RESILIENCE-ORIENTED RISK REDUCTION IN THE CYBER-PHYSICAL POWER GRID FOR NEXT GENERATION ENERGY MANAGEMENT

A Dissertation

by

AMARACHI TOCHI UMUNNAKWE

Submitted to the Graduate and Professional School of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Katherine Davis
Committee Members,	Thomas Overbye
	Ana Goulart
	Dileep Kalathil
Head of Department,	Costas Georghiades

August 2023

Major Subject: Electrical Engineering

ABSTRACT

Electric power grids are critical infrastructure that enhance the security, economy, and productivity of nations. In modern societies, power grids are continually evolving into smarter grids which incorporate automation to improve reliability using information and communication technologies, forming the cyber layer. The cyber layer interacts with the physical power grid by acquiring measurements from, and sending control commands, to field devices, forming an interconnection between the cyber and physical layers, referred to as the cyber-physical power grid.

Although these layers are essential to grid operation, they are vulnerable to a myriad of threats which can evolve to high impact disruptive events, resulting in catastrophic failures and losses such as widespread blackouts, loss of critical services enabled by electricity, and loss of lives and property. These events often cripple economic operations, disrupt societies, and threaten national security. Hence, strengthening the power grid against these threats has easily become a top priority, achieved by improving the resilience of the power grid.

This dissertation presents risk reduction against cyber and physical threats via a resilience-oriented perspective, intended to build into the vision of next generation energy management. The work presented in this dissertation focuses on common threats that have begun to more frequently affect the reliability and resilient operations of power systems, some leading to bankruptcy and strained customer relations for several utilities. Hence, this dissertation answers the question: ***How Can We Proactively Reduce Critical Power Infrastructure Risk to High Impact Cyber and Physical Threats, Automating the Risk Reduction Process, with Resilience at the Forefront?***

Toward this objective, this dissertation first presents an approach based on the axiomatic design process to enable the standardization of power system resilience, an issue that has been elusive to the power system resilience community in the past decade, which elucidates the studies herein. Then, the threats which highly impact the resilience of the power grid as a cyber-physical system are introduced, since the power grid is threatened by adversaries from both the cyber and physical domains. In the cyber layer, the dissertation presents risk reduction to threats of adversary intrusion and ensuing false data injection attacks using different techniques centered around graph-based modeling, where we propose a proactive framework to reduce the impact of adversary intrusion on the system, and develop a detector for stealth attacks which evades conventional power system detectors, respectively. Further on the cyber layer, the dissertation proposes techniques and implements modeling via emulation which achieve automation in the crucial provision of sandbox environments for the risk evaluations of critical infrastructure. These aid to improve system resilience via use cases such as cyber deception where redundancy against adversaries is provided to power system networks. In the physical layer, the dissertation focuses on the frequent and high impact threat of wildfires. The risk minimization builds on accurately modeling wildfire threats in a proposed novel technique that is designed to be efficient for the bulk power grid as opposed to conventional methods in which power systems adapt techniques better suited for wildlands. The proposed technique uses spatio-temporal and data-driven deep learning methods, which can effectively reduce power system risk from endogenous wildfires caused by the power grid, and exogenous wildfire from external sources. Beyond risk assessment and minimization, the dissertation proceeds to present the first-of-its-kind resilience-comprehensive design and development of a self-sufficient low-cost wildfire mitigation model which automates the risk reduction process towards mitigating wildfires in grid operation through all phases in which the power system lies before, during, and after a wildfire threat or event.

DEDICATION

TO ME

ACKNOWLEDGMENTS

I would like to express my heartfelt gratitude to the brilliant and amazing minds I have had the opportunity to meet, collaborate with, teach, mentor, and be mentored by. In particular, I would like to appreciate my "AWESOME" advisor, Professor Katherine R. Davis, for her support, encouragement, and supervisory style which has enabled me spread my wings and explore diverse facets of the power grid presented here in. With this wholesome style of inclusion, I have partaken in several high-end opportunities to tangibly participate in offering large-scale trainings, lead projects, contribute to and lead grant proposals. This has further elevated my confidence to flourish in my next endeavors as I graduate from Texas A&M University, and for these, I am grateful.

I would also like to thank my committee members Prof. Thomas Overbye, Prof. Ana Goulart, and Prof. Dileep Kalathil for their time and efforts, and even more so, their comments, insights, and valuable contributions to this work.

It was a pleasure to work with my brilliant colleagues Dr. Abhijeet Sahu, Dr. Hao Huang, Dr. Osman Boyaci, Dr. Zeyu Mao, Patrick Wlazlo, and Dr. Rasoul Narimani. I would like to thank all my collaborators for the perspectives they have contributed towards the development of this work.

Last but not least, I would like to acknowledge my family for their time and efforts, advice and free therapy, in the course of this long journey that has culminated in gratitude.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supported by a thesis committee consisting of Professor Katherine Davis, Professor Thomas Overbye, and Professor Dileep Kalathil of the Electrical and Computer Engineering Department, and Professor Ana Goulart of the Electronic Systems Engineering Technology Department at Texas A&M University.

