attacker-operator interactions for DNs with DER-powered microgrids (Sec. 6.3). The maximin value of (P2), $\mathcal{L}_{\text{MG}}$, denotes the worst-case post-contingency loss incurred by the operator for the given microgrid and DER capabilities; see Figure 6-1. Then, $\mathcal{R}_{\text{MG}} := 100\,(1 - {}^{\mathcal{L}_{\text{MG}}}/_{\mathcal{L}_{\max}})$ can be viewed as a resilience metric of the DN under the microgrid-enabled operator response. Furthermore, the relative value of timely microgrid response (or equivalently, the improvement in DN resilience due to microgrids) can be evaluated as $(\mathcal{R}_{\text{MG}} - \mathcal{R}_{\text{Mm}})$. We posit that advances in DER-enabled microgrids and emergency control operations at substation level can be leveraged to implement timely resiliency-improving response actions (less than a few seconds after a disturbance event).

In [114], we considered three operator response capabilities:

(a) Remote control by the control center during nominal conditions;

(b) Autonomous disconnection of individual components (tripping of DGs or loads under nodal violations in operating conditions); and

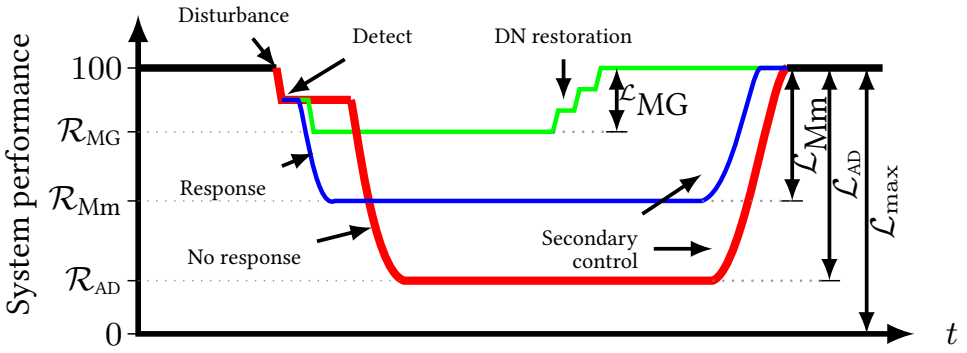


Figure 6-1: Performance under various response capabilities.

(c) Emergency control by a secure Substation Automation (SA) system.

In this paper, we consider the following extension of (c):

(d) emergency control by the SA involving microgrid islanding and DER dispatch.

Analogous to [114], we consider that the SA system can detect the disrupted components from changes in measurements of net nodal consumption. By using knowledge of the attack the SA can compute and implement the operator response in a timely manner. For our purposes, response (d) is an optimal second-stage response in (P2). Our analysis relies on the premise that such response can be implemented via modern SA systems during disruptions. Indeed, the continued improvements in SA systems' disturbance detection and control capabilities can further assist in restoration operations.

The resiliency of a system also reflects how quickly it can rebound to its nominal state after a disruption [93, 114]. Microgrids can provide partial demand satisfaction during the system restoration process, especially during the time when the DN is fully disconnected from the TN. We consider an admittedly simple, but practically relevant, multi-period DN restoration problem in which the disrupted DN components are gradually restored over several periods; refer to "DN restoration" in Figure 6-1. Our goal in this problem is to compute an operator strategy in each time period (roughly, on the order of a few minutes). Such a strategy is comprised of reconnecting disrupted components, modifying the microgrid islanding configuration, and dispatching the DERs within individual microgrids.

Our modeling approach addresses some key issues regarding microgrid and DER operations. In particular, we allow for the formation of one or more microgrid islands in radial DNs. When all the microgrids are connected to the transmission network (TN), the DN is operating in the *grid-connected* regime. If none of the microgrids are connected to the TN, then the DN is operating in the *fully-islanded* regime. In our approach, the DN can also operate in a *partially-islanded* regime, in which some of the microgrids are connected to the TN while other microgrids are not. In both partially- and fully- islanded regimes, each microgrid can operate as an isolated microgrid or as a part of a bigger microgrid. To model power flows in each of the microgrids, we introduce a natural extension of the LinDistFlow equations. The resulting network model captures DN operations in all the above-mentioned regimes (Sec. 6.2). We limit attention to linear power flows mainly for the ease of exposition.

Importantly, we consider the parallel operation of multiple DERs for the provision of *grid-forming* services, which involve providing voltage and frequency references, as well as maintaining voltage and frequency within operating bounds (i.e. *regulation* services). When a microgrid is connected to the TN, the bulk generators provide the grid-forming services. However, when a microgrid is disconnected from the TN, then at least one DER within that microgrid must provide the grid-forming services [84]. Depending on the number of grid-forming DERs within a microgrid, one can consider two modes of DER operation under islanded regimes namely: Single-Master Operation (with a single grid-forming DER) and Multi-Master Operation (with more than one grid-forming DER) [84]. Our model is simple and flexible enough to capture both the single-/multi- master modes of DER operation. In addition to voltage regulation, we also consider frequency regulation, which becomes important for microgrids due to low inertia of the DERs. By using the appropriate droop control equations, we capture both frequency and voltage regulation aspects resulting from multiple DERs operating in parallel within a microgrid.

Our main contributions are as follows:

($\star$) We capture the different microgrid regimes as well as DER operating modes by developing a new mixed-integer linear network model. This modeling approach enables us to formulate (P2) as a Bilevel Mixed-Integer Problem (BiMIP). In [114],

we showed that (P1) is also a BiMIP, and can be solved using a Benders Decomposition (BD) algorithm. In Sec. 6.3, we show that this algorithm can be applied to the extended formulation (P2).

($\star$) Our network model is also well-suited for formulating a DN restoration problem as a multi-period Mixed-Integer Problem (MIP). In our restoration problem, the network state in any period only depends on the operator response actions in that period, and the network state in the previous period. We exploit this feature and propose a greedy heuristic that seeks to reconnect the disrupted components in each period such that the post-contingency losses for that period are minimized (Sec. 6.4).

6.2 Multi-microgrid network model

In this section, we develop a model of a radial DN with one or more microgrids. This network model extends the LinDistFlow model [16] to multi-microgrid settings.

We distinguish between two operating stages o and c, which denote the pre- and post-contingency stage, respectively. The network is initially in o stage, and after the disturbance event, it enters in the c stage; see Sec. 6.3 for details on the disturbance model. Let $\eta \in \{o, c\}$ denote the operating stage of the network. We define the network state as $\mathrm{x}^\eta := (p^\eta, q^\eta, P^\eta, Q^\eta, \mathrm{v}^\eta, f^\eta)^\top$, where each of these entries are themselves row vectors of appropriate dimensions, and are described in Table 6.1.

In our DN model, we consider a radial network consisting of one or more microgrids. We refer to a distribution line $(i, j) \in \mathcal{M} \subseteq \mathcal{E}$ as a microgrid *connecting line* if it connects a microgrid to the TN or to other microgrids; see Figure 6-2. Here $\mathcal{M}$ denotes a given fixed set of connecting lines. For a connecting line $(i, j) \in \mathcal{M}$, we use $kl_{ij}^\eta = 0$ (resp. $kl_{ij}^\eta = 1$) to indicate that it is in closed (resp. open) state. Based on the states of the connecting lines, the DN can operate in any of the following "regimes":

- *Grid-connected regime* when all connecting lines are closed (i.e $kl_{ij}^\eta = 0 \quad \forall\, (i, j) \in \mathcal{M}$),
- *Fully-islanded regime* when all connecting lines are open (i.e. $kl_{ij}^\eta = 1 \quad \forall\, (i, j) \in \mathcal{M}$), or

Table 6.1: Table of Notations.

DN parameters	
$\mathcal{N}$	set of nodes in DN
$\mathcal{E}$	set of edges in DN
0	substation node label
$\mathcal{M} \subseteq \mathcal{E}$	set of microgrid connecting lines
$\mathcal{N}_i \subseteq \mathcal{N}$	nodes belonging to i^{th} microgrid
$\mathcal{M}_i \subseteq \mathcal{M}$	set of lines which if open isolate the i^{th} microgrid
$\mathbf{j}$	complex square root of -1, $\mathbf{j} = \sqrt{-1}$
$\mathrm{v}^{\mathbf{nom}}$	nominal squared voltage magnitude (1 pu)
$\mathbf{f}^{\mathbf{nom}}$	nominal system frequency (1 pu)
$\mathcal{P}_i \subseteq \mathcal{E}$	lines on the path between node i and substation node
DER categories	
$\mathcal{S}$	set of DERs
$\mathcal{S}_{\text{gf}} \subseteq \mathcal{S}$	set of grid-forming DERs
$\mathcal{S} \subseteq \mathcal{S}_{\text{gf}}$	set of PQ Inverter (PQI)-controlled DERs
$\mathcal{S}_{\text{pq}}^{\text{fixed}} \subseteq \mathcal{S}_{\text{pq}}$	set of PQI-controlled DERs with fixed setpoints
$\mathcal{S}_{\text{pq}}^{\text{var}} \subset \mathcal{S}_{\text{pq}}$	set of PQI-controlled DERs with controllable setpoints
$\mathcal{S}_{\text{gf}}^{\text{utility}} \subseteq \mathcal{S}_{\text{gf}}$	set of utility-owned grid-forming DERs
$\mathcal{S}_{\text{gf}}^{\text{facility}} \subseteq \mathcal{S}_{\text{gf}}$	set of facility level microgrid-specific grid-forming DERs
$\mathcal{S}_{\text{gi}} = \mathcal{S}_{\text{gf}} \bigcup \mathcal{S}_{\text{pq}}^{\text{var}}$	set of grid-interactive DERs
Nodal quantities of node $i \in \mathcal{N}$	
v_i	squared voltage magnitude at node i
f_i	system frequency measured at node i
$\underline{\mathbf{vc}}_i, \overline{\mathbf{vc}}_i$	lower, upper voltage bounds for load i
$\underline{\mathbf{vg}}_i, \overline{\mathbf{vg}}_i$	lower, upper voltage bounds for DG i
$\underline{\mathbf{fc}}_i, \overline{\mathbf{fc}}_i$	lower, upper frequency bounds for load i
$\underline{\mathbf{fg}}_i, \overline{\mathbf{fg}}_i$	lower, upper frequency bounds for DG i
$\overline{\mathbf{pc}}_i + \mathbf{j}\overline{\mathbf{qc}}_i$	nominal demand at node i
$pc_i + \mathbf{j}qc_i$	actual power consumed at node i
$kc_i \in \{0, 1\}$	0 if load i is connected to DN; 1 otherwise
β_i	fraction of demand satisfied at node i
$\underline{\beta}_i$	lower bound of load control parameter β_i
$\overline{\mathbf{pg}}_i + \mathbf{j}\overline{\mathbf{qg}}_i$	nominal generation of DG $i \in \mathcal{S}_{\text{pq}}^{\text{fixed}}$
$pg_i + \mathbf{j}qg_i$	actual power generated by DER $i \in \mathcal{S}_{\text{pq}}^{\text{fixed}}$
$y_i \in \{0, 1\}$	0 if DG $i \in \mathcal{S}_{\text{pq}}^{\text{fixed}}$ is connected to DN; 1 otherwise
Quantities of DER $s \in \mathcal{S}$	
$j(s)$	the DN node where the DER $s \in \mathcal{S}_{\text{gf}}$ is located
$J(S) \subseteq \mathcal{N}$	the set of DN nodes where the DERs in the set $S \subseteq \mathcal{S}$ are located
$\overline{\mathbf{sn}}_s$	apparent power capability of microsource $s \in \mathcal{S}_{\text{gf}}$
$\underline{\mathbf{pn}}_s, \overline{\mathbf{pn}}_s$	lower, upper active power bounds of microsource $s \in \mathcal{S}_{\text{gf}}$
$\underline{\mathbf{qn}}_s, \overline{\mathbf{qn}}_s$	lower, upper reactive power bounds of microsource $s \in \mathcal{S}_{\text{gf}}$
$pn_s + \mathbf{j}qn_s$	total power supplied by microsource $s \in \mathcal{S}_{\text{gf}}$
$\overline{\mathbf{se}}_s$	apparent power capability of storage device $s \in \mathcal{S}_{\text{gf}}$
$\underline{\mathbf{pe}}_s, \overline{\mathbf{pe}}_s$	lower, upper active power bounds of storage $s \in \mathcal{S}_{\text{gf}}$
$\underline{\mathbf{qe}}_s, \overline{\mathbf{qe}}_s$	lower, upper reactive power bounds of storage $s \in \mathcal{S}_{\text{gf}}$
$pe_s + \mathbf{j}qe_s$	total power supplied by storage $s \in \mathcal{S}_{\text{gf}}$
$kr_s \in \{0, 1\}$	1 if DER $s \in \mathcal{S}_{\text{gf}}$ contributes to grid-forming services
$pr_s + \mathbf{j}qr_s$	total power supplied by DER $s \in \mathcal{S}_{\text{gf}}$
$pr_s^{\text{ref}}, qr_s^{\text{ref}}$	active, reactive power references of DER $s \in \mathcal{S}_{\text{gf}}$
$f_s^{\text{ref}}, \mathrm{v}_s^{\text{ref}}$	frequence, voltage references of DER $s \in \mathcal{S}_{\text{gf}}$
Parameters of edge $(i, j) \in \mathcal{E}$	
$kl_{ij} \in \{0, 1\}$	1 if (i, j) is switched open; 0 otherwise
$P_{ij} + \mathbf{j}Q_{ij}$	power flowing from node i to node j
$\mathbf{r}_{ij}, \mathbf{x}_{ij}$	resistance and reactance of line $(i, j) \in \mathcal{E}$

- *Partially-islanded regime* when there exists at least two connecting lines such that one of them is closed and other is open (i.e. $\exists\ (i,j),(m,n) \in \mathcal{M}$ such that $kl^{\eta}_{ij} = 0$ and $kl^{\eta}_{mn} = 1$).

Let $\{\mathcal{N}_1, \cdots, \mathcal{N}_{|\mathcal{M}|}\}$ denote the set of disjoint microgrid subnetworks of the DN, where each $\mathcal{N}_i$ for $i \in \{1, \cdots, |\mathcal{M}|\}$ denotes a connected subnetwork when all connecting lines are open, i.e. $kl^{\eta}_{mn} = 1$ for all $(m,n) \in \mathcal{M}$. For each subnetwork $\mathcal{N}_i$, let $\mathcal{M}_i \subseteq \mathcal{M}$ denote the set of connecting lines which need to be open for $\mathcal{N}_i$ to be completely isolated (i.e. autonomously operating). A *microgrid island* is formed when an individual microgrid or a connected subnetwork of more than one microgrid no longer receives power supply from the TN. Also, let $\mathcal{P}_i$ denote the set of lines along the path connecting node i to the substation node. For example, in Figure 6-2, the set of connecting lines for the subnetwork $\mathcal{N}_1 = \{1,2\}$ is $\mathcal{M}_1 = \{(0,1),(2,3),(2,5)\}$, and $\mathcal{P}_5 = \{(0,1),(1,2),(2,5)\}$. Also, if $kl^{\eta}_{01} = 1$, $kl^{\eta}_{23} = 0$, and $kl^{\eta}_{25} = 1$, then the microgrid $\mathcal{N}_3$ is operating as an isolated island, whereas microgrids $\mathcal{N}_1$ and $\mathcal{N}_2$ are operating together as part of one bigger microgrid island.

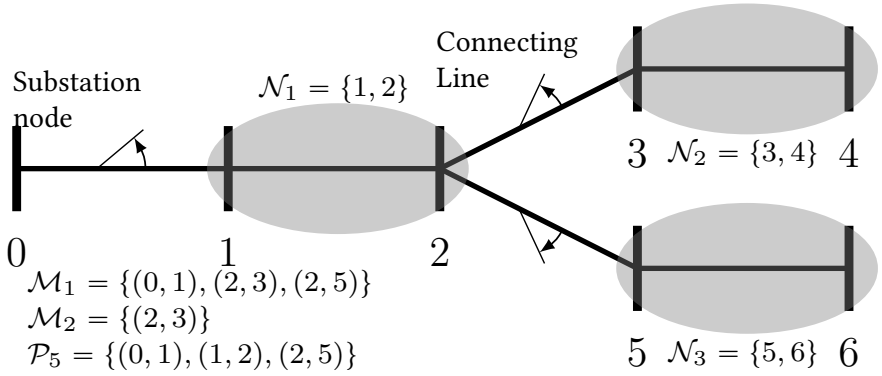


Figure 6-2: Multi-microgrid DN model.

Remark 8. The smaller microgrids are typically used for supplying power to a critical facility (e.g. hospital, university, prison). In our model, these microgrids can be leveraged to supply power to the DN during emergency conditions (fully- or partially- islanded regimes).

Now, we describe the constraints related to the power flows, nodal frequencies and load connectivity in microgrids. Unless explicitly stated, the following constraints are

valid for either operating stage $\eta \in \{o, c\}$.

1. *Power flows:* A connecting line permits power flow through it if and only if it is *closed*. We model this constraint as follows:

$$\left|P_{ij}^{\eta}\right| \leqslant \left(1 - kl_{ij}^{\eta}\right) \mathrm{L} \qquad \forall\, (i,j) \in \mathcal{M} \tag{6.1a}$$

$$\left|Q_{ij}^{\eta}\right| \leqslant \left(1 - kl_{ij}^{\eta}\right) \mathrm{L} \qquad \forall\, (i,j) \in \mathcal{M}, \tag{6.1b}$$

where L is a large constant. This typical modeling trick to use a constraint of the type $|a - c| \leqslant y\mathrm{L}$ where $y \in \{0, 1\}$, enforces an equality $a = c$ only when $y = 0$; otherwise the equality is not binding. We use this trick repeatedly to model various other constraints of a similar type.

2. *Voltage drop:* The voltage drop along a non-connecting line $(i, j) \notin \mathcal{M}$ is given by the standard voltage drop equation of the LinDistFlow model [16]:

$$\mathrm{v}_j^{\eta} = \mathrm{v}_i^{\eta} - 2\mathbf{r}_{ij}P_{ij}^{\eta} - 2\mathbf{x}_{ij}Q_{ij}^{\eta} \quad \forall\, (i,j) \in \mathcal{E} \backslash \mathcal{M}. \tag{6.2}$$

However, for a connecting line, the voltage drop constraint is active only if it is closed, and is inactive, otherwise, i.e.

$$\left|\mathrm{v}_j^{\eta} - \left(\mathrm{v}_i^{\eta} - 2\mathbf{r}_{ij}P_{ij}^{\eta} - 2\mathbf{x}_{ij}Q_{ij}^{\eta}\right)\right| \leqslant kl_{ij}^{\eta}\mathrm{L} \quad \forall\, (i,j) \in \mathcal{M}. \tag{6.3}$$

3. *Nodal frequencies:* In islanded regimes, the DER(s) must provide grid-forming and regulation services [83, 84]. Moreover, a microgrid island can have multiple DERs operating in parallel. We assume that DERs can rapidly synchronize their frequencies to a common value with the help of power electronics [84]. This value can be regarded as the island's frequency. To model that the nodal frequencies within a microgrid island are identical in steady state, we can write:

$$f_i^{\eta} = f_j^{\eta} \quad \forall\, i, j \in \mathcal{N}_k \text{ and } \forall\, k = 1, \cdots, |\mathcal{M}|\,,$$

which is equivalent to writing:

$$f_i^\eta = f_j^\eta \qquad \forall\ (i,j) \in \mathcal{E}\backslash\mathcal{M}, \tag{6.4}$$

because if a line (i,j) is not a connecting line, i.e. $(i,j) \in \mathcal{E}\backslash\mathcal{M}$, then nodes i and j both belong to the same microgrid. Generically, frequency of every microgrid island can be different from the frequency of the TN-connected substation node. Moreover, the frequencies of any two microgrid islands that are not connected to each other can also be different. We model this constraint as follows:

$$\left|f_i^\eta - f_j^\eta\right| \leqslant kl_{ij}^\eta \mathrm{L} \qquad \forall\ (i,j) \in \mathcal{M}. \tag{6.5}$$

Finally, we model the constraint that the load gets disconnected (i.e. $kc_i^\eta = 1$) when the nodal frequency violates the safe operating bounds:

$$kc_i^\eta \geqslant \underline{\mathbf{fc}}_i - f_i^\eta, \qquad kc_i^\eta \geqslant f_i^\eta - \overline{\mathbf{fc}}_i \qquad \forall\ i \in \mathcal{N}. \tag{6.6}$$

Distributed Energy Resources (DERs)

We now introduce a generic taxonomy of DERs that is relevant to microgrid operations (see [71]) and a model which captures both single- and multi-master operating modes of DERs. Please refer to Figure 6-3 for DER categories and Table 6.2 for a comparison of their capabilities.

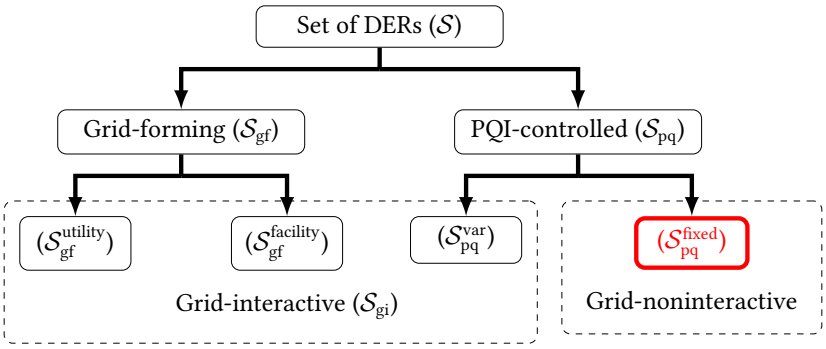


Figure 6-3: Basic taxonomy of DERs [71].