The work presented in Chapter 2 is in collaboration with Dr. Abhijeet Sahu of the National Renewable Energy Laboratory, Prof. Mohammad Rasoul Narimani of the Department of Electrical Engineering in California State University Northridge, and Prof. Saman Zonouz at the Schools of Cybersecurity and Privacy, and Electrical and Computer Engineering at Georgia Tech. The work presented in Chapter 3 is in collaboration with Dr. Osman Boyaci who has graduated from the Electrical and Computer Engineering Department at Texas A&M University. All other work presented in this dissertation was completed by the student independently.

Funding Sources

Graduate study was supported by: Deep Cyber-Physical Situational Awareness for Energy Systems (CyPRES) from the US Department of Energy (DOE) under award DE-OE0000895, the National Science Foundation under Grant 1916142, and Texas A&M Engineering Experiment Station's Smart Grid Center.

TABLE OF CONTENTS

Page

LIST OF FIGURES

FIGURE Page

LIST OF TABLES

TABLE Page

1. INTRODUCTION

The electric power grid is a complex and essential infrastructure that facilitates all facets of modern societies. In the United States, there are 16 critical infrastructures including food, water, medical care, communications, finance, and more which heavily depend on the electric grid [1]. The goal of the power grid is to maintain reliable provision of electricity to end users. As technologies advance and civilizations expand, the demand for electricity grows and the power grid constantly evolves to meet modern needs by adopting new technologies, architectures, operational and planning approaches, while integrating security and affordability. If the electric power grid goes down, the United States arguably gets moved back, past the pre-Web 1980s, into the pre-electric grid 1880s [2]. In hostile environments such as those influenced by malicious attacks and hazards that threaten the grid, this goal of providing reliable power and trustworthy operations is met by improving grid resilience.

Resilience was first introduced as a measure to determine the system's ability to absorb changes to its state and driving variables [3]. Resilience has quickly become paramount in power systems operations and planning, with substantial federal infrastructure investments catering to High Impact Low Frequency (HILF) events like natural disasters and cyber threats [4]. However, since power systems keep evolving, the definition of power system resilience has yet to be consolidated. The following sections are dedicated to understanding power system resilience, to facilitate the science and perspective of resilience-oriented risk reduction.

1.1 Power System Resilience

Resilience is typically characterized by: (a) the magnitude of shock the system can absorb and remain within a given state, (b) the degree to which the system is capable of self-organization, (c) the degree to which the system can build capacity for learning and adaptation [5]. In power systems, resilience is defined as the grid's ability to prepare for and adapt to changing operating conditions, as well as withstand and recover rapidly from major disruptions caused by naturally occurring threats or deliberate cyber-physical attacks [4, 6, 7].

1.1.1 The Resilience Trapezoid

The resilience trapezoid provides a visual illustration of resilience, showing the different phases in which the system lies in the course of HILF events. As illustrated Fig. 1.1, in the pre-event phase, system operates at normal conditions, and as the disruptive event strikes, the system absorbs some shock and goes into the alert state. Further degradation sends the system into an emergency state, then to the outage phase which is an abnormal state. In this state, corrective and emergency resources are applied towards critical load restoration, also known as the self-recovery when the emergency resources are pre-integrated into system operations. After prioritized restoration of critical loads, recovery efforts continue with repair and restoration of damaged infrastructure.

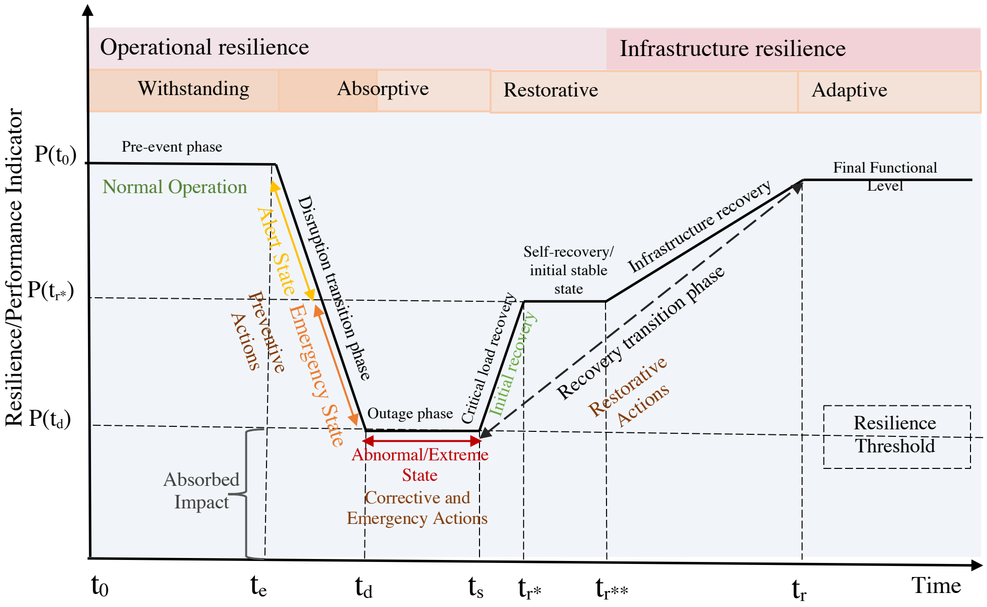


Figure 1.1: The Resilience Trapezoid, with power system performance $P(t)$ at original state t_0, disruptive event occurrence t_e, post-disruption state t_d, initiation of recovery actions t_s, initial system recovery t_{r*}, infrastructure restoration begins t_{r**}, and full system restoration state t_r. Reprinted from [7].