Attribute	Grid-noninteractive ($\mathcal{S}_{pq}^{fixed}$)	Grid-interactive ($\mathcal{S}_{gi} = \mathcal{S}_{gf} \bigcup \mathcal{S}_{pq}^{var}$)
Power output	fixed	variable/responsive to grid conditions
Controllable by response (a)	yes	no (can act as zero output source while being connected)
Controllable by response (b)	yes (due to operating bound violations)	no (LVRT & LFRT available)
Controllable by response (c)	N/A	yes
Controllable by response (d)	yes	yes

(a) Grid-interactive vs. grid-noninteractive DERs

Attribute	PQI-controlled DERs with variable setpoints ($\mathcal{S}_{pq}^{var}$)	Grid-forming ($\mathcal{S}_{gf}$)
Grid-forming	no	yes (under specific islanding conditions)
Output control	Remote setpoint control	Droop-based control

(b) PQI-controlled vs. grid-forming DERs.

Attribute	Utility-owned ($\mathcal{S}_{gf}^{utility}$)	Facility level ($\mathcal{S}_{gf}^{facility}$)
Ownership	Utility	Facility
Islanding condition	microgrid not connected to TN but can stay connected to other microgrid(s) (explained later in (6.7))	microgrid operates as an isolated island (explained later in (6.8))

(c) Utility (operator) owned grid-forming DERs vs. facility level grid-forming DERs.

Table 6.2: Comparison of DER categories.

DER classification

Our classification is based on the output behaviour and service capabilities of DERs. First, we distinguish between grid-forming DERs (which provide voltage and frequency references) and DERs whose active (P) and reactive (Q) power output is controlled by PQ inverters. We denote the sets of grid-forming and PQ Inverter (PQI-) controlled DERs by $\mathcal{S}_{\text{gf}}$ and $\mathcal{S}_{\text{pq}}$, respectively. Then, there are further two sub-categories of PQI-controlled DERs: those whose PQ setpoints can be remotely controlled (denoted by $\mathcal{S}_{\text{pq}}^{\text{var}}$), and others whose PQ setpoints are fixed (denoted by $\mathcal{S}_{\text{pq}}^{\text{fixed}}$). Since the output of the DERs belonging to the set $\mathcal{S}_{\text{pq}}^{\text{fixed}}$ does not vary with the grid conditions, they can be considered as grid-noninteractive DERs. On the other hand, since the output of the DERs in the sets $\mathcal{S}_{\text{gf}}$ and $\mathcal{S}_{\text{pq}}^{\text{var}}$ can change with grid-conditions, we consider them as grid-interactive DERs (denoted by $\mathcal{S}_{\text{gi}}$); see Table 6.2a. For the sake of clarity, we refer to DERs in set $\mathcal{S}_{\text{pq}}^{\text{fixed}}$ as distributed generators (DGs). Since the output of these DGs cannot be changed, if operating bound violations occur, then they need to be disconnected either by remote means or through autonomous disconnections.

In contrast, the grid-interactive DERs can stay connected to DN as zero output sources even under fluctuations in the network state. Particularly, we assume that these DERs are fitted with low-voltage and low-frequency ride through (LVRT and LFRT) functionalities. This allows DERs to stay connected to the DN during temporary voltage and frequency bound violations at nodes. Furthermore, the output of grid-interactive DERs can be changed by two control mechanisms. In the case of grid-forming DERs ($\mathcal{S}_{\text{gf}}$), droop-based primary control is activated under specific islanding conditions. In the case of DERs in the set $\mathcal{S}_{\text{pq}}^{\text{var}}$, their active-reactive (PQ) setpoints can be controlled by the SA system; see Table 6.2b.

Let $\mathcal{I} \subseteq \mathcal{N}$ be a subset of nodes such that they can form a microgrid island within the DN. Let $\mathcal{N}_{\mathcal{I}}$ denote the corresponding microgrid island. Recall from Sec. 6.2 that a microgrid island can consist of one or more microgrids. Based on the number of DERs contributing to grid-forming services, a microgrid island can be in the following operating modes [84]:

1. Single Master Operation (SMO): One DER operates as a single grid-forming DER (i.e. $\left|J(\mathcal{S}_{\text{gf}}) \bigcap \mathcal{N}_{\mathcal{I}}\right| = 1$), while all other DERs operate in the PQ mode.

2. Multi Master Operation (MMO): More than one DER (but not necessarily all) operate as grid-forming DERs (i.e. $\left|J(\mathcal{S}_{\text{gf}}) \bigcap \mathcal{N}_{\mathcal{I}}\right| \geqslant 2$).

In the multi-master operation, the output of multiple grid-forming DERs changes based on nodal voltage and frequency values under the droop control constraints. These constraints ensure appropriate power sharing among DERs based on their capacities. The nodal frequencies (resp. voltages) are used for active (resp. reactive) power sharing. Our network model for radial DNs is flexible enough to allow DN operations in both SMO and MMO modes.

Finally, there are two sub-categories of grid-forming DERs, namely utility (or operator) owned grid-forming DERs and grid-forming DERs belonging to some facilities. Each of these categories contributes to grid-forming services depending on the specific islanding conditions; see Table 6.2c. Let $kr_s^{\eta} = 1$ if the islanding condition for DER $s \in \mathcal{S}_{\text{gf}}$ is satisfied, and $kr_s^{\eta} = 0$ otherwise. The two main islanding conditions of interest are as follows:

1. An utility grid-forming DER contributes to grid-forming services when the node to which it belongs becomes a part of a microgrid island (i.e. the node is not connected to the TN). Consider a DER $s \in \mathcal{S}_{\text{gf}}^{\text{utility}}$ and a microgrid $\mathcal{N}_k$ such that $j(s) = i \in \mathcal{N}_k$. Then, DER s contributes to grid-forming if and only if $\mathcal{N}_k$ is not connected to the TN, or equivalently, at least one connecting line along the path connecting node i to the substation is open, i.e.

$$kr_s^{\eta} = 1 \iff \exists\ (m,n) \in \mathcal{M} \bigcap \mathcal{P}_i \ \text{ such that } \ kl_{mn}^{\eta} = 1.$$

We formulate this condition using the following mixed-integer linear constraints:

$$kr_s^{\eta} \geqslant kl_{mn}^{\eta} \qquad \forall\ (m,n) \in \mathcal{M} \bigcap \mathcal{P}_i \tag{6.7a}$$

$$kr_s^{\eta} \leqslant \textstyle\sum_{(m,n) \in (\mathcal{M} \bigcap \mathcal{P}_i)} \ kl_{mn}^{\eta}. \tag{6.7b}$$

2. The facility level DERs (denoted by $\mathcal{S}_{\text{gf}}^{\text{facility}}$) also contribute to grid-forming services

when the microgrid to which they belong operates as an isolated island (i.e. not connected to the TN and to any other microgrid). Consider a DER $s \in \mathcal{S}_{\text{gf}}^{\text{facility}}$ and a microgrid $\mathcal{N}_i$ such that $j(s) \in \mathcal{N}_i$. Then, DER s contributes to grid-forming if and only if all the connecting lines connecting the microgrid $\mathcal{N}_i$ to the TN or other microgrids are open, i.e.

$$kr_s^\eta = 1 \iff kl_{mn}^\eta = 1 \; \forall \; (m,n) \in \mathcal{M}_i.$$

We formulate this condition using the following mixed-integer linear constraints:

$$kr_s^\eta \geqslant \left(\textstyle\sum_{(m,n)\in\mathcal{M}_i} \; kl_{mn}^\eta \right) - (|\mathcal{M}_i| - 1) \tag{6.8a}$$

$$kr_s^\eta \leqslant kl_{mn}^\eta \qquad \forall \; (m,n) \in \mathcal{M}_i. \tag{6.8b}$$

DER output model

Next, we describe the output model for the DERs. Each grid-forming DER $s \in \mathcal{S}_{\text{gf}}$ consists of a microsource and a storage device (batteries or flywheels) [84]. The microsource supplies power (quadrants I or II) in all three regimes. Thus, the output of the microsource is constrained as follows:

$$Gn_s [pn_s^\eta \quad qn_s^\eta]^\top \leqslant hn_s \quad \forall \; s \in \mathcal{S}_{\text{gf}}, \tag{6.9}$$

where $Gn_s \in \mathbb{R}^{6\times 2}$ is a matrix and $hn_s \in \mathbb{R}^6$ is a vector that represents the polytope as shown in Figure 6-4a.

For the sake of modeling simplicity, we assume that the storage device supplies power only in the islanded regimes, whereas it consumes power in the grid-connected regime (quadrants III and IV); see Figure 6-4. One justification for this restriction is that the life of a storage device significantly degrades with frequent charging/discharging cycles [84]. Indeed, advances in storage technology make them viable sources of power supply even in grid-connected regime. Still our modeling assumption is relevant to situations where fixed storage capacity is set aside as contingency reserve to be used in islanded regimes.

Thus, the output of a storage device is constrained as follows:

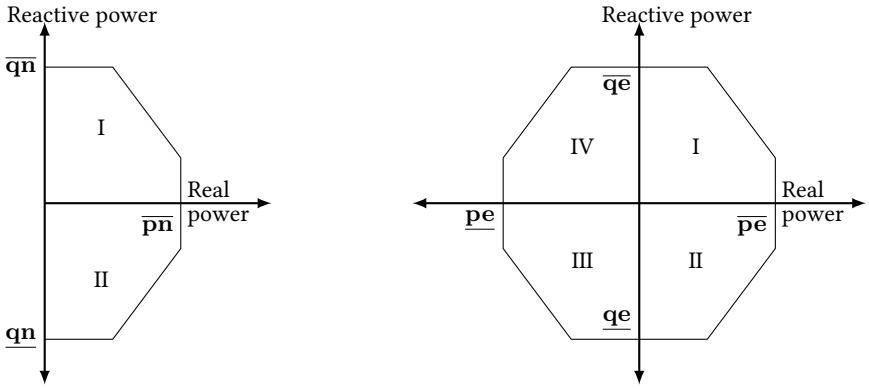
$$Ge_s[pe_s^\eta \quad qe_s^\eta]^\top + H_s kr_s^\eta \leqslant he_s \quad \forall\, s \in \mathcal{S}_{\text{gf}}, \tag{6.10}$$

where the $Ge_s, H_s \in \mathbb{R}^{8\times 2}$ are matrices and $he_s \in \mathbb{R}^8$ is a vector such that the DER operates in quadrants III and IV when $kr_s^\eta = 0$; and in quadrants I and II when $kr_s^\eta = 1$; see Figure 6-4b.

The total output of the DER is given by:

$$\begin{aligned} pr_s^\eta &= pn_s^\eta + pe_s^\eta \qquad \forall\, s \in \mathcal{S}_{\text{gf}} \\ qr_s^\eta &= qn_s^\eta + qe_s^\eta \qquad \forall\, s \in \mathcal{S}_{\text{gf}}. \end{aligned} \tag{6.11}$$

On the other hand, PQI-controlled DERs ($\mathcal{S}_{\text{pq}}$) consist only of microsource, and do not have a storage device. Thus, their output is constrained as in Figure 6-4a. We can simply assume that $\forall\, s \in \mathcal{S}_{\text{pq}},\ pe_s^\eta = qe_s^\eta = 0$.



(a) Microsource model (b) Storage device model

Figure 6-4: DER output model [110].

Droop control equations

We model the regulation services provided by one or more grid-forming DERs using the voltage and frequency droop control equations [83]. This allows the DERs to adjust their active and reactive power outputs based on local voltage and frequency measurements, thus eliminating the need for explicit coordination among DERs (for the purpose of reg-

ulation).

The output changes of a grid-forming DER $s \in \mathcal{S}_{\text{gf}}$ depend on whether or not it is contributing to regulation (i.e. kr_s^η = 1 or 0) based on the islanding conditions (see (6.7) and (6.8)). Then, the classical voltage droop equation [83] can be refined to model the reactive power output of grid-forming DER as follows (see Figure 6-5a):

$$\begin{aligned} \left| \mathrm{v}_i^\eta - \left(\mathbf{v}_s^{\text{ref}} - \mathbf{mq}_i (qr_s^\eta - qr_s^{\text{ref}}) \right) \right| \leqslant (1 - kr_s^\eta)\, \mathrm{L} \\ \forall\ s \in \mathcal{S}_{\text{gf}}, i \in \mathcal{N} \ \text{ and } \ i = j(s). \end{aligned} \tag{6.12}$$

eq. (7.22) implies that when a DER provides regulation, it contributes more (resp. less) reactive power as the voltage drops (resp. rises) relative to a reference value.

Similarly, the classical frequency droop control equation [83] can be refined to model the active power output of a grid-forming DER as follows (see Figure 6-5b):

$$\begin{aligned} \left| f_i^\eta - \left(f_s^{\text{ref}} - \mathbf{mp}_s \left(pr_s^\eta - pr_s^{\text{ref}} \right) \right) \right| \leqslant (1 - kr_s^\eta)\, \mathrm{L} \\ \forall\ s \in \mathcal{S}_{\text{gf}}, i \in \mathcal{N} \ \text{ and } \ i = j(s). \end{aligned} \tag{6.13}$$

eq. (6.13) ensures proper power sharing in the sense that DERs can adjust their active power contributions for frequency regulation depending on their individual capacities. The reference setpoints $(f_s^{\text{ref}}, \mathbf{v}_s^{\text{ref}}, pr_s^{\text{ref}}, qr_s^{\text{ref}})$ and the droop coefficients $(\mathbf{mp}_s, \mathbf{mq}_s)$ are given constants.[1]

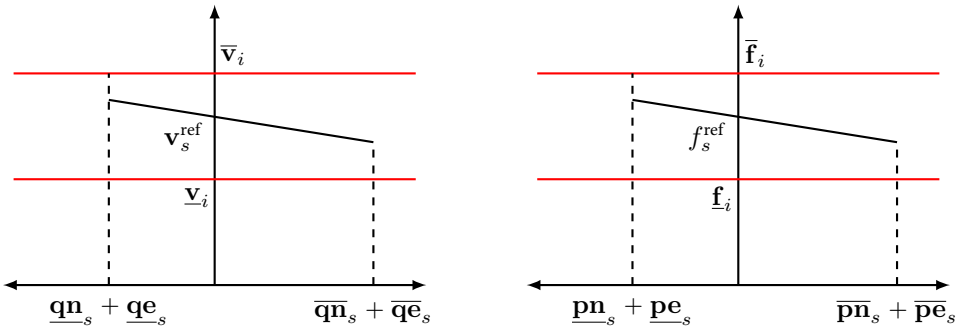
As in [114], we assume that each node has a DG without loss of generality. Then, similar to the loads, we model the dependence of DG connectivity on the nodal voltage and frequency as follows:

$$y_i^\eta \geqslant \underline{\mathbf{vg}}_i - \mathrm{v}_i^\eta, \quad y_i^\eta \geqslant \mathrm{v}_i^\eta - \overline{\mathbf{vg}}_i \quad \forall\ i \in \mathcal{N}, \tag{6.14}$$

$$y_i^\eta \geqslant \underline{\mathbf{fg}}_i - f_i^\eta, \quad y_i^\eta \geqslant f_i^\eta - \overline{\mathbf{fg}}_i \quad \forall\ i \in \mathcal{N}. \tag{6.15}$$

eq. (6.15) implies that a DG will disconnect if the corresponding nodal frequency violates

[1] The secondary control of voltage and frequency regulation could change the reference setpoints of the DERs, namely the voltage, frequency, active and reactive power setpoints [62]. Secondary control may also include changing the droop coefficients of the DERs [117]. However, for the sake of simplicity, we consider primary (but not secondary) control in this paper.



(a) Voltage droop control.

(b) Frequency droop control.

Figure 6-5: Droop control model [83].

safe operating bounds.

The net power consumed at a node i is the power consumed by the load minus the power generated by the DGs and other grid-interactive DERs at that node, i.e.

$$p_i^\eta = pc_i^\eta - pg_i^\eta - \textstyle\sum_{s\in\mathcal{S}_{\text{gi}}|j(s)=i} pr_s^\eta \qquad \forall\, i \in \mathcal{N} \tag{6.16a}$$

$$q_i^\eta = qc_i^\eta - qg_i^\eta - \textstyle\sum_{s\in\mathcal{S}_{\text{gi}}|j(s)=i} qr_s^\eta \qquad \forall\, i \in \mathcal{N}. \tag{6.16b}$$

Finally, we summarize the LinDistFlow and connectivity constraints described in [114] as follows:

$$P_{ij}^\eta = \sum_{k:(j,k)\in\mathcal{E}} P_{jk}^\eta + p_j^\eta \qquad \forall\, (i,j) \in \mathcal{E} \tag{6.17}$$

$$Q_{ij}^\eta = \sum_{k:(j,k)\in\mathcal{E}} Q_{jk}^\eta + q_j^\eta \qquad \forall\, (i,j) \in \mathcal{E} \tag{6.18}$$

$$pg_i^\eta = (1 - y_i^\eta)\,\overline{\mathbf{pg}}_i \qquad \forall\, i \in \mathcal{N} \tag{6.19}$$

$$qg_i^\eta = (1 - y_i^\eta)\,\overline{\mathbf{qg}}_i \qquad \forall\, i \in \mathcal{N} \tag{6.20}$$

$$pc_i^\eta = \beta_i^\eta \overline{\mathbf{pc}}_i, \quad qc_i^\eta = \beta_i^\eta \overline{\mathbf{qc}}_i \qquad \forall\, i \in \mathcal{N} \tag{6.21}$$

$$(1 - kc_i^\eta)\underline{\beta}_i \leqslant \beta_i^\eta \leqslant (1 - kc_i^\eta) \qquad \forall\, i \in \mathcal{N}. \tag{6.22}$$

$$kc_i^\eta \geqslant \underline{\mathbf{vc}}_i - \mathrm{v}_i^\eta, \quad kc_i^\eta \geqslant \mathrm{v}_i^\eta - \overline{\mathbf{vc}}_i \forall\, i \in \mathcal{N} \tag{6.23}$$

This completes the discussion of our multi-regime microgrid network model with parallel operation of DERs.

6.3 Disruption and Operator response models

In [114], we modeled the sequential interaction between the attacker and operator as a bilevel mixed-integer problem (BiMIP). We now extend this model to include microgrid operations and DER dispatch capabilities. Our revised BiMIP formulation considers multi-regime microgrid operations with multiple DERs/DGs. It also accounts for TN-side voltage and frequency disturbances as part of the overall disturbance model.

TN-side disruption

We consider TN-side disturbance in our attack model because the DN can face significant loss if the attacker targets DN during an active TN failure event. In general, a TN-side disturbance (e.g. failure of a transmission line or bulk generator) can impact the system frequency as well as the substation voltage of the DN, and this can influence the attacker's strategy. We model the impact of a TN-side failure as a perturbation in the substation voltage and frequency, denoted $\Delta \mathrm{v}_0$ and Δf_0, respectively. Then, the voltage and frequency at the substation node in the post-contingency stage can be written as follows:

$$\mathrm{v}_0^c = \mathrm{v}^{\mathbf{nom}} - \Delta \mathrm{v}_0. \tag{6.24}$$

$$f_0^c = \mathbf{f}^{\mathbf{nom}} - \Delta f_0. \tag{6.25}$$

DN-side disruption

For the sake of consistency, we consider the same model of DN-side disruption as in [114], i.e. an attacker-induced compromise of the DG management system (DGMS) results in simultaneous disruption of multiple DGs. We model this attack as follows:

$$y_i^c \geqslant d_i \quad \forall \quad i \in \mathcal{N}. \tag{6.26}$$

Let k denote the maximum number of DGs that the attacker can disrupt. Then, the set of all possible attacker strategies, denoted $\mathcal{D}_{\mathrm{k}}^{\mathrm{m}}$, is given by

$$\mathcal{D}_{\mathrm{k}}^{\mathrm{m}} = \{d \in \{0,1\}^{\mathcal{N}} \mid \textstyle\sum_{i \in \mathcal{N}} d_i \leqslant \mathrm{k}\}.$$

Unlike DGs (set $\mathcal{S}_{\text{pq}}^{\text{fixed}}$), the output of grid-interactive DERs (set $\mathcal{S}_{\text{gi}}$) changes depending on the grid conditions. In particular, the DER output either changes autonomously based on the droop control equations, or the DERs are explicitly coordinated by the SA. The DERs are not vulnerable under our assumed disruption model because they are not affected by the compromised DGMS.

Note that the above-mentioned disruption model can be extended to other types of attacks, including disruption of loads or circuit breakers. One can model such attacks as follows:

$$\begin{aligned} kc_i^c &\geqslant dc_i && \forall\, i \in \mathcal{N} \\ kl_{ij}^c &\geqslant dl_{ij} && \forall\, (i,j) \in \mathcal{E}, \end{aligned}$$

where $dc \in \{0,1\}^{\mathcal{N}}$ and $dl \in \{0,1\}^{\mathcal{E}}$ denote the corresponding attacks for loads and DN lines, respectively. Thus, despite its simplicity, our approach to modeling DN-side disruptions can be applied to capture the physical impact of a broad class of security failure scenarios. This class includes Distributed Denial-of-Service (DDoS) attacks on the power grid components that can result in simultaneous failures [49, 120, 144]. Another relevant attack scenario is motivated by the vulnerabilities of Internet connected customer-side devices (e.g. smart inverters, air conditioners, water heaters), also known as Internet-of-Things (IoT) devices [49]. An adversary can hack into these components via a cyberattack, create an IoT botnet, and can access them via the internet. Indeed, recent work in cyber-security of power systems has identified risk of correlated failures (e.g. simultaneous on/off events) induced/caused by IoT botnets [120]. In our disruption model, the impact of such an attack can be straightforwardly modeled by load/DG/line disconnects, leading to a sudden supply-demand disturbance. However, a single point of failure such as a cyberattack on the DGMS is perhaps a more critical threat to DNs with significant penetration of DGs.