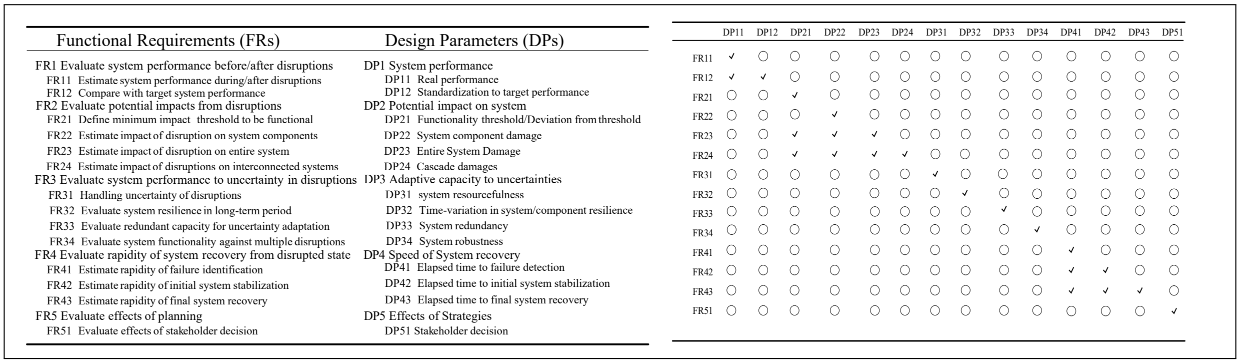
1.1.2 Resilience Capabilities and Dimensions

Resilience phases can be associated with different capabilities including the withstanding, absorptive, adaptive and restorative capabilities. These capabilities can also be associated with the resilience dimensions namely robustness, redundancy, resourcefulness, and rapidity, also known as the 4Rs of resilience [8]. Robustness, associated with the withstanding capability, is the ability of the system to withstand disruption up to a given level without loss of functionality. Redundancy is the extent to which components and subsystems can be substituted to satisfy the suffered loss of functionality. It is associated with the absorptive capability at the disruption transition and outage phases. Resourcefulness is the ability of the system to identify system failures, prioritize and mobilize resources when conditions threaten the system, or towards meeting target recovery. It can be assessed between the disruption and restorative transition phases. Rapidity is the ability to meet recovery priorities in a timely manner in order to contain losses and maintain functionality. Further details can be found in our work [7].

1.1.3 Towards Resilience Unification and Standardization

A major issue in power system resilience is a lack of standardization. Our work in [7] pioneers a solution via an approach based on the Axiomatic Design Process (ADP). The ADP is the logical process towards an objective through a series of domains [9,10], including the (1) Service Domain, (2) Functional Domain, (3) Physical Domain, and (4) Process Domain. In this work, the resilience capabilities are adapted as the power system resilience objectives towards meeting customer needs in the service domain during a HILF event. These objectives are then transformed into functional requirements (FRs) in the Functional Domain, and Design Parameters (DPs) are defined in the Physical Domain to specify the recognized FRs. The interaction between FRs and DPs, in Table 1.1, is the major design process [11]. Hence, for the power system to be considered resilient, it should meet the functional requirements, which can be achieved using the outlined DPs.

Table 1.1: 1) Defining FRs and DPs for Power System Resilience, 2) Decoupled Design Matrix. Reprinted from [7].



Functional Requirements (FRs)	Design Parameters (DPs)
FR1 Evaluate system performance before/after disruptions	DP1 System performance
FR11 Estimate system performance during/after disruptions	DP11 Real performance
FR12 Compare with target system performance	DP12 Standardization to target performance
FR2 Evaluate potential impacts from disruptions	DP2 Potential impact on system
FR21 Define minimum impact threshold to be functional	DP21 Functionality threshold/Deviation from threshold
FR22 Estimate impact of disruption on system components	DP22 System component damage
FR23 Estimate impact of disruption on entire system	DP23 Entire System Damage
FR24 Estimate impact of disruptions on interconnected systems	DP24 Cascade damages
FR3 Evaluate system performance to uncertainty in disruptions	DP3 Adaptive capacity to uncertainties
FR31 Handling uncertainty of disruptions	DP31 system resourcefulness
FR32 Evaluate system resilience in long-term period	DP32 Time-variation in system/component resilience
FR33 Evaluate redundant capacity for uncertainty adaptation	DP33 System redundancy
FR34 Evaluate system functionality against multiple disruptions	DP34 System robustness
FR4 Evaluate rapidity of system recovery from disrupted state	DP4 Speed of System recovery
FR41 Estimate rapidity of failure identification	DP41 Elapsed time to failure detection
FR42 Estimate rapidity of initial system stabilization	DP42 Elapsed time to initial system stabilization
FR43 Estimate rapidity of final system recovery	DP43 Elapsed time to final system recovery
FR5 Evaluate effects of planning	DP5 Effects of Strategies
FR51 Evaluate effects of stakeholder decision	DP51 Stakeholder decision