Remark 9. Another attack model that is well-studied in the literature considers false-data injection attacks to a (small) subset of sensors in order to inject biases in state estimates, while being undetected by anamoly detectors [54, 59, 81]. Available results include iden-

tification and security of "critical" sensors and attack-resilient state estimation. However, a less commonly studied aspect is that of incorrect control actions that could be implemented as a result of biased state estimation. Based on our previous work [112], one can argue that our disruption model can be tailored to capture the changes in supply/demand of network nodes due to disruption of DGs/loads and/or component disconnect actions that may be induced by successful false-data injection attacks on sensor data used by the control center.

Remark 10. Our disruption model can be extended to the compromise of grid-interactive DERs as well; see, for example, [109] we consider in which DERs in $\mathcal{S}_{\text{pq}}^{\text{var}}$ are compromised by setpoint manipulation.

Operator response model

Recall the response capabilities (a), (b), (c) and (d) from Sec. 6.1. Since our attack model is concerned with compromised DGMS, we rule out response (a) as an operator response. We considered (b) and (c) in [114]; see Figure 6-1. Our underlying assumption is that (c) is not prone to cyberattacks, because distribution utilities are being regulated under NERC CIP standards [94], which provide specific guidelines for secure *reperimeterisation* of the substation cyber infrastructure. We consider the response (d) to be executed by the SA, and thus assume that it is secure.

Also the responses (b) and (c) do not consider grid-interactive DERs or microgrid islanding capabilities. In contrast, (d) utilizes both these capabilities, in addition to load control and preemptive disconnection of components. Particularly, we model the operator response (d) as follows: $u := (kl, kr, pr, qr, \beta, kc, y)$. Then, the set of all response strategies, denoted $\mathcal{U}_{\text{m}}$, can be defined as $\mathcal{U}_{\text{m}} := \{0,1\}^{\mathcal{M}} \times \{0,1\}^{\mathcal{S}_{\text{gf}}} \times (\mathbb{R} \times \mathbb{R})^{\mathcal{S}_{\text{gi}}} \times \mathcal{B} \times \{0,1\}^{\mathcal{N}} \times \{0,1\}^{\mathcal{N}}$. Moreover, given the attacker-induced disruption d, let the set $\mathcal{U}_{\text{m}}(d) := \{u \in \mathcal{U}_{\text{m}} \mid eq.\ (6.26) \text{ holds}\}$ denote the set of feasible response strategies available to the operator after the disruption.

For the sake of simplicity, we consider that in the pre-contingency stage, the DN is in grid-connected regime and all components are connected. That is, there are no microgrid islands ($kl^n = \mathbf{0}$), and all the loads and DGs are connected to the DN ($kc^n = \mathbf{0}$ and $y^n =$

0). Consequently, the grid-forming DERs are not contributing to regulation in the pre-contingency stage o, i.e. $kr_s^n = 0$ for all $s \in \mathcal{S}$. Recall that we also assumed the output of the grid-interactive DERs in mode o to be zero, i.e. $pr_s^n = qr_s^n = 0$ for all $s \in \mathcal{S}_{\text{gi}}$. These are not restrictive assumptions, however, they allow us to straightforwardly compare the effectiveness of each of the response (b), (c) and (d).

Post-contingency costs

The post-contingency loss incurred by the operator, denoted L_{m}, is the sum of the following costs: (i) cost due to loss of voltage regulation, (ii) cost of load control, (iii) cost of load shedding, and (iv) cost of islanding:

$$\begin{aligned} L_{\text{m}} =& \mathrm{W}_{\text{VR}} \left\| \mathrm{v}^{\mathbf{nom}} - \mathrm{v} \right\|_{\infty} + \mathrm{W}_{\text{FR}} \left\| \mathbf{f}^{\mathbf{nom}} - f \right\|_{\infty} \\ &+ \mathrm{W}_{\text{LC}} \textstyle\sum_{i \in \mathcal{N}} \left(\mathbf{1}_N - \beta_i \right) \overline{\mathbf{pc}}_i \\ &+ \left(\mathrm{W}_{\text{LS}} - \mathrm{W}_{\text{LC}} \right) \textstyle\sum_{i \in \mathcal{N}} kc_i \overline{\mathbf{pc}}_i \\ &+ \mathrm{W}_{\text{MG}} \textstyle\sum_{(i,j) \in \mathcal{M}} kl_{ij}, \end{aligned} \tag{6.27}$$

where $\mathrm{W}_{\text{LC}} \in \mathbb{R}_+$ denotes the cost of per unit load controlled, $\mathrm{W}_{\text{LS}} \in \mathbb{R}_+$ and $\mathrm{W}_{\text{LS}} \geqslant \mathrm{W}_{\text{LC}}$ is the cost in dollars of per unit load shed, W_{MG} is the cost of a single islanding control action, $\mathrm{W}_{\text{VR}} \in \mathbb{R}_+$ is the cost of unit absolute deviation of nodal voltage from the nominal value $\mathrm{v}^{\mathbf{nom}} = 1$ pu, and W_{FR} is the cost of unit absolute deviation of nodal frequency from the nominal value $\mathbf{f}^{\mathbf{nom}} = 1$ pu; see Table 6.4 for a comparison of the cost coefficients.

For a given operator response $u \in \mathcal{U}_{\text{m}}$, let $\mathcal{X}_{\text{m}}(u)$ denote the set of post-contingency states x that satisfy the constraints (7.28)-(6.25). Then, we can restate our bilevel formulation (P2) as:

$$\begin{aligned} \mathcal{L}_{\text{MG}} \;\coloneqq\; & \max_{d \in \mathcal{D}_{\text{k}}^{\text{m}}} \; \min_{u \in \mathcal{U}_{\text{m}}(d)} \; L_{\text{m}}(u, \mathrm{x}^c) \\ & \text{s.t. } \mathrm{x}^c \in \mathcal{X}_{\text{m}}(u). \end{aligned} \tag{P-MG}$$

Since (P-MG) is a BiMIP with the same mathematical structure as the BiMIP in [114], we solve it using the Benders Decomposition algorithm that we developed in [114].

Computational study

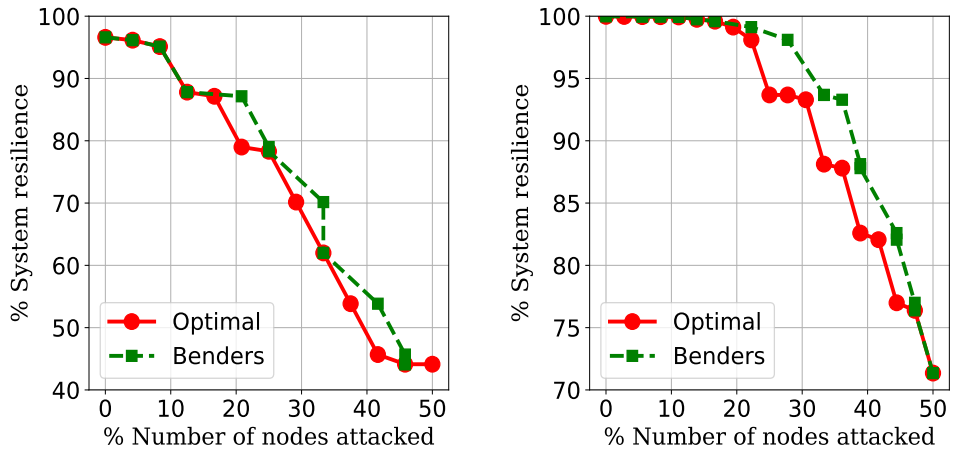
Now, we present computational results to: (i) compare the output value of our BD algorithm with the optimal value (generated for small networks by simple enumeration); (ii) compare the DN resilience under response capabilities (b), (c) and (d); and (iii) show the scalability of our approach to realistically large DN network sizes $N \in \{24, 36, 118\}$.

Setup for computational study

We consider three networks: modified IEEE 24-, 36-, and 118- node networks; see Figure 6-10. The set of connecting lines $\mathcal{M}$ are shown with thick edges. The individual microgrid networks $\mathcal{N}_1, \cdots, \mathcal{N}_{|\mathcal{M}|}$ can be obtained by setting $kl_{ij} = 1 \; \forall \; (i,j) \in \mathcal{M}$. Each line $(i,j) \in \mathcal{E}$ has an identical impedance of $\mathbf{r}_{ij} = 0.01, \mathbf{x}_{ij} = 0.02$. Half of the nodes have a DG each and half have a load each. Consider a parameter $\alpha = \frac{6}{N}$. Before the contingency, each DG has active power output of $\overline{\mathbf{pg}}_i = \alpha$, and each load has a demand of $\overline{\mathbf{pc}}_i = 1.25\alpha$. The voltage bounds are $\underline{\mathbf{vc}}_i = 0.9$, $\overline{\mathbf{vc}}_i = 1.1$, $\underline{\mathbf{vg}}_i = 0.92$ and $\overline{\mathbf{vg}}_i = 1.08$. The reactive power values are chosen to be exactly one third that of the corresponding active power value, i.e. a 0.95 lagging power factor for each load and DG. The values are chosen such that the total net active power demand in the DN is 0.75 pu, and the lowest voltage in the network before any contingency is close to $\underline{\mathbf{vg}}$. The maximum load control parameter is $\underline{\beta}_i = 0.8$, i.e. at most 20% of each load demand can be curtailed. For the sake of simplicity, we assume that all DGs and loads are homogeneous. $\mathrm{W}_{\mathrm{LC}} = \frac{100}{\overline{\mathbf{pc}}_i}, \mathrm{W}_{\mathrm{VR}} = 100, \mathrm{W}_{\mathrm{FR}} = 100, \mathrm{W}_{\mathrm{LS}} = \frac{1000}{\overline{\mathbf{pc}}_i}, \mathrm{W}_{\mathrm{MG}} = 400$. Each microgrid has one utility-owned and one facility level grid-forming DERs. Consider a parameter $\gamma = \frac{\sum_{i \in \mathcal{N}} \overline{\mathbf{pc}}_i}{8|\mathcal{M}|}$. Then, each facility level DER has the following parameters: $\forall \; s \in \mathcal{S}_{\mathrm{gf}}^{\mathrm{facility}}, \overline{\mathbf{sn}}_s = \overline{\mathbf{se}}_s = \gamma$, $\mathbf{mp}_s = 0.02$, $\mathbf{mq}_s = 0.04$; and, each utility-owned DER has the following parameters: $\forall \; s \in \mathcal{S}_{\mathrm{gf}}^{\mathrm{utility}}$, $\overline{\mathbf{sn}}_s = \overline{\mathbf{se}}_s = 2\gamma$, $\mathbf{mp}_s = 0.1$, $\mathbf{mq}_s = 0.2$. These parameters are chosen such that the total capacity of grid-noninteractive DGs is 80% of the total demand, whereas the total capacity of all grid-interactive DERs is 75% of the total demand of all loads. However, the total capacity of grid-interactive DERs may not be fully available to meet the demand because the microgrids are typically not of exact uniform size and topology, and the storage devices supply power only under the specific islanding configurations.

Benders Decomposition vs. Simple Enumeration

We evaluate the ability of our implementation of the BD algorithm to compute optimal attacks in the islanding regime for small ($N \in \{24, 36\}$) networks. For each possible cardinality of attack we first compute the optimal attack with maximum loss using simple enumeration. Then we fix the maximum loss as $\mathcal{L}_{\text{target}}$ for BD algorithm. If the BD algorithm can find an attack with the same cardinality, then indeed the BD algorithm has computed the optimal attack. Otherwise, it has computed a suboptimal attack.



(a) $N = 24$ (b) $N = 36$

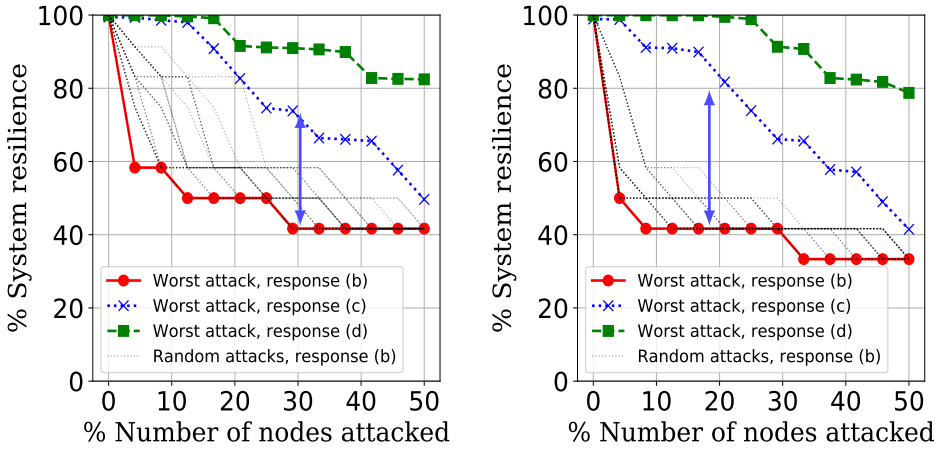
Figure 6-6: System resilience ($\mathcal{R} = 100\,(1 - \mathcal{L}/\mathcal{L}_{\max})$) vs. k. Near-optimal performance of BD algorithm.

The results of the BD algorithm implemented for solving (P-MG) are shown in Figure 6-6. Naturally, the attack cardinality computed by BD algorithm is greater than or equal to the optimal min-cardinality computed using simple enumeration. In some cases, however, the BD algorithm does not obtain the optimal attack. The BD algorithm involves iteratively eliminating sub-optimal attacks using Benders cuts [114]. Each cut involved an ϵ which results in a tradeoff between the accuracy and computational time. For a very small choice of ϵ, the BD algorithm eliminates exactly one sub-optimal attack in each iteration, and performs as worse as simple enumeration. For a large value of ϵ, relatively more attacks, including optimal attacks are eliminated. Hence, the BD algorithm terminates faster although at some loss of optimality. Still, for both 24- and 36- node networks, the BD algorithm computes attacks whose cardinalities are at most 8-23% more than the

cardinalities of the corresponding optimal attacks.

Value of timely response

In [114], we used post-contingency loss to define the metric of resilience for autonomous disconnections ($\mathcal{R}_{\text{AD}}$) and operator response without microgrid capabilities ($\mathcal{R}_{\text{Mm}}$). In Sec. 6.1, we introduced an analogously defined metric of resilience for operator response involving microgrid islanding and DER dispatch capabilities ($\mathcal{R}_{\text{MG}}$). Figure 6-7 compares the resiliency values for the three cases for varying attack cardinalities, where computation of $\mathcal{R}_{\text{MG}}$ and $\mathcal{R}_{\text{Mm}}$ involves using the BD algorithm to solve the corresponding BiMIPs, and $\mathcal{R}_{\text{AD}}$ is computed using Algorithm "Uncontrolled cascade under autonomous disconnections (response (b))" in [114]. Indeed, under response (d), the SA triggers microgrid islanding and DER dispatch in a preemptive manner to reduce the impact of the attack. This leads to a smaller loss in comparison to using just load control and/or component disconnects (that is, response (c)). Indeed, our computational results validate that $\mathcal{R}_{\text{MG}} \geqslant \mathcal{R}_{\text{Mm}} \geqslant \mathcal{R}_{\text{AD}}$. The difference between the dashed (green) and solid (red) curves in Figure 6-7 indicate the value of response (d) relative to response (b). The difference between the dashed (green) and cross-marked (blue) curves indicate the relative value of timely response (d) over response (c).



(a) $\Delta v_0 = 0$ (b) $\Delta v_0 = 0.02$

Figure 6-7: DN resilience under varying attacker-operator interaction scenarios. (The blue double-sided arrows indicate the value of timely microgrid response relative to the autonomous disconnections case.)

Scalability of the BD algorithm

We tabulate the performance of the BD algorithm in terms of its computational time and number of iterations to compute min-cardinality attacks for different network sizes and varying values of the resilience metric $\mathcal{R}_{\text{target}} = 100\,(1 - \mathcal{L}_{\text{target}}/\mathcal{L}_{\max})$; see Table 6.3. We also note the cardinalities of attacks output by the BD algorithm as well as the corresponding DN resilience. Note that the $N = 118$ node network has 2^{118} possible configuration vectors. Still, with $\mathcal{R}_{\text{target}} = 80\%$, the BD algorithm computes an attack in ≈ 1 minute. In comparison, for the $N = 36$ node network, the simple enumeration method took ≈ 6 hours.

Table 6.3: Resiliency metric evaluated using the BD algorithm for 24-, 36- and 118-node networks. The realized resilience metric can significantly fall short of the target resilience metric ($\mathcal{R}_{\text{target}} = 100\left(1 - \frac{\mathcal{L}_{\text{target}}}{\mathcal{L}_{\max}}\right)$); for example, when the attack cardinality changes from 6 to 7, the percentage resilience for the 24-node network decreases sharply from 98.91% to 91.33%. This means that the 24-node DN is at least 90% (actual value 91.33%) resilient to k = 7 cardinality attacks.

Entries are resilience metric of DN (in percentage), number of iterations (written in brackets), time (in seconds), attack cardinality.			
$\mathcal{R}_{\text{target}}$	$N = 24$	$N = 36$	$N = 118$
99	98.91, (15), 0.41, 6	98.95, (10), 0.37, 5	98.95, (8), 2.48, 4
95	91.33, (16), 0.46, 7	94.12, (12), 0.51, 7	94.28, (15), 3.91, 11
90	82.8, (18), 0.57, 9	88.23, (17), 0.91, 11	89.73, (20), 10.62, 16
85	82.8, (18), 0.57, 9	81.9, (20), 1.23, 14	83.49, (29), 28.79, 25
80	78.73, (21), 0.74, 12	71.46, (21), 1.75, 15	79.9, (40), 67.38, 36

6.4 Multi-period network restoration

We recall that the resilience of a system is related to its ability to not only minimize the impact of a disturbance, but also quickly recover from it; see Figure 6-1. Our attack model assumes that a compromise of the DGMS leads to remote disconnection of multiple DGs. However, the actual functionality of disconnected DGs is not compromised. In response (d), we consider that the SA has the ability to detect and obtain knowledge of the complete attack. Moreover, the SA can also control DG connectivity. We now discuss how the SA can restore the disrupted DGs, and bring the DN back to its nominal performance. In this section, we present a simple MIP that models the process of restoring system performance.

Our model of the DN restoration process entails progressively reconnecting the disrupted DGs, and eventually restoration to the grid-connected mode of DN operation. We consider a multi-period horizon $\mathcal{T} := \{0, 1, \cdots, \mathrm{M}\}$, where M is the maximum of two periods: one plus the time period when all disrupted DGs can be reconnected, and the time period when the TN-disturbance clears. Let a period be denoted by $m \in \mathcal{T}$, where each period m is of fixed time duration (say, a few minutes). Furthermore, the operator response at period m is denoted by u^m. Then, under the assumed detection and response capabilities of the SA, $m = 0$ coincides with the time of initial post-contingency response, i.e. $u^0 = u^c$. Period $m = \mathrm{M}$ denotes the time at which the system performance of the DN is fully restored.

We consider two types of constraints to model the restoration actions of the operator across time periods: monotonicity constraints and resource constraints. Consider a period $m \in \{1, 2, \cdots, \mathrm{M}\}$. The monotonicity constraints for period m are as follows.

$$kl_{ij}^m \leqslant kl_{ij}^{m-1} \quad \forall\, (i,j) \in \mathcal{M}, \tag{6.28a}$$

$$y_i^m \leqslant y_i^{m-1} \quad \forall\, i \in \mathcal{N}. \tag{6.28b}$$

eq. (7.19) implies that during the restoration process, once a connecting line is closed, it remains closed until the restoration process is completed. Similarly, (6.28b) implies that a disconnected DG becomes operational after being reconnected, and then remains operational until the restoration is complete. The monotonicity constraints can be justified based on the practical consideration that frequently changing the status of connecting lines can create large fluctuations in nodal voltages and frequencies of the microgrids due to the low inertia of DERs. Moreover, the battery life of storage devices would reduce due to frequent changes from charging modes (quadrants III and IV) to discharging modes (quadrants I and II), and vice versa; see Figure 6-4.

The resource constraint merely limits the number of DG reconnections. Specifically, we consider that during period m, at most G^m DGs can be reconnected, where G^m denotes

the restoration budget for that period:

$$\sum_{i\in\mathcal{S}_{\text{pq}}^{\text{fixed}}} y_i^m \geqslant \sum_{i\in\mathcal{S}_{\text{pq}}^{\text{fixed}}} y_i^{m-1} - \mathrm{G}^m. \tag{6.29}$$

Restrictions on the number of connecting line closing operations can be similarly considered. eq. (6.29) can also be justified in a way similar to that of monotonicity constraints. Naturally, the operator wants to avoid a large number of simultaneous DG reconnections as that could lead to large voltage and frequency fluctuations.