	DP11	DP12	DP21	DP22	DP23	DP24	DP31	DP32	DP33	DP34	DP41	DP42	DP43	DP51
FR11	✓	○	○	○	○	○	○	○	○	○	○	○	○	○
FR12	✓	✓	○	○	○	○	○	○	○	○	○	○	○	○
FR21	○	○	✓	○	○	○	○	○	○	○	○	○	○	○
FR22	○	○	○	✓	○	○	○	○	○	○	○	○	○	○
FR23	○	○	✓	✓	✓	○	○	○	○	○	○	○	○	○
FR24	○	○	✓	✓	✓	✓	○	○	○	○	○	○	○	○
FR31	○	○	○	○	○	○	✓	○	○	○	○	○	○	○
FR32	○	○	○	○	○	○	○	✓	○	○	○	○	○	○
FR33	○	○	○	○	○	○	○	○	✓	○	○	○	○	○
FR34	○	○	○	○	○	○	○	○	○	✓	○	○	○	○
FR41	○	○	○	○	○	○	○	○	○	○	✓	○	○	○
FR42	○	○	○	○	○	○	○	○	○	○	✓	✓	○	○
FR43	○	○	○	○	○	○	○	○	○	○	✓	✓	✓	○
FR51	○	○	○	○	○	○	○	○	○	○	○	○	○	✓

1.2 Risk and Resilience

Risk is a common term encountered with power system resilience, and had earlier been used interchangeably [12]. However as in (1.1), risk is a function of threat, which could be adversarial and intentional or otherwise, that leverages vulnerability. Since threat occurrence can be assumed certain and beyond the control of the system operator, the operator would aim to take actions that minimize adversary impact or minimize system vulnerabilities to threats, in order to reduce risk. These actions function to strengthen the system and herein tie back to system resilience.

$$\begin{aligned}\text{Risk} &= Likelihood \times Impact\\ \text{Likelihood} &= Threat \times Vulnerability\\ \text{Threat} &= Capability \times Intent\end{aligned} \tag{1.1}$$

The relationship between risk and resilience can be envisaged as color coded in Fig.1.2. The impact can be seen as the “dip” in the resilience trapezoid, and hence reducing this “dip” minimizes risk and improves resilience.

1.2.1 Risk and Situational Awareness

A goal of risk assessment is to aid situational awareness, which is defined as the perception of the elements in an environment within a volume of time and space, the comprehension of their

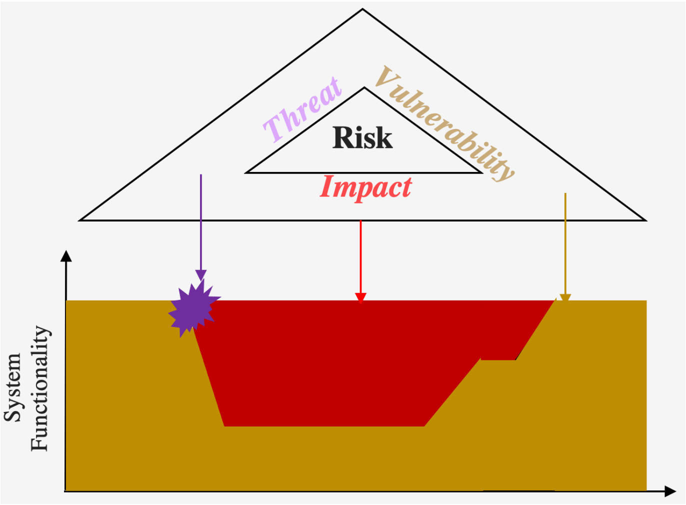


Figure 1.2: Relating Resilience and Risk. As the power system carries out its functionalities, several inherent vulnerabilities exist (in the yellow area), and can be leveraged by an adversary via threat capabilities (purple event), to impact the system (the red area).

meaning and a projection of their status in the near future [13]. Hence, situational awareness implies spatio-temporal observation and forecast/ prediction/ estimation of a system's state. In power systems, this can be near real-time as in power systems operations or longer, towards planning. Hence, situational awareness involves the recognition of system elements that inform the system state and enable effective power system response. For instance, perception of system states would include: generation, transmission, distribution data, schedules for load and market, device (e.g., switch, breaker, bus, relay) status, environmental and atmospheric conditions.

Therefore, the comprehension of these perceptions would include: analyzing and understanding the resulting deviation between the expected (estimated) vs. current state of the system, system capabilities and vulnerabilities, possible actions and operator responses. The implication here is that within this comprehension of the perceived state lies risk assessment. The projection of this understanding is the inference of future system state and the time criticality of operator response. These characteristics of SA can be seen as a cycle in power systems where projecting the future system states would lead to further perception of that future "projected" state as illustrated in Fig. 1.3. Similarly, to aid decision making in risk situations, SA models like the Observe, Orient,

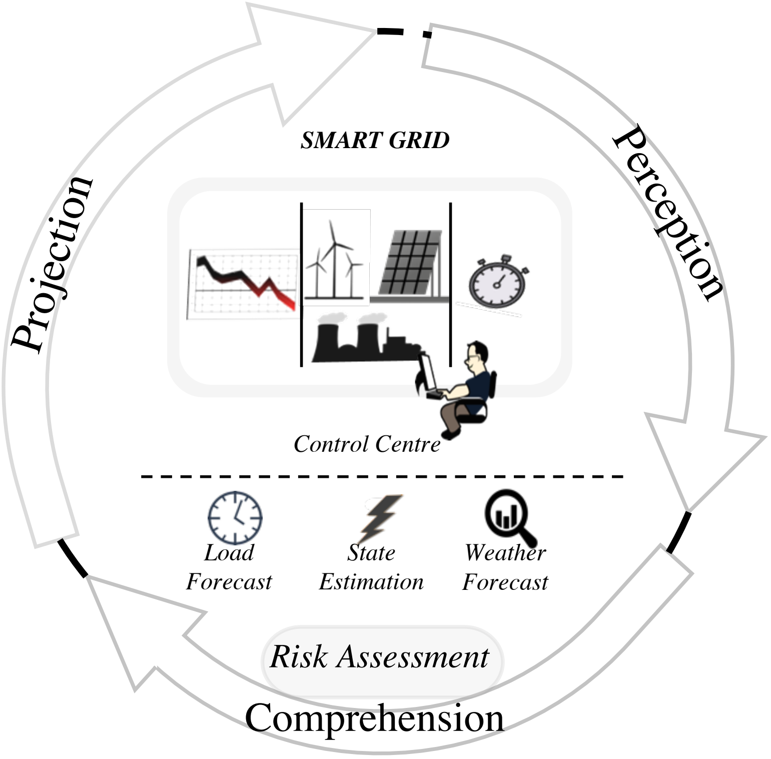


Figure 1.3: The Situational Awareness Cycle

Decide, Act (OODA) loop were developed [14]. However, for resilience, the SAAL—Sensing, Anticipating, Adapting, and Learning model expands on the OODA to emphasize the nuance that resilience additionally requires the ability to anticipate and learn [15].

1.2.1.1 State Estimation in Power Systems

Power System State Estimation (PSSE) is a technique that informs situational awareness by collecting data from the bulk power grid, in a process to estimate the electrical state of a network by eliminating inaccuracies and errors from measurement data, and analysing the data to minimize risk. The PSSE's objective is to estimate system state $\boldsymbol{x}$ by minimizing the following function:

$$\hat{\boldsymbol{x}} = \min_{\boldsymbol{x}} (\boldsymbol{z} - h(\boldsymbol{x}))^T \boldsymbol{R}^{-1} (\boldsymbol{z} - h(\boldsymbol{x})), \tag{1.2}$$

where $\boldsymbol{x}$ is the state vector which will have the form $\boldsymbol{x}^{\tau} = [\theta_2, \theta_3, \cdots, \theta_N, V_1, V_2, \cdots, V_N.]$ when bus 1 is the slack bus, $\boldsymbol{z}$ represents measurements/observations from field devices consisting of active and reactive power injections at buses (P_i, Q_i) and active and reactive power flows on branches (P_{ij}, Q_{ij}) [16]. P_i and Q_i at bus i is given as:

$$\begin{aligned} P_i &= \sum_{j \in \Omega_i} V_i V_j (G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij}) = P_{Gi} - P_{Li} \\ Q_i &= \sum_{j \in \Omega_i} V_i V_j (G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij}) = Q_{Gi} - Q_{Li} \end{aligned} \tag{1.3}$$

The P_{ij} and Q_{ij} from bus$i$ to bus$j$ is:

$$\begin{aligned} P_{ij} &= V_i^2 (g_{si} + g_{ij}) - V_i V_j (g_{ij} \cos\theta_{ij} + b_{ij} \sin\theta_{ij}) \\ Q_{ij} &= -V_i^2 (b_{si} + b_{ij}) - V_i V_j (g_{ij} \sin\theta_{ij} - b_{ij} \cos\theta_{ij}). \end{aligned} \tag{1.4}$$

Therefore, if the estimated state of the system derived from system status measurements deviates from expectations, the power system utilizes bad data detection (BDD) to identify bad (erroneous) measurements, which could have sourced from power grid threats.

1.3 Threats to the Power Grid

A crucial type of threat to characterize and defend in the critical power grid is the type of threat that presents operational impact and threat to reliability. Specifically, for state estimation attacks, this could appear as false data that drives the deviation of grid operating points, as much as possible, from normal. The power grid is vulnerable to threats from a myriad of sources. The vulnerability of the grid can arise from aging infrastructure, which when combined with increasing power demand, makes the grid susceptible to faults and failures e.g., cascading failures, as has been witnessed during periods of harsh weather. Hence, modernizing the grid has become a high priority for the U.S. Congress and industry [17].

Modernization, however, incorporates the integration of a continually growing network of hardware and software which redefine and increase the attack surface, favoring grid adversaries. This creates a new reality which is that most grid components operate in internet-accessible digital environments. Operation in digital environments has shifted operational technology towards increasingly allowing external connections and remote access to business networks, which could lead to threat actors accessing the systems to disrupt operations. For instance, the distribution grid operation using Internet of Things (IoT) could be compromised by adversaries where devices can be manipulated and used to launch coordinated demand-side attacks. Furthermore, the modern grid integrates widely available devices, which use traditional networking protocols for controlling grid components. This can further increase the threat surface for the grid, e.g., Phasor Measurement Units (PMUs) which are dependent on GPS timing to monitor grid state towards control of generation, transmission, and distribution functions, can be attacked and desynchronized.