As stated before, we choose M large enough so that all disrupted DGs can be reconnected before the last period M, i.e. $\mathrm{M} \geqslant \min\{m' | \sum_{m=1}^{m'} \mathrm{G}^m \geqslant \mathrm{k}\} + 1$. Indeed, the TN-disturbance may clear any time, before or after the DG reconnections. However, since our analysis is focussed on determining worst-case resilience of the DN, we assume that the TN-side disturbance clears after the disrupted DGs are fully reconnected. In particular, we assume that the TN-side disturbance ceases to exist at the last time period. We model this as follows:

$$\mathrm{v}_0^m = \begin{cases} \mathrm{v}^{\mathbf{nom}} - \Delta\mathrm{v}_0 & \text{if } m \neq \mathrm{M} \\ \mathrm{v}^{\mathbf{nom}} & \text{if } m = \mathrm{M} \end{cases} \tag{6.30a}$$

$$f_0^m = \begin{cases} \mathbf{f}^{\mathbf{nom}} - \Delta f_0 & \text{if } m \neq \mathrm{M} \\ \mathbf{f}^{\mathbf{nom}} & \text{if } m = \mathrm{M}. \end{cases} \tag{6.30b}$$

Let $\mathcal{Y}_{\text{m}}^m(u^{m-1})$ denote the feasible set of response strategies for u^m, i.e. $\mathcal{Y}_{\text{m}}^m(u^{m-1}) = \{u^m \in \mathcal{U}_{\text{m}} \mid \text{such that (6.28) – (6.29) hold}\}$. Also, given an operator response $u \in \mathcal{U}_{\text{m}}$, let $\mathcal{X}_{\text{m}}^m(u)$ denote the set of network states x^m which satisfy the constraints (7.28)-(6.14) and (6.30). Hence, the restoration problem can be posed as follows:

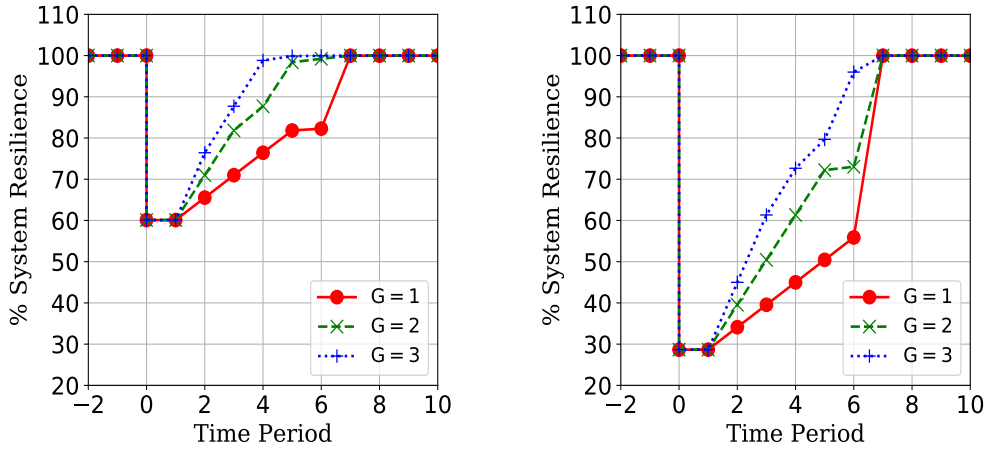
$$
\begin{aligned}
\mathcal{L}_{\text{res}}(d) := \min_{\{u^m\}_{m\in\mathcal{T}}} \quad & \sum_{m\in\mathcal{T}} L_{\text{m}}\left(u^m, \text{x}^m\right) \\
\text{s.t.} \quad & u^0 \in \mathcal{U}_{\text{m}}(d) \\
& u^m \in \mathcal{Y}^m_{\text{m}}(u^{m-1}) \quad \forall\, m = 1, \cdots, \text{M} \\
& \text{x}^m \in \mathcal{X}^m_{\text{m}}(u^m) \quad \forall\, m = 0, \cdots, \text{M}
\end{aligned}
\tag{P3}
$$

Problem (P3) is a Mixed-Integer Problem (MIP), and can be solved using off-the-shelf MIP solvers. However, due to the large number of binary variables, it can become computational expensive to solve for larger networks. In fact, we solve (P3) using a simple greedy algorithm; see Algorithm 10. In each period, the operator simply chooses that response which minimizes the post-contingency loss during that time period subject to the monotonicity and resource constraints. Algorithm 10 is based on the feature that the network state in any period depends only on the operator actions in that period, and the network state in the previous period. The algorithm returns with the operator actions, resulting network state, and corresponding post-contingency loss for each time period.

Algorithm 10 Greedy Algorithm

1: $u^0, \text{x}^0 \leftarrow \underset{u\in\mathcal{U}_{\text{m}}(d)}{\text{argmin}} \quad L_{\text{m}}(u, \text{x}) \quad \text{s.t.} \quad \text{x} \in \mathcal{X}(u).$
2: **for** $m = 1, \cdots, \text{M}$ **do**
3: $\quad u^m, \text{x}^m \leftarrow \underset{u\in\mathcal{Y}^m_{\text{m}}(u^{m-1})}{\text{argmin}} \quad L_{\text{m}}(u, \text{x}) \quad \text{s.t.} \quad \text{x} \in \mathcal{X}^m_{\text{m}}(u).$
4: $\quad L^m \leftarrow L_{\text{m}}(u^m, \text{x}^m)$
5: **end for**
6: **return** $\{u^m, \text{x}^m, L^m\}_{m\in\mathcal{T}}$

Figure 6-8 shows the system performance during the restoration of the DN over multiple time periods for different resource constraints. For each system restoration curve, we chose G^m to be a constant for all time periods $m \in \mathcal{T}$. One can see that after the TN-side and DN-side disturbances, the system performance drops. Then, as disrupted components are connected, the system performance gradually recovers. Also, the post-contingency losses are higher for larger TN-side disturbances. However, as the restoration budget increases, the system recovers faster.



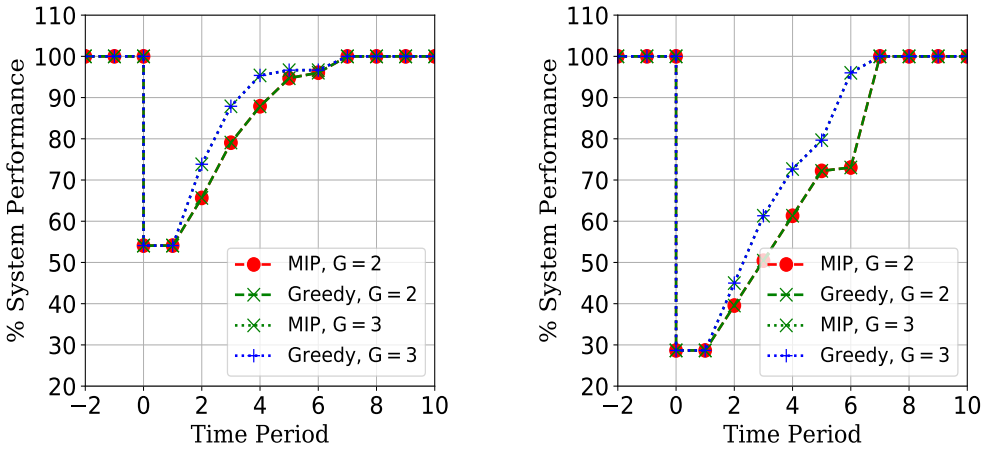
(a) $\Delta v_0 = 0.1$. (b) $\Delta v_0 = 0.2$.

Figure 6-8: Multi-period DN restoration ($N = 36$).

MIP vs. Greedy Recovery Algorithm

Figure 6-9 shows the comparison of the system performance recovery curves obtained using Algorithm 10 and by directly solving the large-scale MIP for $N = 24$ and $N = 36$ node networks. The TN-side voltage disturbance for both the networks is set to $\Delta v_0 = 0.2$. In this experiment, we set the time limit of the (Gurobi) solver to 7200 seconds. While solving the large-scale MIP for $N = 36$ and $G = 3$ we were able to achieve an optimality gap of 16.54% after 2 hours. However, the Algorithm 10 was able to attain the same system performance recovery curve using the default solver settings (no presolve and Simplex method), and compute the near-optimal solution in approximately 10 seconds.

In order to implement the response computed in (P3), the SA may need to coordinate with the individual microgrid controllers. A detailed description of such a communication architecture is beyond the scope of this paper. We refer the reader to [60] for a hierarchical control architecture which can support the coordination between SA and individual microgrid controllers.

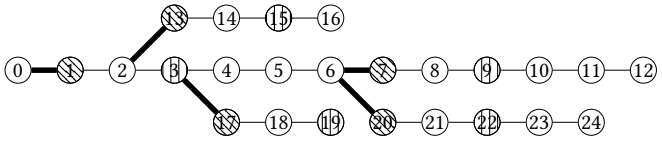


(a) $N = 24$. (b) $N = 36$.

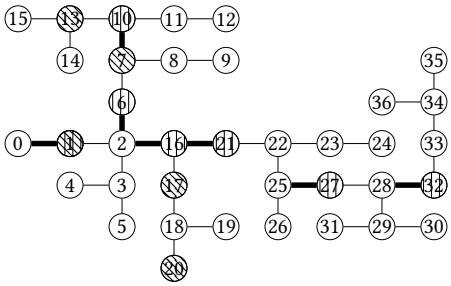
Figure 6-9: Near-optimal performance of Greedy Algorithm 10.

Weights	Typical values
W_{LC}	$\frac{1}{4}\times$ 11 cents
W_{VR}	$\frac{2}{100}\times$ 11 cents
W_{FR}	$\frac{2}{100}\times$ 11 cents
W_{LS}	3 dollars
W_{MG}	1 dollar

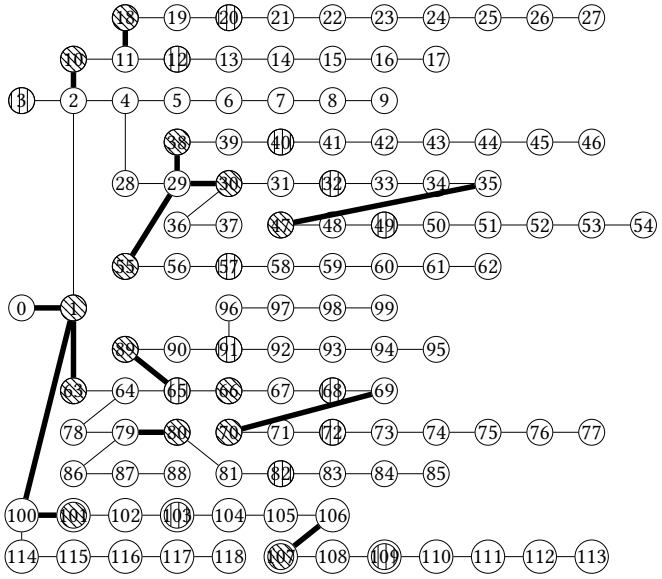
Table 6.4: Typical values of cost parameters.



(a) 24 node network.



(b) 36 node network.



(c) 118 node network.

Figure 6-10: Modified IEEE test networks. Connecting lines are indicated by thick edges. Utility-owned (resp. facility level) grid-forming DERs are indicated by northwest (resp. vertical) lines.

Chapter 7

Resource Allocation and Restoration for Storm-induced failures

Weather-related outages in electricity distribution networks (DNs) continue to show an upward trend as utilities face the dual problems of deteriorating power grid infrastructure and higher frequency of natural disasters (such as hurricanes [31, 79]). Prolonged delays in restoring the power system of Puerto Rico in the aftermath of Hurricane Maria highlight the importance of strategic planning and efficient response to such events. This chapter is motivated by the need for developing a modeling framework that (i) accounts for estimated locations of component failures in assessing the extent of damage in the DN; and (ii) enables the design of pre-storm resource allocation strategies as well as post-storm repair operations. To address this issue, we formulate a two-stage stochastic optimization problem based on an uncertainty model of storm-induced failures.

7.1 Two-stage stochastic optimization formulation

Our uncertainty model utilizes predictions of storm tracks and surface wind velocities over a spatial region during the expected duration of the storm (see [139] for a related approach). Hours or days in advance of a storm, the track forecasts can be obtained by public sources such as the National Hurricane Center (NHC). For each forecasted storm track, the surface wind velocity field can be estimated using well-known parametric models [68]. We focus on wind-induced damage (as opposed to flooding-induced failures), as strong winds

during a storm are reported to be one of the primary factors for failures of above ground DN components, such as the failures resulting from falling of trees/vegetation on power lines and poles [76]. The failure probabilities of DN components are then estimated using a non-homogeneous Poisson process (NHPP) model, which parametrically depends on the estimated location-specific wind velocities [149]-[7]. Then, these failure probabilities are used as an input to the two-stage stochastic formulation.

A significant aspect of our formulation is that we allow for the partial DN operation in situations when bulk supply (from the transmission side) is no longer available and microgrids can be operationalized during the recovery and repair period. Indeed, extensive literature is available on the allocation of repair crew and optimal response operations [11, 126, 132, 137]. These contributions primarily focus on resource limitations, failure uncertainties, and physical constraints. However, the problem of proactive allocation of temporary generators in the pre-storm stage has received limited attention in the literature. This opportunity becomes especially relevant given the technological progress in portable Distributed Energy Resources (DERs) and microgrid technologies [39]. The significance of proactive DER allocation in the face of natural disasters has already been acknowledged by federal agencies [65, 129]. Our formulation allows for strategic placement of DERs at a subset of DN nodes in the pre-storm stage, given the uncertainty in component failures and the resulting lost load for a particular storm. These DERs can be used to sustain microgrids in the post-storm stage and to dispatch power to critical loads [15], while the line repair operations are being completed and the connection to bulk supply is being restored.

More specifically, our two-stage stochastic mixed-integer problem considers the DER placement decisions in Stage I (pre-storm), and a multi-period repair problem with DER dispatch within each microgrid in Stage II (post-storm). The objective is to minimize the sum of the cost incurred in DER allocation and the expected cost of unmet demand during the time period of repair and recovery operations. For a given DER allocation (placement) and for a realization of DN component disruptions, Stage II is a deterministic multi-period problem in which line repair schedules and dispatch within each microgrid are jointly determined. From a practical viewpoint, each period can be viewed as one work shift

of the repair crews. In the 0^{th} period, the subnetworks formed as a result of disruptions start to operate as microgrids using the available DER supply. In the subsequent time periods, damaged lines are repaired, permitting connections between smaller microgrids to progressively form larger microgrids. In the last time period, the DN is connected back to the main grid, and normal operation is restored. Crucially, the Stage II problem relies on an estimate of the total number of time periods needed for full recovery. It also utilizes a novel model of linear power flow within a microgrid island with parallel operation of multiple DER inverters. Figure 7-1 summarizes the order of events and decisions in our formulation.

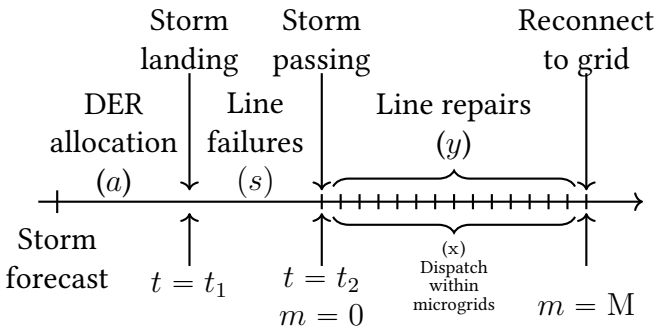


Figure 7-1: Timeline of events and decision stages. The DER placement decision (a) is made before the storm hits the network ($t = t_1$). Uncertainty s is realized over the course of the storm. After passing of the storm ($t = t_2$, $m = 0$), optimal power flow and line repair decisions (x, y) are made. At $m = \mathrm{M}$ (end of repair time horizon), the network is fully restored.

Our formulation considers a tree DN with nodes and distribution lines $\mathcal{G} = (\mathcal{N} \bigcup \{0\}, \mathcal{E})$, where $\mathcal{N}$ denotes the set of all DN nodes. The substation node is labeled as 0, and it also forms the connection to the bulk supply through a transmission network. The set $\mathcal{E}$ denotes the set of directed edges, such that the edges are directed away from the substation node. The first-stage problem is as follows [4]:

$$\min_{a \in \mathcal{A}} \left\{ g\left(a\right) \coloneqq {\mathrm{W}_{\text{alloc}}}^{T} a + \mathbb{E}_{S \sim \mathcal{P}} J\left(a, S\right) \right\}, \tag{7.1}$$

where a denotes a resource allocation strategy to be chosen from the set of feasible strategies $\mathcal{A}$. The uncertainty in the random vector S characterizes the random failures of distribution lines and has a probability distribution $\mathcal{P}$ defined over the set of possible line

failure scenarios $\mathcal{S} := \{0,1\}^{\mathcal{E}}$. In (7.1), $\mathrm{W}_{\text{alloc}}$ is a length-$|\mathcal{N}|$ vector of the allocation cost per unit resource at the nodes, ${\mathrm{W}_{\text{alloc}}}^T a$ is the cost of resource allocation and $\mathbb{E}_{S\sim\mathcal{P}} J(a,S)$ is the expected cost of unmet demand under allocation scheme a.

To model the post-storm multi-period dispatch with repair scheduling, we consider an a priori fixed time horizon with M periods. Let $\mathcal{M} := \{0,1,\cdots,\mathrm{M}\}$ denote the set of all periods. We denote a period by m. For a specific realization of line failures $s \in \mathcal{S}$, $J(a,s)$ denotes the optimal value of the second-stage problem which is given as follows:

$$\begin{aligned} J(a,s) := \min_{\mathrm{x}^s, y^s} \quad & \textstyle\sum_{m=0}^{\mathrm{M}} {\mathrm{W}_{\text{dem}}}^T \mathrm{x}^{m,s} \\ \text{s.t.} \quad & y^s \in \mathcal{Y}(s), \quad \mathrm{x}^s \in \mathcal{X}(a,s,y), \end{aligned} \tag{7.2}$$

where the scenario-specific second-stage decision variables $\mathrm{x}^s = \{\mathrm{x}^{m,s}\}_{m\in\mathcal{M}}$ and $y^s = \{y^{m,s}\}_{m\in\mathcal{M}}$ respectively denote the collection of dispatch and line repair actions for each period. For a failure scenario $s \in \mathcal{S}$, $\mathcal{Y}(s)$ denotes the set of feasible repair schedules, and $\mathcal{X}(a,s,y)$ denotes the set of feasible power flows under the DER allocation a, and chosen line repair schedule $y \in \mathcal{Y}(s)$. Calculating $\mathbb{E}_{S\sim\mathcal{P}} J((x,y),S)$ is computationally intractable for large networks because the number of all possible scenarios grows exponentially ($2^{|\mathcal{E}|}$) for a network with $|\mathcal{E}|$ number of edges. Using the sample average approximation (SAA) method [4], one can obtain an approximate solution to the stochastic optimization problem. This solution can be obtained by solving the following problem:

$$\min_{a\in\mathcal{A}} \left\{ \hat{g}_{\widehat{\mathcal{S}}}(a) := {\mathrm{W}_{\text{alloc}}}^T a + \frac{1}{K} \textstyle\sum_{s\in\widehat{\mathcal{S}}} J(a,s) \right\}, \tag{7.3}$$

where $\widehat{\mathcal{S}} \subset \mathcal{S}$ is a suitably chosen (preferably small) subset of the set of failure scenarios, $K := |\widehat{\mathcal{S}}|$, and $\hat{g}_{\widehat{\mathcal{S}}}(a)$ is the SAA objective value obtained using K samples drawn from the distribution $\mathcal{P}$. The set of constraints for the problem will be discussed in Sec. 7.3.

The outline of this chapter is as follows. In Sec. 7.2, we describe the storm wind field prediction and NHPP failure model. In Sections 7.3 and 7.4, we describe the DER placement model, repair scheduling model, DER dispatch model, and *LinDistFlow* model for islanded microgrids. Then, we describe our computational results on a 12-node network,

and end the chapter with description of future extensions to our work.

7.2 Stochastic failure model

Recall that, in general, the probability distribution $\mathcal{P}$ governing the random vector of line failures S can be supported over $\{0,1\}^{\mathcal{E}}$. For $S = s$, $s_e = 1$ if line e has failed, and 0 otherwise. To capture the physical impact of the storm wind field on DN components, we adopt an approach that characterizes $\mathcal{P}$ by combining: (i) wind velocity prediction model given forecast of the storm track, and (ii) a Non-Homogeneous Poisson Process (NHPP) model for prediction of line failure rates.

First, the two-dimensional area of the power network is broken into grids indexed by h, which form the set $\mathcal{H}$. For example, the area of each grid h is chosen to be roughly 1km$\times$1km. Next, we estimate the wind velocity and Poisson failure rate within each grid every hour while the storm is passing over the network. In our setup, Poisson rates are given per unit time (hr) and line length (km). The failure probabilities of distribution lines, which are roughly of length 1km in our study and can pass through multiple grids, are a function of the Poisson rates.

Poisson distribution has been used to model power line failure rates under normal (non-storm) conditions. However, previous studies [7, 149] simulate the total number of line failures within a region while assuming a spatially-constant velocity in the region at every time step. Since the failure probabilities differ significantly across larger networks, we instead model the failure probability of each line with a Bernoulli random variable.

In our approach, the prediction of velocity measurements $v_{h,t}$ in each grid h and time $t \in [t_1, t_2]$ is based on the storm center location at time t and three wind field parameters: maximum intensity V_t, radius of maximum winds R_t, and shape parameter B_t. The predicted velocities can be obtained from the classical Holland model which expresses velocity $v_{h,t}$ as a function of distance $r_{h,t}$ from the storm center [68]:

$$v_{h,t} = V_t \left(\frac{R_t}{r_{h,t}}\right)^{B_t/2} \exp\left(1 - \left(\frac{R_t}{r_{h,t}}\right)^{B_t}\right)^{1/2}. \tag{7.4}$$

Then, an estimate of location and time-dependent Poisson failure rates $\lambda_{h,t}$ can be ob-

tained using a quadratic NHPP model [7, 76, 149]:

$$\lambda_{h,t} = \begin{cases} \left(1 + \alpha\left(\left(\frac{v_{h,t}}{v_{crit}}\right)^2 - 1\right)\right)\lambda_{norm}, & \text{if } v_{h,t} \geqslant v_{crit} \\ \lambda_{norm}, & \text{if } v_{h,t} < v_{crit}. \end{cases} \tag{7.5}$$

In the above model, the failure rate is λ_{norm} if $v_{h,t}$ is below a critical velocity v_{crit} and increases quadratically with respect to wind speed above v_{crit}. Specifically, we use the parameters $\alpha = 4175.6$, $v_{crit} = 40$ knots, and $\lambda_{norm} = 0.49$ failures/yr/mi, which are obtained from a previous study [76] and converted to appropriate units. We select these parameters because they were estimated using historical storm data that includes Category 1-3 hurricanes.

The failure rate is given at hourly intervals and measured per hour. Hence, the cumulative intensity function Λ_h per km at grid h from storm arrival (${t_1}^{th}$ hour) over the network to its departure (${t_2}^{th}$ hour) can be approximately calculated by summing the rate over the time interval:

$$\Lambda_h(t_2 - t_1) = \textstyle\sum_{t=t_1}^{t_2} \lambda_{h,t}. \tag{7.6}$$

Recall that a line may span multiple grids. Let $l_{e,h}$ denote the length of edge e in grid h. Then, the cumulative intensity function for line e can be computed as:

$$\nu_e(t_2 - t_1) = \textstyle\sum_{h \in \mathcal{H}} l_{e,h} \Lambda_h(t_2 - t_1). \tag{7.7}$$

Then, the probability of line e failing during the storm is

$$F_e(t_2 - t_1) = 1 - e^{-\nu_e(t_2 - t_1)}. \tag{7.8}$$

Finally, the probability of a failure scenario s is given by:

$$\mathbf{Pr}(s) = \textstyle\prod_{e \in \mathcal{E}} \left(s_e F_e(t_2 - t_1) + (1 - s_e)(1 - F_e(t_2 - t_1))\right) \tag{7.9}$$

which characterizes the failure probability distribution $\mathcal{P}$.

Recall that since the SAA method relies on solving the two-stage problem for a subset of scenarios $\widehat{\mathcal{S}}$, selecting this subset is an important aspect [48]. To obtain $\widehat{\mathcal{S}}$, we begin by generating 1,000 realizations s of the random vector S and sort s in decreasing order of

their probabilities $\mathbf{Pr}(s)$. Then, we randomly choose a small subset $\widehat{\mathcal{S}}$ ($\leqslant 10$ number of scenarios) from the 100 most probable of these scenarios. This procedure gives a small set of scenarios, which is representative of the worst-case failures in the DN. The question of how well this sample represents the distribution $\mathcal{P}$ is outside the scope of this paper. Nevertheless, we use the set $\widehat{\mathcal{S}}$ as an input to the problem (7.3), the variables and constraints of which are described in the next section.

A distribution line $e \in \mathcal{E}$ connects a node, say node j, to its parent node, say node i, in the tree network. Here i and j are the from and to nodes of line e, which are denoted by e^- and e^+, respectively. Each distribution line $e \in \mathcal{E}$ has a complex impedance $\mathbf{z}_e = \mathbf{r}_e + \mathbf{j}\mathbf{x}_e$ where $\mathbf{r}_e > 0$ and $\mathbf{x}_e > 0$ denote the resistance and inductance of the line e, respectively, and $\mathbf{j} = \sqrt{-1}$. Also, let $N := |\mathcal{N}|$.

7.3 Allocation of Distributed Energy Resources

Let $\mathcal{S}$ denote the set of available, not necessarily homogeneous DERs. In order for a DER to be deployed at a DN node, an appropriate temporary DER site needs to first be developed at that node. Development may include land acquisition or security provisions to protect DERs from natural hazards and ensure continued fuel supply for DERs such as diesel storage or natural gas pipelines [50, 129]. Let $\mathcal{U} \subseteq \mathcal{N}$ denote the subset of nodes where such DER sites may be developed. Let $u \in \{0,1\}^{\mathcal{U}}$ be a vector, where $u_i = 1$ denotes that a DER site is developed at node i; otherwise $u_i = 0$. Let $\mathrm{W}^{\mathrm{SD}} \in \mathbb{R}^{\mathcal{U}}_{+}$ be a cost vector such that $\mathrm{W}^{\mathrm{SD}}_i$ denotes the cost of developing a DER site at node $i \in \mathcal{U}$.

Let $yg \in \{0,1\}^{\mathcal{U}\times\mathcal{S}}$ denote a map of DER allocation to DER sites, such that $yg_{is} = 1$ denotes that a DER s is allocated at site i. A site $i \in \mathcal{U}$ is operational if and only if there is at least one DER allocated to that site, i.e.

$$u_i \leqslant \textstyle\sum_{s\in\mathcal{S}} yg_{is} \qquad \forall\, i \in \mathcal{U} \tag{7.10a}$$

$$yg_{is} \leqslant u_i \qquad \forall\, s \in \mathcal{S}, i \in \mathcal{U}. \tag{7.10b}$$

Since there are at most $|\mathcal{S}|$ DERs, Equation (7.10b) can be rewritten with fewer constraints as $\sum_{s\in\mathcal{S}} yg_{is} \leqslant u_i\,|\mathcal{S}|\ \ \forall\, i \in \mathcal{U}$.

Clearly, a DER s can be allocated to at most one site, i.e.

$$\sum_{i\in\mathcal{U}} yg_{is} \leqslant 1 \qquad \forall\, s \in \mathcal{S}. \tag{7.11}$$

Let G denote the maximum number of DERs that can be allocated in a DN. Then

$$\sum_{i\in\mathcal{U}} \sum_{s\in\mathcal{S}} yg_{is} \leqslant \mathrm{G}. \tag{7.12}$$

Thus, the first stage decision variable in eq. (7.3) can be defined as $a := (u, yg)$, and the set of feasible resource allocation strategies can be defined as $\mathcal{A} := \{(u, yg) \in \mathcal{U} \times \mathcal{S} \mid (7.10) - (7.12) \text{ hold}\}$.

7.4 Joint multi-period repair and dispatch problem

Multi-period repair scheduling model

We assume that at period $m = 0$, the uncertainty of line failures due to the hurricane is completely realized, and the pre-placed DERs are dispatched to supply power. From period $m = 1$, the utility crew starts repairing the damaged lines subject to resource constraints. We choose M large enough to allow all necessary line repairs in the DN to complete. Furthermore, we assume that the transmission network will take more time to repair than the DN. Since, the DN performance will not change after the DN repair until the main grid is connected back, we can constrain that at period $m = \mathrm{M}$, the DN is connected back to the bulk power grid (see Figure 7-1).

Consider a scenario $s \in \widehat{\mathcal{S}}$ denoting the locations of line failures. For each such scenario s, for $m \in \mathcal{M}$, let $yl \in \{0,1\}^{\mathcal{E}_s \times \mathcal{M}}$ denote the decision variables concerning repair of failed lines, where $yl_e^{m,s} = 1$ for $(e, m) \in \mathcal{E}_s \times \mathcal{M}$ denotes that line e is repaired during the time interval $(m-1, m]$.

Since the repair crew may take some time to reach the failed lines immediately after the hurricane, there are no lines repaired in the first period, i.e.

$$yl_e^{m,s} = 0 \quad \forall\, e \in \mathcal{E}_s, m = 0. \tag{7.13}$$

A line can at most be repaired once, i.e.

$$\sum_{m=0}^{\mathrm{M}} yl_e^{m,s} \leqslant 1 \quad \forall\, e \in \mathcal{E}_s. \tag{7.14}$$

Furthermore, at most Y number of lines can be repaired during any time period, i.e.

$$\sum_{e \in \mathcal{E}_s} yl_e^{m,s} \leqslant \mathrm{Y} \qquad \forall\, m \in \mathcal{M} \tag{7.15}$$

Y models the resource constraints with respect to the crew or repair equipment.[1]

Finally, we constrain that the DN is connected to the main grid at period $m = \mathrm{M}$, i.e.

$$yl_e^{m,s} = 1, \quad m = \mathrm{M}, e \in \mathcal{E}, e^- = 0. \tag{7.16}$$

Since the DN is typically connected to the main grid only after complete DN repair, imposing the restriction (7.16) as part of worst-case analysis is a reasonable assumption.

Thus, the repair schedule variable for each scenario s in eq. (7.2) can be defined as $y^s := \{yl_e^{m,s}\}_{e \in \mathcal{E}_s, m \in \mathcal{M}}$, and the set of feasible repair schedules $\mathcal{Y}(s) := \{yl |$ (7.13) – (7.16) holds$\}$.

For the fixed scenario s, let $kl_e^{m,s} \in \{0, 1\}$ denote whether the line $e \in \mathcal{E}$ is operational at time $m \in \mathcal{M}$. $kl_e^{m,s} = 1$ denotes that the line e is not operational at period m.

As a result of failures of lines in $\mathcal{E}_s$, the state of the lines at period $m = 0$ is as follows:

$$kl_e^{m,s} = 1, \qquad m = 0, \forall\, e \in \mathcal{E}_s \tag{7.17}$$

Since the main grid is also likely to be damaged by the hurricane, we assume that the line connecting the DN to the substation is rendered disconnected, i.e. for $e \in \mathcal{E}$ such that $e^- = 0$, $kl_e^0 = 1$, or equivalently $e \in \mathcal{E}_s$. The lines not damaged by the hurricane remain operational during all periods, i.e.

$$kl_e^{m,s} = 0 \quad \forall\, m \in \mathcal{M}, e \notin \mathcal{E}_s \tag{7.18}$$

[1] It is indeed possible that the maximum number of repairable lines may vary across periods. For the sake of simplicity , we chose a fixed Y.

A failed line becomes operational after it is repaired, and then continues to remain operational, i.e.

$$kl_e^{m,s} = kl_e^{m-1,s} - yl_e^{m,s} \quad \forall\, m \in \mathcal{M} \backslash 0, e \in \mathcal{E}_s \tag{7.19}$$

Since, for all m, the variables $kl_e^{m,s}$ and $yl_e^{m,s}$ can only take binary values, (7.19) automatically ensures that a failed line can at most be repaired once, i.e. $\forall\, e \in \mathcal{E}_s,\ \sum_{m=0}^{\mathrm{M}} yl_e^{m,s} \leqslant 1$.

Multi-period dispatch model

Henceforth, in the subsequent equations, we will drop the $\forall\, m \in \mathcal{M}, s \in \widehat{\mathcal{S}}$, for brevity.

DER model

Depending upon whether a DER s is allocated at a site $i \in \mathcal{U}$, its contribution to the power generated at node i at any timestep t is constrained as follows, i.e.

$$\begin{aligned} 0 \leqslant \quad pg_{is}^{m,s} \quad &\leqslant (1 - yg_{is})\, \overline{\mathbf{pg}}_s \quad \forall\, i \in \mathcal{N}, s \in \mathcal{S} \\ |qg_{is}^{m,s}| \quad &\leqslant \overline{\eta} pg_{is}^{m,s} \qquad\quad \forall\, i \in \mathcal{N}, s \in \mathcal{S} \end{aligned} \tag{7.20}$$

where $\overline{\eta}$ denotes the $\tan\arccos$ of maximum power factor.[2] If a DER is not allocated to a node, its active and reactive power contribution to the node is zero, i.e.

$$pg_{is}^{m,s} = qg_{is}^{m,s} = 0, \quad \forall\, i \notin \mathcal{U}, s \in \mathcal{S}. \tag{7.21}$$

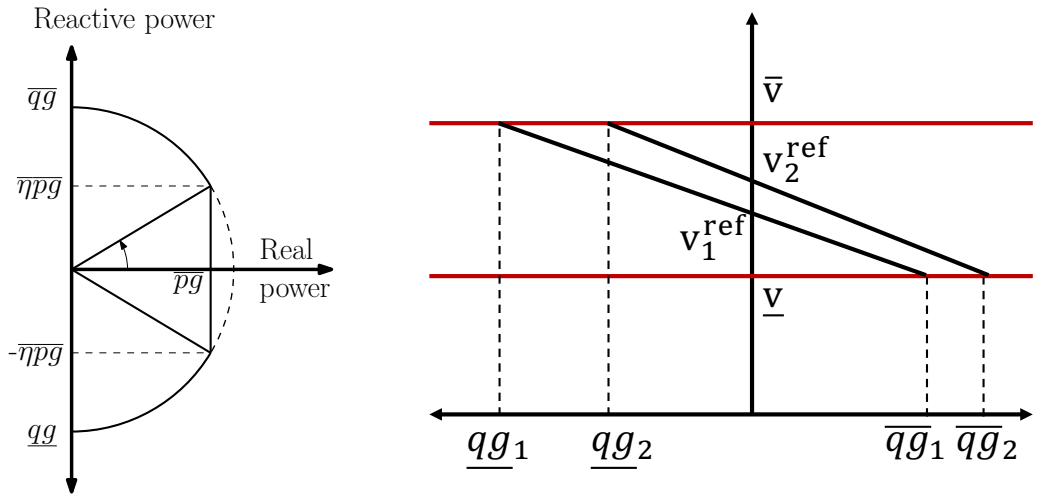
In a microgrid island, a DER can adjust its reactive power output depending upon the voltage of the node to which it allocated, according to a voltage droop control equation expressed as follows:

$$\begin{aligned} \left|\mathrm{v}_i^{m,s} - \left(\mathrm{v}_s^{\mathrm{ref}} - \mathbf{mq}_s qg_{is}^{m,s}\right)\right| &\leqslant (1 - yg_{is})\, \mathrm{L}, \\ \forall\, i \in \mathcal{U}, s \in \mathcal{S}, m \neq \mathrm{M} \end{aligned} \tag{7.22}$$

where $\mathbf{mq}_s$ denotes the voltage droop coefficient of the DER s; $\mathrm{v}_s^{\mathrm{ref}}$ denotes the idle (no load) terminal voltage reference setpoint of the DER (see Figure 7-2 [26]); and L is a large

[2] Typical value for $\overline{\eta} \approx \frac{1}{3}$ corresponds to a power factor value of 0.95.

constant.[3] If $yg_{is} = 1$, (7.22) simplifies to $qg_{is}^{m,s} = \frac{1}{\mathbf{mq}_s}\left(\mathrm{v}_s^{\mathrm{ref}} - \mathrm{v}_i^{m,s}\right)$, which models the standard droop control law that determines the reactive power contribution of DER at node i to help voltage regulation of the islanded microgrid. Such a DER is said to be operating in the voltage source inverter (VSI) control mode [83]. When the DN is connected to the main grid, the "stiff" AC system of the bulk power grid essentially determines the terminal voltage of the DER. Hence, the voltage droop equation does not apply at period $m = \mathrm{M}$. Note that, in our model, any DER within an island is capable of operating in the VSI control mode, thereby contributing to the voltage regulation of the microgrid island, in parallel operation with other DERs in the same island. Similar equations for frequency droop control can also be included [27].



(a) DER output model [130]

(b) Voltage droop control [83]

Figure 7-2: DER model as a voltage source inverter.

Without loss of generality, we assume every node has a load. We consider only the constant power model for loads.

Load model

Let $\overline{\mathbf{pc}}_i + \mathbf{j}\overline{\mathbf{qc}}_i$ denote the nominal power demand at node i. Let $kc_i^{m,s} \in \{0, 1\}$ denote the load connectivity where $kc_i^{m,s} = 1$ denotes the load at node i is disconnected at time

[3] This modeling trick to use a constraint of the type $|b| \leqslant k\mathrm{L}$ where $k \in \{0, 1\}$ enforces an equality constraint $b = 0$ only when $k = 0$; otherwise the equality constraint is not binding. We repeatedly use this trick to model various other conditional equalities.

period m. When connected, a load's actual consumption can be scaled down to a fraction of its nominal demand. We model such a flexibility by introducing a load control parameter $\beta_i^{m,s} \in [\underline{\beta}_i, 1]$ (when $kc_i^{m,s} = 0$, otherwise $\beta_i = 0$), where $\underline{\beta}_i \in [0, 1]$ denotes the minimum fraction of the load's nominal demand that should be satisfied provided the load is connected, i.e.

$$\begin{aligned} pc_i^{m,s} &= \beta_i^{m,s}\, \overline{\mathbf{pc}}_i \quad \forall\, i \in \mathcal{N} \\ qc_i^{m,s} &= \beta_i^{m,s}\, \overline{\mathbf{qc}}_i \quad \forall\, i \in \mathcal{N}, \end{aligned} \tag{7.23}$$

where

$$(1 - kc_i^{m,s})\, \underline{\beta}_i \leqslant \beta_i^{m,s} \leqslant (1 - kc_i^{m,s}) \qquad \forall\, i \in \mathcal{N}. \tag{7.24}$$

The connectivity of a load depends on whether the nodal voltage lies within safe operating bounds, i.e.

$$\begin{aligned} kc_i^{m,s} &\geqslant \underline{\mathbf{vc}}_i - \mathrm{v}_i^{m,s} \qquad \forall\, i \in \mathcal{N} \\ kc_i^{m,s} &\geqslant \mathrm{v}_i^{m,s} - \overline{\mathbf{vc}}_i \qquad \forall\, i \in \mathcal{N}, \end{aligned} \tag{7.25}$$

where $\underline{\mathbf{vc}}_i$ and $\overline{\mathbf{vc}}_i$ denote the lower and upper voltage bounds for the loads at node i.

The net actual real and reactive power consumed (denoted by $p_i^{m,s}$ and $q_i^{m,s}$, respectively) at node i is given by:

$$\begin{aligned} p_i^{m,s} &= pc_i^{m,s} - \textstyle\sum_{s \in \mathcal{S}} pg_{is}^{m,s} \qquad \forall\, i \in \mathcal{N} \\ q_i^{m,s} &= qc_i^{m,s} - \textstyle\sum_{s \in \mathcal{S}} qg_{is}^{m,s} \qquad \forall\, i \in \mathcal{N}. \end{aligned} \tag{7.26}$$

Linear Power Flow model for microgrids

We adopt the *LinDistFlow* model [16] to develop a novel linear power flow model over microgrids for a computational advantage.

$$\begin{aligned} P_e^{m,s} &= \sum_{l : l^- = e^+} P_l^{m,s} + p_j^{m,s}, \quad \forall\, e \in \mathcal{E}, j = e^+ \\ Q_e^{m,s} &= \sum_{l : l^- = e^+} Q_l^{m,s} + q_j^{m,s}, \quad \forall\, e \in \mathcal{E}, j = e^+ \end{aligned} \tag{7.27}$$

eq. (7.27) denotes the standard power conservation equations for real and reactive power flows of the *LinDistFlow* model.

Since the failed lines are not operational, there are no power flows on these lines, until they are repaired, i.e.

$$\begin{aligned} |P_e^{m,s}| &\leqslant (1 - kl_e^{m,s})\,\mathrm{L} \qquad \forall\, e \in \mathcal{E} \\ |Q_e^{m,s}| &\leqslant (1 - kl_e^{m,s})\,\mathrm{L} \qquad \forall\, e \in \mathcal{E}. \end{aligned} \tag{7.28}$$

Similarly, the voltage drop equation of the *LinDistFlow* model along a line e will be enforced only if line e is operational, i.e.

$$\begin{aligned} \left|\mathrm{v}_j^{m,s} - (\mathrm{v}_i^{m,s} - 2\,(\mathbf{r}_e P_e^{m,s} + \mathbf{x}_e Q_e^{m,s}))\right| &\leqslant \mathrm{L} kl_e^{m,s} \\ \forall\, e \in \mathcal{E}, i = e^-, j = e^+ \end{aligned} \tag{7.29}$$

Note that, if a line e is operational (i.e. $kl_e^{m,s} = 0$), then eq. (7.29) simplifies to $\mathrm{v}_j^{m,s} = \mathrm{v}_i^{m,s} - 2\,(\mathbf{r}_e P_e^{m,s} + \mathbf{x}_e Q_e^{m,s})$, which is the standard voltage drop equation of the *LinDistFlow* model [16].

When the DN is connected back to the TN, the substation voltage is assumed to be the nominal voltage, i.e. for $m = \mathrm{M}, \mathrm{v}_0^{m,s} = \mathrm{v}^{\mathbf{nom}}$.

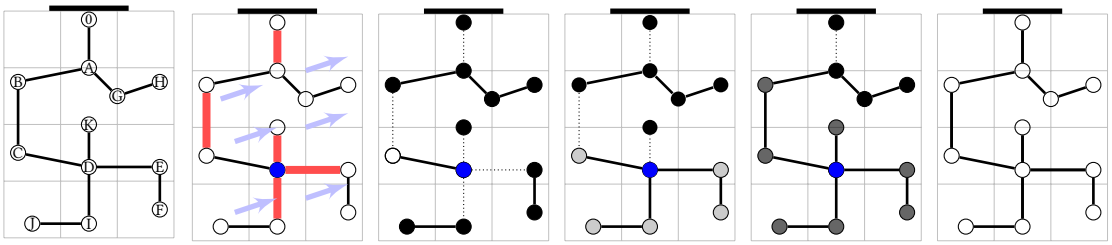
Then, we define the dispatch variable for a fixed scenario $s \in \mathcal{S}$ in eq. (7.2) as $\mathrm{x}^s := \{pg^{m,s}, qg^{m,s}, \beta^{m,s}, kc^{m,s}, p^{m,s}, q^{m,s}, P^{m,s}, Q^{m,s}, \mathrm{v}^{m,s}\}_{m \in \mathcal{M}}$, and the set of feasible dispatch decisions as $\mathcal{X}(a, s, y) := \{\mathrm{x} \mid (7.17) - (7.29) \text{ hold}\}$. Thus, the SAA problem (7.3) can be more specifically written as:

$$\begin{aligned} \min_{a,\mathrm{x},y} \; & \sum_{i \in \mathcal{U}} \mathrm{W}_i^{\mathrm{SD}} u_i + \frac{1}{K} \sum_{m=0}^{\mathrm{M}} \sum_{i \in \mathcal{N}} [\mathrm{W}_i^{\mathrm{LC}} (1 - \beta_i^{m,s}) + \mathrm{W}_i^{\mathrm{LS}} kc_i^{m,s}] \\ \text{s.t.} \; & a = (u, yg), y^s \in \mathcal{Y}(s), \mathrm{x}^s \in \mathcal{X}(a, s, y) \;\; \forall\, s \in \widehat{\mathcal{S}}. \end{aligned} \tag{7.30}$$

where $\mathrm{W}_i^{\mathrm{LC}}$ is the cost of complete load control at node i; $\mathrm{W}_i^{\mathrm{LS}}$ is the cost of complete load shedding at node i; $\mathrm{x} := \{\mathrm{x}^s\}_{s \in \widehat{\mathcal{S}}}$ and $y := \{y^s\}_{s \in \widehat{\mathcal{S}}}$. Note that the entries in $\mathrm{W}_{\text{alloc}}$ are non-zero only for site development ($\mathrm{W}_i^{\mathrm{LS}}$), i.e. the cost of allocating DERs to a site is zero. This assumption maybe justified by considering that building a site immune to flooding,

electrical fires or other storm-induced damage, and with uninterrupted fuel supply will be more expensive than transportation and installation of DERs at the site.