Reported cyber events have increased, and suspicious activity with unidentified causes which can be physical or cyber attacks, have increased as well. In April 2021, the Colonial pipeline attacks affected roughly 45% of the East Coast's supply of energy resources [18]. The University of Cambridge posits that cyber-related incidents to the grid has cost the United States an upwards of \$243 - \$1000 billion [19]. According to [20], the purpose of a cyber attack on a SCADA system could range from a hacker trying to access and scale through system defenses, to an adversary possibly generating "false" information to the SCADA system for espionage. In this dissertation, we focus our studies on risk reduction to the cyber threats of adversary intrusion and false data injection attacks.

Threats to the grid can also be physical. These can be due to vandalism or attacks from local nation state adversaries to power plants and substations. This, according to The North American Electric Reliability Corporation (NERC), calls for a risk-based approach [22]. Physical threats can also include existential threats from weather-based events such as hurricanes, tornados, wildfires, and floods, that have devastating impacts on the power grid. The response to these events have been led by the Department of Homeland Security's (DHS's) emergency response organization, Federal Emergency Management Agency (FEMA). As shown in Fig. 1.4, the top threats that have affected the U.S. grid which have generally increased over the past couple of years. Severe weather can be

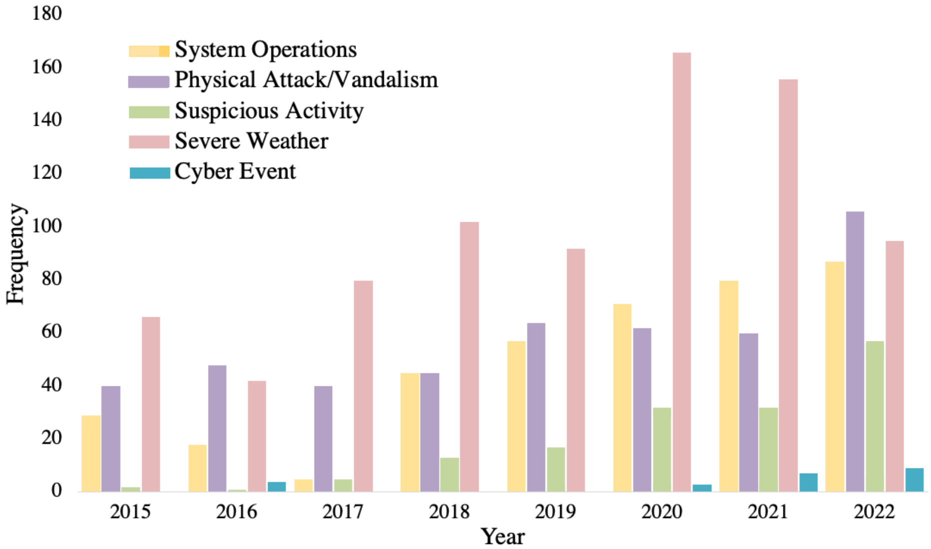


Figure 1.4: Top threats to the U.S. power grid based on data from [21].

seen to be the most frequent and also the most impactful [21]. Extreme weather conditions are the most common cause of energy disruptions in the U.S. where major power outages from weather related events in the U.S. increased by approximately 67% since 2000 [23]. In June 2021, unusual high summer temperatures caused record-high demands to the Texas grid putting the grid under enormous pressure. On a similar note, February 2021 saw extreme cold weather conditions lead to a winter storm which destabilized the Texas power grid, causing millions of people to lose power for multiple days in the freezing temperatures thus leading to 702 deaths [23]. Wildfire threats, as shown in Fig. 1.5, cause increasing widespread impact to the power grid. The impact ranges from increasing acres burnt, to loss of lives and property, bankruptcy of utilities, law suits against utilities, lost opportunity costs, and significant costs on the federal, state, local, and territory levels.

1.3.1 Cyber Threats of Adversary Intrusion

The modernization and hence, digitization of utility networks which has also expanded to commercial services and external-facing websites, such as corporate and vendor websites, exposes the power network to threats of adversary intrusion from these internet-facing hosts. According to an