Illustrative example



(a) (b) (c) $m = 0$ (d) $m = 1$ (e) $m = 2$ (f) $m = \mathrm{M}$

Figure 7-3: The subfigures show (a) nominal DN (white nodes indicate no load control), (b) pre-storm DER allocation based on storm forecast (blue node denotes DER allocation, red lines illustrate a disruption scenario), (c) microgrid islands (dotted lines indicate failed lines that are not repaired, black nodes denote the shed loads), (d) partial line repairs enable partial load restoration (light gray nodes), (e) line repairs completed leading to more load restoration, although with further load control (dark gray nodes), and finally (f) reconnection to main grid and restoration of nominal performance.

Figure 7-3 provides an illustration of various aspects of our problem formulation. In Figure 7-3a, the DN is in nominal operating conditions, i.e. each node is connected to the grid and no load control is exercised.

Based on the storm characteristics determined from the track and wind-field forecasts, we obtain line failure probabilities, and generate failure scenarios. Suppose that the utility has resources to develop only one DER site in Stage I, and now has to decide its location. Further suppose that due to the powerflow and voltage drop constraints ((7.27) and (7.29)), transmitting power over across two lines result in voltage bound violations. Hence, from any site location, the DERs will be able to meet the demand of nodes which are at most two hops away from the site. For example, a DER placed at node H can only supply power to nodes A, G, and H. Note that the nodes A, B, G, H form the largest connected island; hence, placing a site at node A, can immediately serve demand at 4 nodes. However, the maximum number of nodes that can be brought back online (considering line repairs) is eight if the site is developed at node D. Hence, allocating the DER to node D is optimal in this scenario, although only two loads will be served during the first period.

In Figure 7-3c, we see that a failure scenario has realized where the set of failed lines $\mathcal{E}_s$ include lines (B,C), (D,E), (D,F), (D,I). The loss of bulk power supply is represented by DN's disconnection from the substation, i.e. (0,A) $\in \mathcal{E}_s$. Consider that the demand at nodes C and D is relatively small; thus, it is completely met (i.e. $kc_i^{m,s} = 0, \beta_i^{m,s} = 0$ for $i \in$ {C,D}, $m = 0$, and $kc_i^{m,s} = 1, \forall\, i \in \mathcal{N}\backslash$\{C,D\}).

Now, the line repairs are to be scheduled. Suppose that $\mathrm{Y} = 2$, i.e. at most two lines can be repaired in each period. Again, looking at the most number of nodes that can be energized, the lines (D,E) and (D,I) should be repaired in the first period, and then lines (D,F) and (B,C) should be repaired in the next period; i.e. $yl_e^{m,s} = 1$ if $m = 1$ and $e \in$ {(D,E), (D,I)} or $m = 2$ and $e \in$ {(D,F), (B,C)}. Following this schedule, in the period $m = 1$, nodes E, F, I, J are connected. However, due to DER limitations, load control is exercised; see Figure 7-3d (i.e. $kc_i^{m,s} = 0$ and $\beta_i^{m,s} < 1$ for $i \in$ {C,D,E,F,I,J}). In Figure 7-3e, due to further line repairs, the loads at nodes B, C and K are energized, although by exercising even more load control ($\beta_i^{m,s} > \beta_i^{m-1,s}$ for $m = 2$ and $i \in$ {C,D,E,F,I,J}). However, due to power flow constraints, the nodes A, G, and H cannot be energized until complete network is restored.

Finally, when the transmission network is repaired, reconnecting the DN back to the substation ($yl_e^{m,s} = 1$ for $e =$(0,A) and $m = \mathrm{M}$) restores the nominal operation of the DN; see Figure 7-3f.

Computational Study

Experimental setup

We use a 12-node test feeder in our computational experiments. 6 randomly chosen nodes have one load each. The loads are homogeneous. For each node i with a load, $\mathrm{W}_i^{\mathrm{LS}} = 1000$, $\mathrm{W}_i^{\mathrm{LC}} = 100$, $\underline{\beta}_i = 0.5$. The total capacity of available DERs is chosen to be 80% of the total demand in the network.

To produce predictions of the storm wind field $v_{h,t}$ using (7.4), we consider two different tracks of a Category 1 storm to account for expected uncertainty in the storm trajectory. The storm tracks we used (hereafter referred to as Track 1 and Track 2) differ

Table 7.1: Mean, minimum, and maximum failure probabilities of distribution lines (*left side*) and median, minimum, and maximum island size (*right side*) for the case studies.

	Failure probability			Size of islands		
	Mean	Min	Max	Med.	Min	Max
Track 1	0.63	0.56	0.75	1.58	1.08	4.20
Track 2	0.26	0.21	0.34	3.22	2.11	5.61

primarily in that the storm eye wall (region of maximum winds) is farther away from the 12-node feeder for Track 2, and thus the wind velocities in the DN are lower as compared to the case with Track 1. We use synthetic values for the Holland parameters (V_t, R_t, B_t) to produce predictions of the storm wind field $v_{h,t}$ using (7.4). We compute predictions for wind velocity fields and line failure probabilities at every hour over the course of one day, using the procedure described in Sec. 7.2.

We implemented the SAA solution approach for the mixed integer program (MIP) optimization model (7.3) in JuliaPro. Solutions are obtained using the Gurobi solver, which employs a branch-and-bound algorithm with heuristics to solve MIPs.

Impact of storm characteristics on DN failures

We generate a total of $S = 1000$ failure scenarios to examine distributions in frequency of failures and number/size of islands. The quadratic relationship between $\lambda_{h,t}$ and $v_{h,t}$ results in a significant increase in probability of failures and decrease in island size if the test feeder is subject to higher storm velocities (see Table 7.1). An average of 5.96 failures occur per scenario in Case 1, while only 2.88 failures occur per scenario in Case 2 (see Figure 7-4a). The smaller median island size under Track 1 corresponds with a larger number of islands (see Figure 7-4b). In contrast, under normal conditions or mild storms with the tropical storm (TS) rating, Poisson intensities are uniformly λ_{norm}, and the failure probability F_e over $[t_1, t_2]$ is < 0.001. Category 2-5 storms have a larger radial region of high winds, and we can expect much higher failure probabilities in such cases.

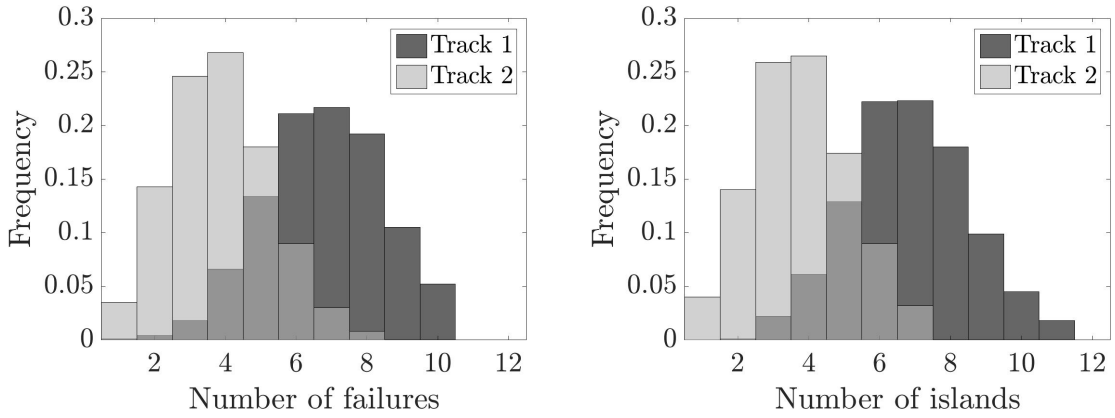


Figure 7-4: Frequency of number of distribution line failures (*left*) and number of islands formed (*right*) in the 12-node network for the two tracks. A total of 1,000 failure scenarios are simulated to produce the histograms.

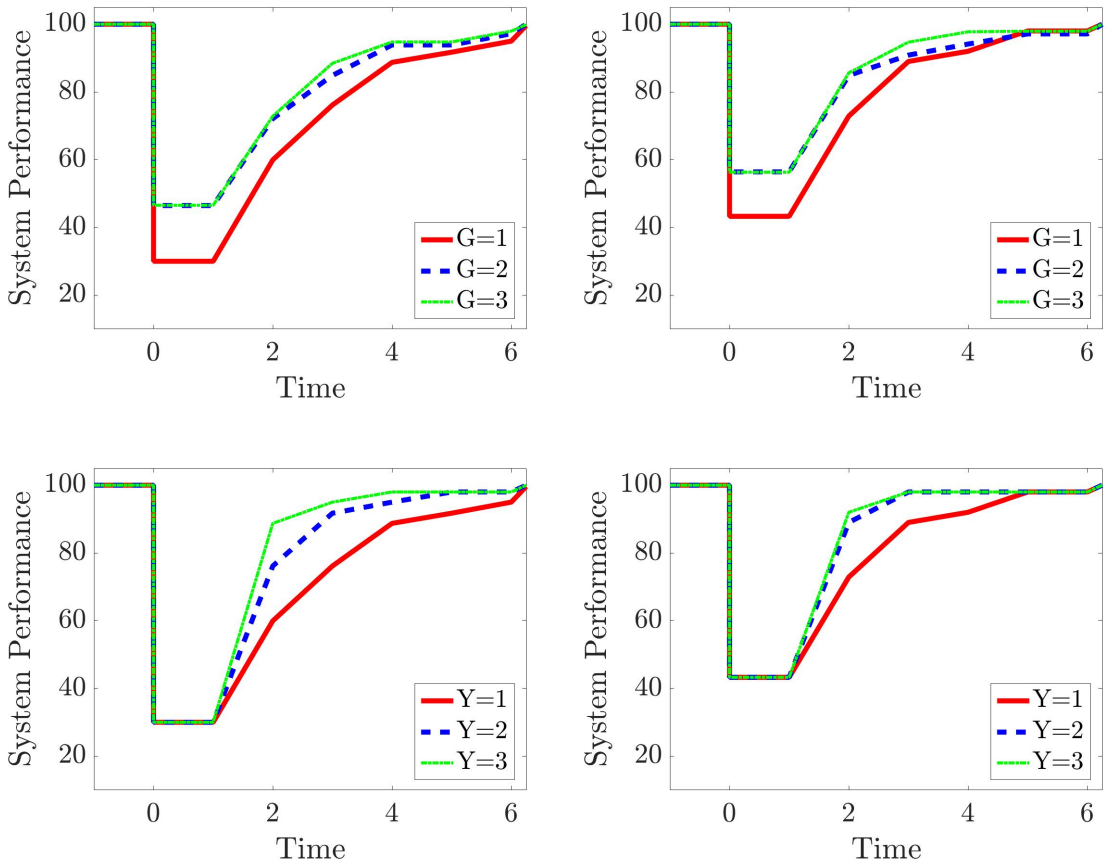
Impact of resource constraints on DN recovery

To evaluate the system performance under different resource constraints, we vary G (number of available DERs) and Y (maximum number of lines repaired in each period). System performance at a period m is defined as the average percentage difference between the cost of unmet demand and the total cost of complete load shedding, averaged over the sampled scenarios, i.e.

$$\text{System performance} = \frac{1}{|\widehat{\mathcal{S}}|} \sum_{s \in \widehat{\mathcal{S}}} 100 \left(1 - \frac{J(a,s)}{\sum_{i \in \mathcal{N}} \mathrm{W}_i^{\mathrm{LS}}} \right). \tag{7.31}$$

The system performance as a function of m for different values of G and Y for two storm tracks is shown in Figure 7-5. Immediately following the storm ($m = 0$), the system performance drops to a minimum, and then improves with each subsequent set of line repairs. Once all the damaged lines are repaired and prior to reconnection of the bulk supply, the system performance is almost (but, not fully) restored. The system performance is fully restored to 100% following the reconnection to the main grid. Since there are more failures on average in the DN under Track 1, the system performance at $m = 1$ is lower than for Track 2.

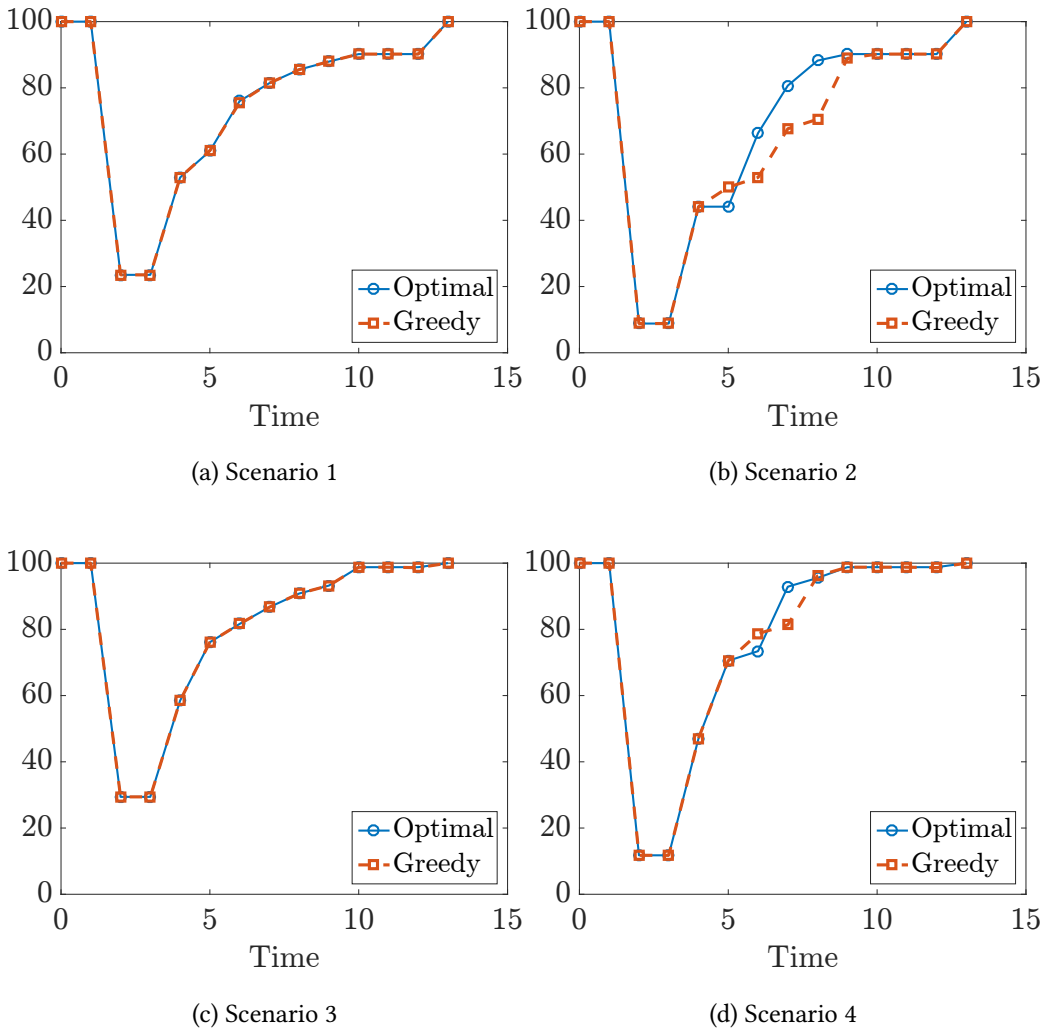
If $\mathrm{G} > 0$, even networks with very high failure probabilities will be able to meet a



(a) Track 1 (b) Track 2

Figure 7-5: Average system performance of the DN under the two track scenarios, varying G while setting $\mathrm{Y} = 1$ (*top row*) and varying Y while setting $\mathrm{G} = 1$ (*bottom row*).

portion of demand given a nonzero DER budget – the network repair time will simply be longer. Increasing G noticeably decreases the average time required to repair the network (return to system performance that is close to 100%) under both track scenarios. Similarly, increasing Y speeds up the system restoration process.



(a) Scenario 1

(b) Scenario 2

(c) Scenario 3

(d) Scenario 4

Figure 7-6: Performance of greedy algorithm for Stage 2.

As noted before, the Stage 2 problem is an MILP for a specific scenario. This MILP consists of a number of binary variables which scales with the square of the number of edges, which does adversely affect the computational time requirements. Since the greedy algorithm was successful in the case of security failures, we tried a greedy algorithm for line repairs. The number of binary variables in the MILP at each stage scales only linearly

with the number of edges. As a result, the number of nodes visited by branch-n-bound algorithm reduces significantly. The results shown in Figure 7-6 compare the performance of the greedy restoration algorithm with the optimal restoration schedule obtained by solving the large-scale MILP. As we can see, the greedy algorithm performs very well in many scenarios. The question of why greedy algorithm performs well is part of our ongoing research work.

7.5 Connections to job scheduling problem

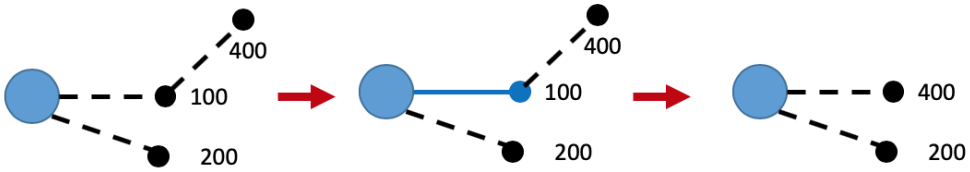
In this section, we argue that the restoration problem in the Stage 2 (7.3) is closely related to a jobs scheduling problem. To this end, we borrow ideas from [29, 99, 126], and present some conceptually interesting ideas which can be developed further. This is part of our ongoing research.

Consider an example as shown in Figure 7-7 to visualize the process of network restoration. In Figure 7-7a, the blue circle denotes an energized core of a DN and the dashed lines indicate the failed lines which need to be repaired. The numbers indicate the "values" of the loads connected to the nodes. The repair times of the lines are assumed to be identical. Assume that load control cannot be exercised. Repair of a line will result in the loads at the corresponding node to become energized, i.e. power supply to the loads will become available. As a result, load shedding worth of the value corresponding to the node will no longer be required.

The operator faces a constraint that only one line can be repaired at a time. Clearly, in this case the line connected to the node with value 200 will be repaired before the line connected the node with value 100. A repair schedule is an ordered sequence of lines which need to be repaired in a sequential manner. Thus, the repair schedule $\{200, 100\}$ results in lower post-contingency loss than the schedule $\{100, 200\}$.

Now, consider another example as shown in Figure 7-7b which consists of an additional node of value 400 connected to the node with value 100. In this case, note that a repair schedule $\{200, 100, 400\}$ would result in post-contingency loss of $200 \times 1 + 100 \times 2 + 400 \times 3 = 1600$. However, the repair schedule $\{100, 400, 200\}$ would result in post-contingency loss of $100 \times 1 + 400 \times 2 + 200 \times 3 = 1500$. No other repair schedule results

(a) Example 1



(b) Example 2

Figure 7-7: Visualizing network restoration.

in a post-contingency loss lower than 1500. Therefore, in the optimal repair schedule the line connected to load 100 should be repaired first because it allows an early power supply restoration to the node with value 400. Then, the node with value 100 becomes part of the energized core as the corresponding loads does not contribute to the cost of load shedding. As a result, the network reduces to an example similar to that in Figure 7-7a with different values (400 and 200). This naturally motivates a recursive algorithm for network restoration which we formalize subsequently in Algorithm 11.

Before describing a recursive algorithm, we discuss how to determine the values of the nodes. Our approach is as follows. Assume that the DN is fully repaired but the bulk power supply from the TN is not restored. Assume that if a load, say i, is energized, then maximum load control parameter will be exercised, i.e. $\beta_i = \underline{\beta}_i$. Determine the optimal subset of loads to which power from the allocated DERs can be supplied subject to constraints of linear power flows, maximum load control, operating bounds of the loads and the DERs, and DER capacities. This can be achieved by solving a simple mixed-integer linear program (MILP). This part of the problem can be solved for well in advance of the storm landing, thereby enabling to not consider the loads which cannot be connected after complete DN restoration (barring the line connecting to the TN).

Next, is a rather simple step, in which we consider a network simplification as illustrated in Figure 7-8. In this step, each connected subnetwork whose lines are not disrupted

by the storm is considered as a single node whose value is the sum of values of the nodes within the subnetwork. As a result, the reduced graph only consists of lines which need to be repaired. This idea has been reported previously in [126].

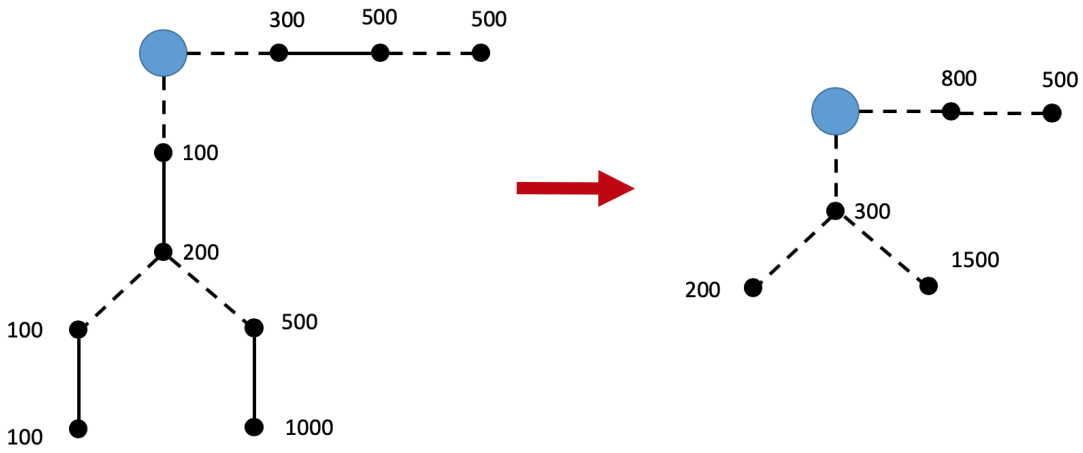


Figure 7-8: Illustration of recursive algorithm.

The second part of the problem concerns with determining optimal restoration schedule. By following the standard terminology in scheduling theory, our problem can be reduced to $Pm|s-prec, p_i = 1|\sum_j w_j C_j$. Here Pm represents m repair crew teams with identical capabilities, $p_i = 1$ indicates unit execution time for each job, and $\sum_j w_j C_j$ is the objective which is to be minimized. In this case, the objective is to minimize the sum of weighted completion time of line repairs. We refer the reader to [29] for the details on this notation. The problem $Pm|s-prec, p_i = 1|\sum_j w_j C_j$ is simpler than the $Pm|s-prec|\sum_j w_j C_j$ problem which is proven to be a NP-hard problem in [126]. However, as shown in [99], the complexity of scheduling problems can drastically change with subtle changes in the constraints. However, $Pm|s-prec, p_i = 1|\sum_j w_j C_j$ is an open scheduling problem in the literature.

In this section, we assume that all DERs are allocated at a single node or that all DERs are allocated to a subnetwork whose lines are not vulnerable to the storm-induced disruptions. This allows us to assume a single energized core before the network restoration process begins. Now, we present a recursive algorithm for restoration when only one line can be repaired in each time period, and describe it using an illustrative example shown in Figure 7-9. In Algorithm 11, OptimalLineRepairSchedule is a recursive pro-

Algorithm 11 Recursive algorithm for optimal line repair schedule with one line.

OptimalLineRepairSchedule($\mathcal{G}$)
procedure OptimalLineRepairSchedule($\mathcal{G}'$)
    if $\mathcal{G}'$ consists of exactly one line e **then**
        return $\{e\}$
    end if
    if $\mathcal{G}'$ consists of a line e connecting root node of $\mathcal{G}'$ to a subtree G **then**
        return append($\{e\}$,OptimalLineRepairSchedule(G))
    end if
    Let $G_1, G_2, \cdots G_k$ be the subtrees connected to the root node of $\mathcal{G}'$
    for $i = 1, \cdots, k$ **do**
        $E_i \leftarrow$OptimalLineRepairSchedule(G_i)
        Let $(A_i, F_i) \leftarrow$GetHighestAverageSubsequence(E_i)
    end for
    Let $\sigma_1, \cdots, \sigma_k$ denote a permutation of F_is in decreasing order of A_is
    Merge the lines in $\sigma_1, \cdots, \sigma_k$ with root node of $\mathcal{G}'$ to form G
    return append($\sigma_1, \cdots, \sigma_k$,OptimalLineRepairSchedule(G)) ▷ Lines sequenced
end procedure
procedure GetHighestAverageSubsequence(E)
    Let $E = \{e_1, \cdots, e_n\}$
    for $j = 1, \cdots, n$ **do**
        Let $A_j \leftarrow$ average($\{e_1, \cdots, e_j\}$)
    end for
    Let y be the largest $j \in [n]$ such that $A_y = \max_j A_j$
    return A_y, $\{e_1, \cdots, e_y\}$
end procedure

cedure which returns the optimal sequence of lines in which they need to be repaired. Lines 3-8 define the base cases of the algorithm. Lines 9-16 define the recursive step of the algorithm. Due to recursion, optimal schedules of the smaller subtrees are obtained. Lines 14-15 show how the optimal schedules for the smaller subtrees can be merged to obtain the optimal schedule for the larger subtree. The merging steps utilize a subprocedure GetHighestAverageSubsequence which identifies a subschedule for repairing the most valuable edges in a subtree.

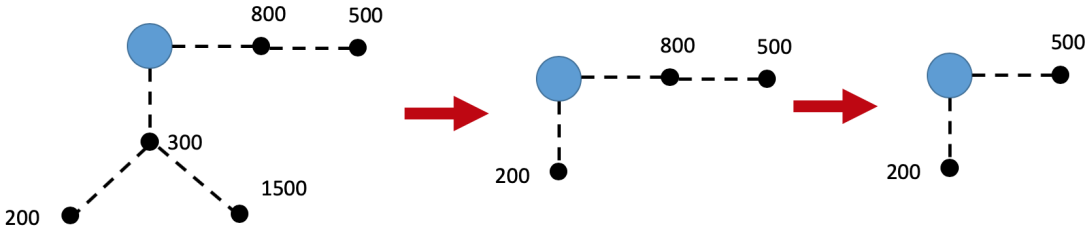


Figure 7-9: Illustrative example for recursive algorithm.

To illustrate the steps of Algorithm 11, consider the example in Figure 7-9. Let $\mathcal{G}$ denote the network on the left. $\mathcal{G}$ comprises of two subtrees $G_1 = \{800, 500\}$ and $G_2 = \{300, 200, 1500\}$. The recursive algorithm will determine the optimal line repair schedule for both G_1 and G_2. G_1, in turn, consists of line 800 connected to subtree consisting of one line 500. Hence, the optimal repair schedule of G_1 returns $800, 500$. G_2 comprises of line 300 connecting subtrees each consisting of one line 200 and 1500, respectively. These subtrees will be sorted based on their average values and then appended to line 300. Thus, the optimal repair schedule of G_2 will be returned as $\{300, 1500, 200\}$. Now, the highest average subsequence procedure for $\{800, 500\}$ returns $(800, \{800\})$, where the second entry denotes the list of lines, and the first entry denotes the average of the values of the nodes connected by these lines. Similarly, the highest average subsequence procedure for $\{300, 1500, 200\}$ returns $(900, \{300, 1500\})$. The higher of the two averages is 900. As a result, the lines $\{300, 1500\}$ are merged with the root node of $\mathcal{G}$, followed by the line 800. Finally, the resulting network on the right remains, for which the recursion continues.

We would like to clarify that there exists an iterative algorithm in the literature [29]

which computes an optimal schedule for $1|s-prec, outtree, p_i = 1|\sum_j w_j C_j$. We can argue using simple interchange arguments presented in [29] that Algorithm 11 also generates optimal schedules for our problem $1|s-prec, outtree, p_i = 1|\sum_j w_j C_j$. For $Pm|s-prec, outtree, p_i = 1|\sum_j w_j C_j$, we tried the approach as presented in [126]. We first generate an optimal schedule assuming $m = 1$. Then, in each time period m lines would be repaired in the order specified by the optimal schedule obtained assuming just single repair team. However, we present a simple counter-example where Algorithm 11 fails to generate a desired optimal schedule. Consider a contrived example as shown in Figure 7-10. In this example, we consider that $m = 2$ lines can be repaired in each time period. Assuming that only one line can be repaired in each time step, the optimal schedule obtained by using Algorithm 11 is $\{a, b, c, d\}$. Hence, for $m = 2$, a repair schedule will be to repair lines a, b in the first time period followed by lines c, d in the next time period. However, the actual optimal schedule is to repair lines c, d in the first time period followed by lines a, b in the next time period. Whether or not a polynomial time algorithm exists for $Pm|s-prec, outtree, p_i = 1|\sum_j w_j C_j$ is an open problem.

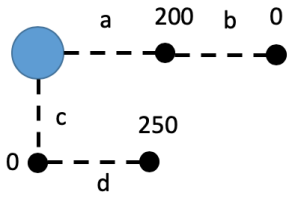


Figure 7-10: Counterexample for recursive algorithm with $m = 2$.

Concluding remarks: To summarize, in this chapter, we developed the following contributions, to address electricity network preparedness for storm-induced outages:

1. Two-stage stochastic optimization formulation for DER placement in DNs under uncertainty in component failure locations

2. Model of post-storm microgrid operation with DERs

3. Nonhomogeneous Poisson process (NHPP) model to predict spatially-varying likelihood of line failures

Our 2-stage stochastic optimization problem captures proactive allocation of resources under uncertainty due to storm-induced disruptions, as well as joint repair and dispatch actions in the post-storm restoration part. For the Stage 2 problem of network restoration, we also presented results based on greedy. Finally, we showed that the restoration problem can be formulated as a job-shop scheduling problem, and presented a recursive algorithm for a special case of single repair team.

Chapter 8

Conclusions

In this chapter, we first summarize the results presented in this thesis (Sec. 8.1), then describe our recommendations to improving the resilience of electricity networks (Sec. 8.2), and finally conclude with the future work related to the thesis (Sec. 8.3).

8.1 Summary of results

In Chapter 2, we presented an end-to-end framework for semantics-aware attack generation and implementation on Energy Management System software. We showed how an attacker could leverage the knowledge of a transmission network to manipulate the critical parameters of a control algorithm. The first part of the effort was regarding attack generation, for which we showed that an optimal attack can generated by solving a bilevel optimization problem. The second part of the effort was to exploit a vulnerability of an Energy Management System software, to locate the critical parameters in the dynamic memory space of the control algorithm. We demonstrated the implementation of such attacks on 5 real world EMS software.

In Chapters 3 to 6, we focused extensively on improving resilience of electricity distribution networks. Firstly, we showed that the impact of a broad class of cyberphysical failure scenarios can be modeled as DN-side disruption of multiple components and/or the disturbances in substation voltage and frequency. developed a quantitative framework to evaluate the resilience of electricity transmission networks to cyber and physical security and reliability failures. We adopted the generic definition of system resilience which is its

ability to minimize the impact after a disturbance, as well as to restore the system performance back to its nominal value. Secondly, we developed a novel network model which captures operations of microgrid(s) under various regimes, and single-/multi- master operation of DERs. Thirdly, we considered a range of operator response strategies: from load control and component disconnects to microgrid islanding and DER dispatch. Fourthly, we formulated the attacker-operator interactions as bilevel mixed-integer problems (P1) and (P2), and developed a computational approach to solve these problems using Benders decomposition algorithm. Finally, we introduced a problem (P3) about restoration of DN performance over multiple time periods, and presented a greedy algorithm for solving it. Our computational results for (P1)-(P3) show the value of timely response under varying operator capabilities in minimizing the impact of disruption as well as speedy system recovery.

One of the main takeaways is that although we assumed linear power flows and considered only basic aspects of microgrid operations, we hope that we have provided a rich and flexible modeling framework to analyze the DN resilience for more sophisticated attacks and response capabilities. Other cyber-physical security scenarios can be similarly analyzed by considering a clear demarcation between the vulnerable and the securely controllable DN components. The computational approach for solving bilevel formulation under linear power flows can be, in principle, extended to a convex (second-order cone) relaxation of nonlinear power flows. We showed the applications of this approach in terms of optimal resource allocation [110] and security investments into the DN [109]. Finally, the framework may be suitable for resiliency assessment of other smart infrastructure networks.

In Chapter 7, we considered the problem of proactive planning and network restoration for improved DN resilience due to weather-induced correlated reliability failures. Our contributions include: (a) Two-stage stochastic optimization formulation for DER placement in DNs under uncertainty in component failure locations, (b) a model of post-storm microgrid operation with DERs, and (c) nonhomogeneous Poisson process (NHPP) model to predict spatially-varying likelihood of line failures. We developed and a solution approach based on an extension of Benders decomposition algorithm.

8.2 Recommendations for building resilient grids

To build resilient grids, several measures need to be taken in both cyber and physical aspects of power system operations in proactive and reactive manner. First, we consider the cybersecurity of critical components, which involve the processes that run the control algorithms, the transmission and distribution substations, and the individual network components. As the NERC guidelines [94] suggest, proper reperimeterization of the substations is essential to prevent any cyberattacks on the controllers within the substations. This involves implementing standard security measures such as role-based access systems, dual factor authentication, increased personnel awareness [98]. Additionally, intrusion detection mechanisms need to be implemented, which will monitor abnormalities in the communication traffic as well as sensor data. Hardware-based protection mechanisms that can isolate critical control parameters are also desirable. Other measures include algorithmic redundancy, controller-command verification, and intrusion-tolerant replication.

Secondly, the critical nodes in the networks, for e.g. the transmission and distribution substations, need to be hardened. These facilities not only transmit huge amount of power, but also consist of substation automation systems that are critical for proper network control. These facilities can be physically protected by security personnel or fencing coupled with video surveillance capabilities. Additionally, proper precautions need to be taken for protection against extreme weather conditions such as heat wave, flooding, hurricanes, etc. Similar precautionary measures need to be taken to safeguard the critical lines of the networks.

Thirdly, diversification among resources is desirable so that the grids do not have any single point of failure. For example, if a DN is operated by centralized control, then the distribution management system is a single point-of-failure. However, if the devices are able to operate in a decentralized manner, as shown in Chapter 3, then the resilience of DN will be higher without requiring huge communication requirements for centralized coordination.

Finally, strategic allocation of resources in anticipation of adverse events should be

routinely carried out. Typically, there is some forecasting of the adverse weather events. Proper tools need to be developed that can take into account the weather forecast data, and assess the vulnerable components as well as the parts of the network that will be most impacted by the weather-induced disruptions. Consequently, the most vulnerable parts of the network should have proper allocation of resources of both portable DERs and repair equipment.

8.3 Future work

Now, we describe what aspects of our work on resilience of electricity networks can be improved upon.

We hope that our work in Chapter 6 can help early adoption and long-term deployment of resilient smart grid technologies, thus ensuring that communities can minimize the overwhelming impact of cyberphysical failures and quickly recover from it. Ensuring synergistic interactions between community microgrids involve several technical challenges. Some specific problems of immediate interest include: (i) modeling of multi-microgrid operations across DNs, (ii) distributed control of individual and inter-connected microgrids, (iii) optimal sensor placement based on microgrid communication protocols, control structures and budgetary restrictions.

In Chapter 7, we would like to improve upon the computational aspects of our solution approach. As stated in Sec. 7.2, the sample $\widehat{\mathcal{S}}$ used for SAA may not approximate the probability distribution $\mathcal{P}$ well. To obtain a more appropriate $\widehat{\mathcal{S}}$ that is representative of $\mathcal{P}$, we will use a scenario reduction method such as the forward selection or backward reduction algorithm [48]. The quality of solutions can be evaluated by calculation of the optimality gap [73]. To decrease computation time, we plan to consider greedy heuristics to solve the multi-step Stage II decision problem. Specifically, we select a small number of nodes based on their criticality. A node has high criticality if restoration of its load has high benefit on other intermediate nodes. The relative weights of the selected nodes are based on their criticality. Running the SAA method on the (minimum spanning tree) subnetwork induced by this smaller set of nodes can lead to a computational speed-up that allows us to feasibly test the model on larger test feeders.

Finally, the solution approaches developed in this thesis are likely applicable to the resilience assessment of other infrastructure networks, e.g. rail transportation, water distribution, etc. We would like to identify the structural properties of these infrastructure networks that will help enable fast solution algorithms.

Bibliography

[1] Amy Abel, Paul W Parfomak, and Dana A Shea. Electric utility infrastructure vulnerabilities: Transformers towers and terrorism, 2004. https://fas.org/sgp/crs/homesec/R42795.pdf.

[2] A. Abur and A.G. Expósito. *Power System State Estimation: Theory and Implementation.* Marcel Dekker, 2004.

[3] Y. P. Agalgaonkar, B. C. Pal, and R. A. Jabr. Distribution Voltage Control Considering the Impact of PV Generation on Tap Changers and Autonomous Regulators. *IEEE Transactions on Power Systems*, 29(1):182–192, Jan 2014.

[4] Shabbir Ahmed, Alexander Shapiro, and Er Shapiro. The sample average approximation method for stochastic programs with integer recourse. *Submitted for publication*, pages 1–24, 2002.

[5] O. Alsac and B. Stott. Optimal load flow with steady-state security. *IEEE Transactions on Power Apparatus and Systems*, PAS-93(3):745–751, May 1974.

[6] O. Alsac, N. Vempati, B. Stott, and A. Monticelli. Generalized state estimation. *IEEE Trans. on Power Systems*, 13(3):1069–1075, 1998.

[7] Karin Alvehag and Lennart Söder. A reliability model for distribution systems incorporating seasonal variations in severe weather. *IEEE Transactions on Power Delivery*, 26(2):910–919, 2011.

[8] Saurabh Amin, Galina A. Schwartz, and S. Shankar Sastry. Security of interdependent and identical networked control systems. *Automatica*, 49(1):186–192, January 2013.

[9] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal. Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance. *IEEE Transactions on Power Systems*, 20(4):1922–1928, Nov 2005.

[10] Göran Andersson. Dynamics and control of electric power systems. Technical report, ETH Zurich, 2012.

[11] Mallik Angalakudati, Siddharth Balwani, Jorge Calzada, Bikram Chatterjee, Georgia Perakis, Nicolas Raad, and Joline Uichanco. Business analytics for flexible resource allocation under random emergencies. *Management Science*, 60(6):1552–1573, 2014.

[12] J. Arrillaga and B. Smith. *AC-DC Power Systems Analysis*. The Institution of Electrical Engineers, 1998.

[13] Michael Assante. Confirmation of a Coordinated Attack on the Ukrainian Power Grid. SANS Industrial Control Systems Security Blog, 2016.

[14] Australia Energy Market Operator. Black System South Australia 28 September 2016. https://www.aemo.com.au/-/media/Files/Electricity/NEM/Market_Notices_and_Events/Power_System_Incident_Reports/2017/Integrated-Final-Report-SA-Black-System-28-September-2016.pdf.

[15] Edward V Badolato. *Hurricane Hugo: Lessons Learned in Energy Emergency Preparedness*. Strom Thurmond Institute of Government and Public Affairs at Clemson University, 1990.

[16] M. Baran and F. F. Wu. Optimal sizing of capacitors placed on a radial distribution system. *IEEE Transactions on Power Delivery*, 4(1):735–743, Jan 1989.

[17] C.R. Bayliss and B.J. Hardy. Power Quality – Voltage Disturbances (Chapter 25). In *Transmission and Distribution Electrical Engineering (Third Edition)*, pages 933 – 944. Newnes, Oxford, third edition edition, 2007.

[18] Vedat Bayram and Hande Yaman. Shelter location and evacuation route assignment under uncertainty: A benders decomposition approach. *Transportation Science*, 52(2):416–436, 2018.

[19] John Belski. Update on power outages from harvey, irma and maria, 2008. http://www.wlky.com/article/update-on-power-outages-from-harvey-irma-and-maria/12445723.

[20] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman. Power grid vulnerability to geographically correlated failures; analysis and control implications. In *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pages 2634–2642, April 2014.

[21] M Mithun Bhaskar, Muthyala Srinivas, and M Sydulu. Security constraint optimal power flow (SCOPF)-a comprehensive survey. *International Journal of Computer Applications*, 11(6):42–52, 2010.

[22] Daniel Bienstock. *Electrical Transmission System Cascades and Vulnerability: An Operations Research Viewpoint*. SIAM, 2015.

[23] Daniel Bienstock. *Electrical Transmission System Cascades and Vulnerability - an Operations Research Viewpoint*, volume 22 of *MOS-SIAM Series on Optimization*. SIAM, 2016.

[24] Daniel Bienstock and Abhinav Verma. The N-k problem in power grids: New models, formulations, and numerical experiments. *SIAM J. on Optimization*, 20(5):2352–2380, June 2010.

[25] Michelle Bloodworth and Paul Bailey. FERC Needs To Act On Resilience, 2017. http://www.americaspower.org/ferc-needs-to-act-on-resilience-part-3/.

[26] K. De Brabandere, B. Bolsens, J. Van den Keybus, A. Woyte, J. Driesen, and R. Belmans. A voltage and frequency droop control method for parallel inverters. *IEEE Transactions on Power Electronics*, 22(4):1107–1115, July 2007.

[27] K. De Brabandere, B. Bolsens, J. Van den Keybus, A. Woyte, J. Driesen, and R. Belmans. A voltage and frequency droop control method for parallel inverters. *IEEE Transactions on Power Electronics*, 22(4):1107–1115, July 2007.

[28] Martin Braun and Philipp Strauss. A review on aggregation approaches of controllable distributed energy units in electrical power systems. *International Journal of Distributed Energy Resources*, 4(4):297–319, 2008.

[29] Peter Brucker. *Scheduling Algorithms*. Springer-Verlag, Berlin, Heidelberg, 3rd edition, 2001.

[30] Eduardo F Camacho, Tariq Samad, Mario Garcia-Sanz, and Ian Hiskens. Control for renewable energy and smart grids. *The Impact of Control Technology, Control Systems Society*, pages 69–88, 2011.

[31] Richard Campbell. Weather-related power outages and electric system resiliency, 2012. https://fas.org/sgp/crs/misc/R42696.pdf.

[32] Richard Campbell. Cybersecurity issues for the bulk power system, congressional research service report, 2015. https://www.fas.org/sgp/crs/misc/R43989.pdf.

[33] Florin Capitanescu, JL Martinez Ramos, Patrick Panciatici, Daniel Kirschen, A Marano Marcolini, Ludovic Platbrood, and Louis Wehenkel. State-of-the-art, challenges, and future trends in constrained optimal power flow. *Electric Power Systems Research*, 81(8):1731–1741, 2011.

[34] Alvaro A. Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry. Attacks against process control systems: Risk assessment, detection, and response. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, pages 355–366, New York, NY, USA, 2011. ACM.

[35] Central Electricity Regulatory Commission (CERC). Report on the grid disturbance on 30^{th} and 31^{st} july, 2012. http://www.cercind.gov.in/2012/orders/Final_Report_Grid_Disturbance.pdf.

[36] Haowen Chan, Hsu-Chun Hsiao, Adrian Perrig, and Dawn Song. Secure distributed data aggregation. *Foundations and Trends in Databases*, 3(3):149–201, 2011.

[37] Haowen Chan, Adrian Perrig, Bartosz Przydatek, and Dawn Xiaodong Song. SIA: secure information aggregation in sensor networks. *Journal of Computer Security*, 15(1):69–102, 2007.

[38] D. Chang, D. Shelar, and S. Amin. Der allocation and line repair scheduling for storm-induced failures in distribution networks. In *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pages 1–7, Oct 2018.

[39] L. Che, M. Khodayar, and M. Shahidehpour. Only connect: Microgrids for distribution system restoration. *IEEE Power and Energy Magazine*, 12(1):70–81, Jan 2014.