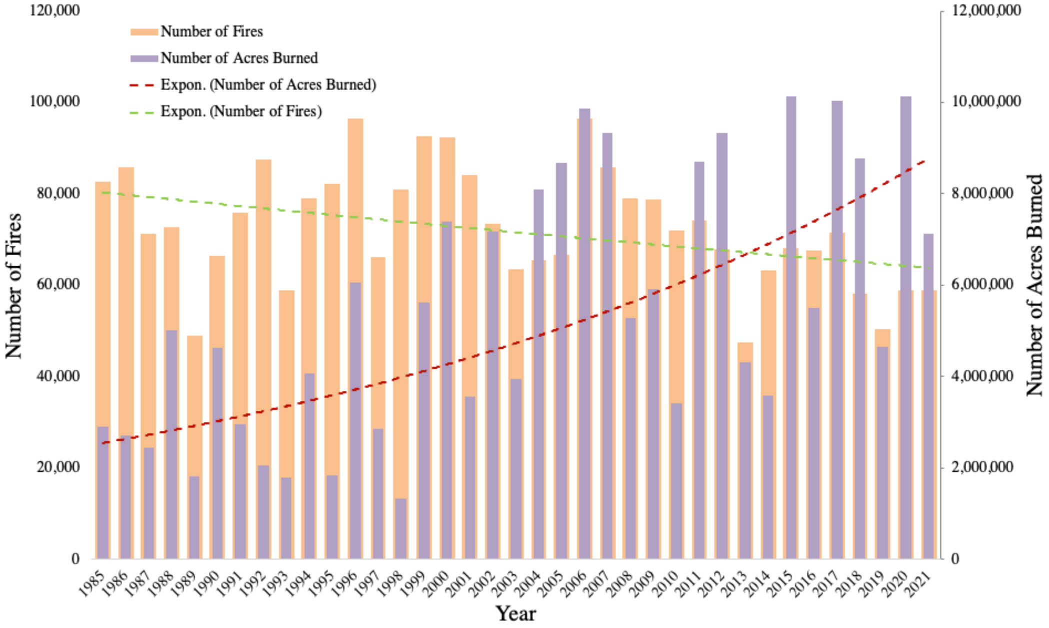


Figure 1.5: Wildfire threat in the United States: frequency, severity and impact, based on data from [24]

independent study carried out by Fortinet, a major problem in SCADA is the complete access often granted to third party organizations, such as vendors, to internal systems [25]. As illustrated in Fig. 1.6, 64% of organizations grant third-party vendors either complete access with no restrictions or high-level access with very few restrictions, to their SCADA/ICS systems. This level of trust and access granted to these third party organizations, business partners, and government organizations, can expose the system to threats of adversary intrusion from these external-facing access points. Hence, from a risk-based perspective, it is highly crucial for critical systems to analyze and access their risk to adversary intrusion that can arise from these sources.

In the cyber space, risk assessment to adversarial threats can be aided by information and frameworks provided by several organizations and agencies. Such agencies include the National Institute of Standards and Technology (NIST) which provides voluntary guides and practices aimed at cultivating trust in Information Technology (IT), and the transition between IT and Operational Technology (OT). The MITRE Corporation is a non-profit and independent adviser that aims to advance national security by providing globally accessible knowledge base of adversary tactics and techniques from real-world observations [26]. Additionally, the National Vulnerability Database (NVD) is the U.S. government repository of standards based vulnerability management data [27], enabling automation of vulnerability management, security measurement, and compliance. The Common Vulnerability Scoring System (CVSS) scores for the Common Vulnerabilities and Exposures (CVE) obtained from the NVD, which is part of NISTS's Security Content Automation Protocol, is formally adopted as an international standard for scoring vulnerabilities. For instance, an attack source vertex may leverage knowledge of required username and password to remotely access another sink vertex with hard-coded SSH credentials by exploiting vulnerability `CVE-xxxx-xxxx` with a score computed using the impact and exploitability subscores [28]. The impact subscore is calculated based on the impact of Confidentiality, Integrity, and Availability, where Confidentiality is the limitation of information access to authorized users and preventing disclosure to unauthorized users, Integrity is the veracity of information, while Availability is the accessibility of information resources or node functionality. The exploitability subscore is calculated based on the attack vector, the attack complexity, the privilege required to execute such attack, and the user interaction as well. Hence, this knowledge base is useful for risk assessment

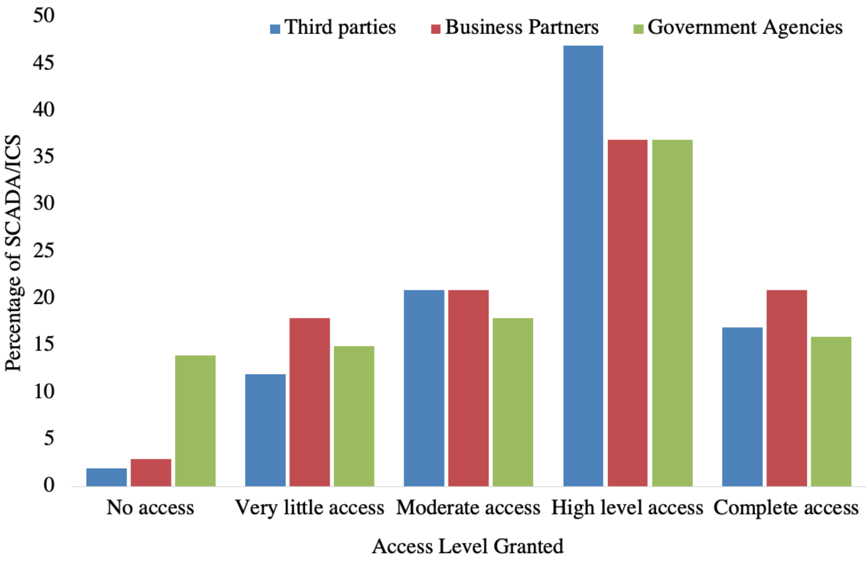


Figure 1.6: Percentage of organizations: access level granted third parties to SCADA/ICS based on data from [25].

to known vulnerabilities giving the ease of exploitation of such vulnerability and it's impact to the system as discussed.