[40] C. Chen, J. Wang, F. Qiu, and D. Zhao. Resilient Distribution System by Microgrids Formation After Natural Disasters. *IEEE Transactions on Smart Grid*, 7(2):958–966, March 2016.

[41] H. D. Chiang and M. E. Baran. On the existence and uniqueness of load flow solution for radial distribution power networks. *IEEE Transactions on Circuits and Systems*, 37(3):410–416, Mar 1990.

[42] China Electricity Council. Statistics of power industry basics. http://english.cec.org.cn/No.118.index.htm.

[43] C Matthew Davis and Thomas J Overbye. Multiple element contingency screening. *Power Systems, IEEE Transactions on*, 26(3):1294–1301, 2011.

[44] Department of Energy. Dynamic Line Rating Systems for Transmission Lines; available at https://www.smartgrid.gov/files/SGDP_Transmission_DLR_Topical_Report_04-25-14_FINAL.pdf, 2016.

[45] Department of Energy. Improving Efficiency with Dynamic Line Ratings; available at https://www.smartgrid.gov/files/NYPA_Improving-Efficiency-Dynamic-Line-Ratings.pdf, 2016.

[46] Department of Homeland Security. Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A.

[47] Florian Dorfler and Francesco Bullo. Kron Reduction of Graphs with Applications to Electrical Networks. *arXiv e-prints*, page arXiv:1102.2950, Feb 2011.

[48] J. Dupačová, N. Gröwe-Kuska, and W. Römisch. Scenario reduction in stochastic programming. *Mathematical Programming*, 95(3):493–511, Mar 2003.

[49] Yury Dvorkin and Siddharth Garg. IoT-enabled distributed cyber-attacks on transmission and distribution grids. *2017 North American Power Symposium (NAPS)*, pages 1–6, 2017.

[50] David Eoff. Diesel generator failures: Lessons taught by hurricanes, 2007. https://www.power-eng.com/articles/print/volume-111/issue-8/departments/dg-update/diesel-generator-failures-lessons-taught-by-hurricanes.html.

[51] Nicolas Falliere, Liam O. Murchu, and Eric Chien. W32.Stuxnet Dossier. Technical report, Symantic Security Response, October 2010.

[52] M. Farivar and S. H. Low. Branch Flow Model: Relaxations and Convexification - Part I. *IEEE Transactions on Power Systems*, 28(3):2554–2564, Aug 2013.

[53] M. Farivar, R. Neal, C. Clarke, and S. Low. Optimal inverter VAR control in distribution systems with high PV penetration. In *2012 IEEE Power and Energy Society General Meeting*, pages 1–7, July 2012.

[54] H. Fawzi, P. Tabuada, and S. Diggavi. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*, 59(6):1454–1467, June 2014.

[55] Matteo Fischetti, Ivana Ljubić, Michele Monaci, and Markus Sinnl. A New General-Purpose Algorithm for Mixed-Integer Bilevel Linear Programs. *Operations Research*, 65(6):1615–1637, 2017.

[56] Matteo Fischetti, Ivana Ljubić, Michele Monaci, and Markus Sinnl. On the use of intersection cuts for bilevel optimization. *Mathematical Programming*, 172(1):77–103, Nov 2018.

[57] Shailendra Fuloria and Ross J. Anderson. Towards a security architecture for substations. In *2nd IEEE PES International Conference and Exhibition on "Innovative Smart Grid Technologies", ISGT Europe 2011, Manchester, United Kingdom, December 5-7, 2011*, pages 1–6, 2011.

[58] L. Gan, N. Li, U. Topcu, and S. H. Low. Exact convex relaxation of optimal power flow in radial networks. *IEEE Transactions on Automatic Control*, 60(1):72–87, Jan 2015.

[59] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla. Smart Grid Data Integrity Attacks. *IEEE Transactions on Smart Grid*, 4(3):1244–1253, Sep. 2013.

[60] N. J. Gil and J. A. P. Lopes. Hierarchical Frequency Control Scheme for Islanded Multi-Microgrids Operation. In *2007 IEEE Lausanne Power Tech*, pages 473–478, July 2007.

[61] J.D. Glover, M.S. Sarma, and T. Overbye. *Power System Analysis and Design*. Cengage Learning, 2011.

[62] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla. Hierarchical Control of Droop-Controlled AC and DC Microgrid–A General Approach Toward Standardization. *IEEE Transactions on Industrial Electronics*, 58(1):158–172, Jan 2011.

[63] Nikos Hatziargyriou, Hiroshi Asano, Reza Iravani, and Chris Marnay. Microgrids: An Overview of Ongoing Research, Development, and Demonstration Projects. *IEEE Power & Energy Magazine*, July/August:19, 08/2007 2007.

[64] Heat wave leaves thousands of Australian homes without power. https://www.reuters.com/article/us-australia-power/heat-wave-leaves-thousands-of-australian-homes-without-power-idUSKBN1FI0CO.

[65] Jon A. Heintz and Christopher Rojahn. Emergency Power Systems for Critical Facilities: A Best Practices Approach to Improving Reliability, September 2014. https://www.fema.gov/media-library-data/1424214818421-60725708b37ee7c1dd72a8fc84a8e498/FEMAP-1019_Final_02-06-2015.pdf.

[66] Hassan Hijazi, Ksenija Bestuzheva, and Dan Gordon. Powertools, 2017. http://hhijazi.github.io/PowerTools/.

[67] I. A. Hiskens. What's smart about the smart grid? In *Design Automation Conference (DAC), 2010 47th ACM/IEEE*, pages 937–939, June 2010.

[68] Greg J Holland. An analytic model of the wind and pressure profiles in hurricanes. *Monthly weather review*, 108(8):1212–1218, 1980.

[69] Bowen Hua, Ross Baldick, and Kevin Wood. Interdiction of a Mixed-Integer Linear System. *INFORMS*, 01/2019 2019.

[70] IEEE Standards Coordinating Committee 21. IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces. *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)*, pages 1–138, April 2018.

[71] F. Katiraei, R. Iravani, N. Hatziargyriou, and A. Dimeas. Microgrids management. *IEEE Power and Energy Magazine*, 6(3):54–65, May 2008.

[72] R Kevin Wood. Bilevel network interdiction models: Formulations and solutions. *Wiley Encyclopedia of Operations Research and Management Science*, 174, 02 2011.

[73] Anton J Kleywegt, Alexander Shapiro, and Tito Homem-de Mello. The sample average approximation method for stochastic discrete optimization. *SIAM Journal on Optimization*, 12(2):479–502, 2002.

[74] S. Kundu and I.A. Hiskens. Overvoltages due to synchronous tripping of plug-in electric-vehicle chargers following voltage dips. *Power Delivery, IEEE Transactions on*, 29(3):1147–1156, June 2014.

[75] Robert Lee, Michael Assante, and Tim Conway. Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center, 2015. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[76] Gengfeng Li, Peng Zhang, Peter B Luh, Wenyuan Li, Zhaohong Bie, Camilo Serna, and Zhibing Zhao. Risk analysis for distribution systems in the northeast us under wind storms. *IEEE Transactions on Power Systems*, 29(2):889–898, 2014.

[77] J. Liang, L. Sankar, and O. Kosut. Vulnerability analysis and consequences of false data injection attack on power system state estimation. *IEEE Transactions on Power Systems*, 31(5):3864–3872, Sept 2016.

[78] Zhiqiang Lin, Xiangyu Zhang, and Dongyan Xu. Automatic reverse engineering of data structures from binary execution. In *Proceedings of Information Security Symposium*, page 5. CERIAS-Purdue University, 2010.

[79] Haibin Liu, Rachel A Davidson, and Tatiyana V Apanasovich. Statistical forecasting of electric power restoration times in hurricanes and ice storms. *IEEE Transactions on Power Systems*, 22(4):2270–2279, 2007.

[80] Yao Liu, Peng Ning, and Michael K Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):13, 2011.

[81] Yao Liu, Peng Ning, and Michael K. Reiter. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.*, 14(1):13:1–13:33, June 2011.

[82] A. Y. Lokhov, M. Vuffray, D. Shemetov, D. Deka, and M. Chertkov. Online Learning of Power Transmission Dynamics. In *2018 Power Systems Computation Conference (PSCC)*, June 2018.

[83] J. A. P. Lopes, C. L. Moreira, and A. G. Madureira. Defining control strategies for microgrids islanded operation. *IEEE Transactions on Power Systems*, 21(2):916–924, May 2006.

[84] J. A. P. Lopes, C. L. Moreira, A. G. Madureira, F. O. Resende, X. Wu, N. Jayawarna, Y. Zhang, N. Jenkins, F. Kanellos, and N. Hatziargyriou. Control strategies for microgrids emergency operation. In *2005 International Conference on Future Power Systems*, pages 6 pp.–6, Nov 2005.

[85] Leonardo Lozano and J. Cole Smith. A Value-Function-Based Exact Approach for the Bilevel Mixed-Integer Programming Problem. *Operations Research*, 65(3):768–786, 2017.

[86] Zhigang Lu and Zongwei Zhang. Bad data identification based on measurement replace and standard residual detection. *Automation of Electric Power Systems*, 13:011, 2007.

[87] Daisuke Mashima and Alvaro A. Cárdenas. Evaluating electricity theft detectors in smart grid networks. In Davide Balzarotti, Salvatore J. Stolfo, and Marco Cova, editors, *Research in Attacks, Intrusions, and Defenses*, pages 210–229, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[88] Stephen McLaughlin, Saman Zonouz, Devin Pohly, and Patrick McDaniel. A trusted safety verifier for controller code. In *NDSS*, 2014.

[89] Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli. CyberâĂŞphysical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, Jan 2012.

[90] Daniel K. Molzahn and Ian A. Hiskens. A Survey of Relaxations and Approximations of the Power Flow Equations. *Foundations and Trends in Electric Energy Systems*, 4(1-2):1–221, 2019.

[91] A. Monticelli, M. V. F. Pereira, and S. Granville. Security-constrained optimal power flow with post-contingency corrective rescheduling. *IEEE Transactions on Power Systems*, 2(1):175–180, Feb 1987.

[92] James T. Moore and Jonathan F. Bard. The Mixed Integer Linear Bilevel Programming Problem. *Operations Research*, 38(5):911–921, 1990.

[93] National Infrastructure Advisory Council. Critical Infrastructure Resilience Final Report and Recommendations, September 2009. https://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

[94] NERC Reliability Standards. CIP-005-5 – Cyber Security - Electronic Security Perimeter(s), December 2015. https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-5.pdf.

[95] NERC Synchronized Measurement Subcommittee (SMS). Fault Induced Delayed Voltage Recovery (FIDVR) Advisory, July 2015. https://goo.gl/Xy6Vwv.

[96] North Start Electric Cooperative Website. Compensation of load control.

[97] F. Pasqualetti, F. DÃűrfler, and F. Bullo. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729, Nov 2013.

[98] Tomo Popovic, Chris Blask, Matthew Carpenter, Stephen Chasko, Glen Chason, Gabriela Ciocarlie, Frances Cleveland, Brian Davison, Dick DeBlasio, Donna Dickinson, Michael David, Pat Duggan, Mark Ellison, Shrinath Eswarahally, Irene Gassko, Erfian Gonzales, Slade Griffin, Virgil Hammond, Jordan Henry, and Scott Rosenberger. Electric Sector Failure Scenarios and Impact Analyses - Version 3.0 (NESCOR), 12 2015.

[99] Damien Prot and Odile Bellenguez-Morineau. How the structure of precedence constraints may change the complexity class of scheduling problems. *arXiv e-prints*, page arXiv:1510.04833, Oct 2015.

[100] H. Qi, X. Wang, L. M. Tolbert, F. Li, F. Z. Peng, P. Ning, and M. Amin. A Resilient Real-Time System Design for a Secure and Reconfigurable Power Grid. *IEEE Trans. on Smart Grid*, 2(4):770–781, Dec 2011.

[101] AA Salam, A Mohamed, and MA Hannan. Technical challenges on microgrids. *ARPN Journal of engineering and applied sciences*, 3(6):64–69, 2008.

[102] J. Salmeron, K. Wood, and R. Baldick. Analysis of electric grid security under terrorist threat. *IEEE Transactions on Power Systems*, 19(2):905–912, May 2004.

[103] J. Salmeron, K. Wood, and R. Baldick. Worst-case interdiction analysis of large-scale electric power grids. *IEEE Transactions on Power Systems*, 24(1):96–104, Feb 2009.

[104] H. Sandberg, S. Amin, and K. H. Johansson. Cyberphysical security in networked control systems: An introduction to the issue. *IEEE Control Systems*, 35(1):20–23, Feb 2015.

[105] Scientific American. U.s. electrical grid undergoes massive transition to connect to renewables. https://www.scientificamerican.com/article/what-is-the-smart-grid/.

[106] N. C. Scott, D. J. Atkinson, and J. E. Morrell. Use of load control to regulate voltage on distribution networks with embedded generation. *IEEE Transactions on Power Systems*, 17(2):510–515, May 2002.

[107] Suvrajeet Sen and Julia L. Higle. The c3 theorem and a d2 algorithm for large scale stochastic mixed-integer programming: Set convexification. *Mathematical Programming*, 104(1):1–20, Sep 2005.

[108] D. Shelar and S. Amin. Analyzing vulnerability of electricity distribution networks to DER disruptions. In *2015 American Control Conference (ACC)*, pages 2461–2468, July 2015.

[109] D. Shelar and S. Amin. Security Assessment of Electricity Distribution Networks Under DER Node Compromises. *IEEE Transactions on Control of Network Systems*, 4(1):23–36, March 2017.

[110] D. Shelar, S. Amin, and I. Hiskens. Towards Resilience-Aware Resource Allocation and Dispatch in Electricity Distribution Networks. *Book chapter in Springer/IMA volume on The Control of Energy Markets and Grids*, 2018.

[111] D. Shelar, J. Giraldo, and S. Amin. A distributed strategy for electricity distribution network control in the face of der compromises. In *2015 54th IEEE Conference on Decision and Control (CDC)*, pages 6934–6941, Dec 2015.

[112] D. Shelar, P. Sun, S. Amin, and S. Zonouz. Compromising security of economic dispatch in power system operations. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 531–542, June 2017.

[113] Devendra Shelar and Saurabh Amin. Security Assessment of Electricity Distribution Networks under DER Node Compromises. *arXiv e-prints*, page arXiv:1601.01342, Jan 2016.

[114] Devendra Shelar, Saurabh Amin, and Ian Hiskens. Resilience of Electricity Distribution Networks - Part I: Cyber-physical Disruption Models. *arXiv e-prints*, page arXiv:1812.01746, Dec 2018.

[115] Devendra Shelar, Saurabh Amin, and Ian Hiskens. Resilience of Electricity Distribution Networks - Part II: Leveraging Microgrids. *arXiv e-prints*, page arXiv:1812.01745, Dec 2018.

[116] Hanif D. Sherali and Barbara M.P. Fraticelli. A modification of benders' decomposition algorithm for discrete subproblems: An approach for stochastic programs with integer recourse. *Journal of Global Optimization*, 22(1):319–342, Jan 2002.

[117] J. W. Simpson-Porco, Q. Shafiee, F. Dörfler, J. C. Vasquez, J. M. Guerrero, and F. Bullo. Secondary Frequency and Voltage Control of Islanded Microgrids via Distributed Averaging. *IEEE Transactions on Industrial Electronics*, 62(11):7025–7038, Nov 2015.

[118] H. Singh and F.L. Alvarado. Network topology determination using least absolute value state estimation. *Power Systems, IEEE Transactions on*, 10(3):1159–1165, 1995.

[119] Thomas B Smith. Electricity theft: a comparative analysis. *Energy Policy*, 32(18):2067 – 2076, 2004.

[120] Saleh Soltan, Prateek Mittal, and H. Vincent Poor. Protecting the Grid against IoT Botnets of High-Wattage Devices. *CoRR*, abs/1808.03826, 2018.

[121] Kin Cheong Sou, H. Sandberg, and K.H. Johansson. Computing critical k -tuples in power networks. *Power Systems, IEEE Transactions on*, 27(3):1511–1520, Aug 2012.

[122] Pengfei Sun, Rui Han, Mingbo Zhang, and Saman Zonouz. Trace-free memory data structure forensics via past inference and future speculations. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pages 570–582. ACM, 2016.

[123] Yan Sun and Thomas J Overbye. Visualizations for power system contingency analysis data. *IEEE Trans. on Power Systems*, 19(4):1859–66, 2004.

[124] Rui Tan, Varun Badrinath Krishna, David KY Yau, and Zbigniew Kalbarczyk. Impact of integrity attacks on real-time pricing in smart grids. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 439–450. ACM, 2013.

[125] Rui Tan, Hoang Hai Nguyen, Eddy YS Foo, Xinshu Dong, David KY Yau, Zbigniew Kalbarczyk, Ravishankar K Iyer, and Hoay Beng Gooi. Optimal false data injection attack against automatic generation control in power grids. In *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, pages 1–10, 2016.

[126] Yushi Tan, Feng Qiu, Arindam K Das, Daniel S Kirschen, Payman Arabshahi, and Jianhui Wang. Scheduling post-disaster repairs in electricity distribution networks. *arXiv preprint arXiv:1702.08382*, 2017.

[127] The Guardian. Massive power failure plunges 80 percent of Pakistan into darkness, 2015. https://www.theguardian.com/world/2015/jan/25/massive-power-failure-plunges-80-of-pakistan-into-darkness.

[128] Reinaldo Tonkoski, Luiz AC Lopes, and Tarek HM El-Fouly. Coordinated active power curtailment of grid connected pv inverters for overvoltage prevention. *IEEE Transactions on Sustainable Energy*, 2(2):139–147, 2011.

[129] Frances Fragos Townsend. The federal response to hurricane katrina, 2006. http://www.au.af.mil/au/awc/awcgate/whitehouse/katrina/katrina-lessons-learned.pdf.

[130] K. Turitsyn, P. Sulc, S. Backhaus, and M. Chertkov. Options for control of reactive power by distributed photovoltaic generators. *Proceedings of the IEEE*, 99(6):1063–1073, June 2011.

[131] Thierry Van Cutsem and Costas Vournas. *Voltage stability of electric power systems*, volume 441. Springer Science & Business Media, 1998.

[132] Pascal Van Hentenryck, Russell Bent, and Carleton Coffrin. Strategic planning for disaster recovery with stochastic last mile distribution. In *International conference on integration of artificial intelligence (AI) and operations research (OR) techniques in constraint programming*, pages 318–333. Springer, 2010.

[133] T. L. Vandoorn, J. C. Vasquez, J. De Kooning, J. M. Guerrero, and L. Vandevelde. Microgrids: Hierarchical Control and an Overview of the Control and Reserve Management Strategies. *IEEE Industrial Electronics Magazine*, 7(4):42–55, Dec 2013.

[134] L. Wang and P. Xu. The Watermelon Algorithm for The Bilevel Integer Linear Programming Problem. *SIAM Journal on Optimization*, 27(3):1403–1430, 2017.

[135] Yong Wang, Zhaoyan Xu, Jialong Zhang, Lei Xu, Haopei Wang, and Guofei Gu. Srid: State relation based intrusion detection for false data injection attacks in scada. In *European Symposium on Research in Computer Security*, pages 401–418. Springer, 2014.

[136] Don Wareham. Step voltage regulators. http://www.cscos.com/wp-content/uploads/NY1839-Eaton-Regulators-D.Wareham.pdf.

[137] Sean David Whipple. *Predictive storm damage modeling and optimizing crew response to improve storm response operations*. PhD thesis, Massachusetts Institute of Technology, 2014.

[138] Allen J Wood and Bruce F Wollenberg. *Power generation, operation, and control*. John Wiley & Sons, 2012.

[139] Lian Xie, Shaowu Bao, Leonard J Pietrafesa, Kristen Foley, and Montserrat Fuentes. A real-time hurricane surface wind forecasting model: Formulation and verification. *Monthly Weather Review*, 134(5):1355–1370, 2006.

[140] Pan Xu and Lizhi Wang. An exact algorithm for the bilevel mixed integer linear programming problem under three simplifying assumptions. *Computers & Operations Research*, 41:309–318, 2014.

[141] R. Yan, N. -Masood, T. Kumar Saha, F. Bai, and H. Gu. The anatomy of the 2016 south australia blackout: A catastrophic event in a high renewable network. *IEEE Transactions on Power Systems*, 33(5):5374–5388, Sep. 2018.

[142] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez. Trilevel Optimization in Power Network Defense. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 37(4):712–718, July 2007.

[143] Daniel Yergin. Ensuring energy security. *Foreign Affairs*, 85(2):69–82, 2006.

[144] Y. Yuan, Z. Li, and K. Ren. Modeling Load Redistribution Attacks in Power Systems. *IEEE Transactions on Smart Grid*, 2(2):382–390, June 2011.

[145] Bo Zeng and Yu An. Solving bilevel mixed integer program by reformulations and decomposition. *Optimization online*, pages 1–34, 2014.

[146] H. Zhang, P. Cheng, L. Shi, and J. Chen. Optimal DoS attack scheduling in wireless networked control system. *IEEE Transactions on Control Systems Technology*, 24(3):843–852, May 2016.

[147] Junhui Zhao, Caisheng Wang, Bo Zhao, Feng Lin, Quan Zhou, and Yang Wang. A Review of Active Management for Distribution Networks: Current Status and Future Development Trends. *Electric Power Components and Systems*, 42(3-4):280–293, 2014.

[148] L. Zhao and B. Zeng. Vulnerability Analysis of Power Grids With Line Switching. *IEEE Transactions on Power Systems*, 28(3):2727–2736, Aug 2013.

[149] Yujia Zhou, Anil Pahwa, and S-S Yang. Modeling weather-related failures of overhead distribution lines. *IEEE Transactions on Power Systems*, 21(4):1683–1690, 2006.

[150] M. Zhu and S. Martínez. On the performance analysis of resilient networked control systems under replay attacks. *IEEE Transactions on Automatic Control*, 59(3):804–808, March 2014.