1.3.2 Threats of False Data Injection to SCADA

When an adversary completes a successful intrusion, there are several threats that the adversary poses to the power system operation. To impact power systems operation, the adversary aims to move the system state as much as possible from normal. To achieve this, the adversary can compromise the communication between sensory/measurement and control devices to inject false information. The false information could be false data from the field measurement devices/sensors, or false command to the control devices, and is referred to as False Data Injection Attacks (FDIA). FDIA will then misinform the system operator, and lead to operational actions which can be detrimental to the power grid.

The objective of the adversary in an FDIA is to create a new measurement vector of sensor readings from field devices in a stealth way such that undetectable errors, that can bypass the BDD, are introduced into the calculations of variables and values used in power system state estimation as in section 1.2.1.1. Mathematically, the FDIA can be represented as in equation (1.5).

$$\begin{aligned} \boldsymbol{z_o} &= h(\hat{\boldsymbol{x}}), \\ \boldsymbol{z_a} &= \boldsymbol{a} + \boldsymbol{z_o} = h(\check{\boldsymbol{x}}), \end{aligned} \tag{1.5}$$

where $\hat{\boldsymbol{x}}$ and $\check{\boldsymbol{x}}$ denote the estimated (original) state vector and false data injected state vector, and $\boldsymbol{z_o}$ and $\boldsymbol{z_a}$ stand for the original and attacked measurements, respectively, and $\boldsymbol{a}$ represents the attack vector which can be any of the following: 1.) Deletion of data from $\boldsymbol{z_o}$, 2.) Change of data in $\boldsymbol{z_o}$, 3.) Addition of fake data to $\boldsymbol{z_o}$.

1.3.3 Power Grid Resilience to Wildfire Threats

Wildfires are natural- or power equipment-caused HILF events that threaten power grid resilience. This realization not only leads to increasing severe economic impact via direct/indirect costs from firefighting [24] as shown in Fig.1.7, infrastructure damage (critical infrastructure such

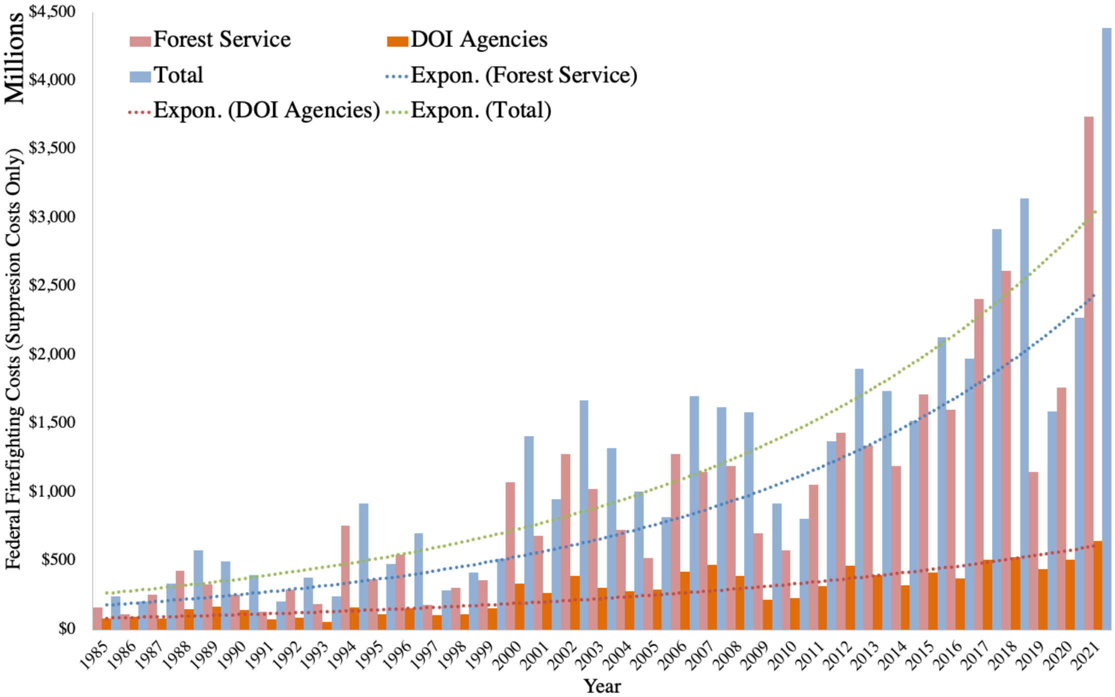


Figure 1.7: Federal economic impact of wildfire suppression costs.

as healthcare, water, gas, power generation dams), lost opportunity costs from public safety power shutoffs, business interruption costs etc., but as well leads to severe social impact including loss of lives and property, manslaughter lawsuits from customers against utilities, and lack of trust from customers to service area utilities. The California Department of Forestry and Fire Protection estimates the dollar cost of wildfires to property owners, taxpayers, and critical utilities, increased by up to 300% over the past decade [29]. In the United States, the annualized economic burden from wildfires is estimated up to $347.8 billion [30]. In 2018 alone, California's wildfires cost the US economy about $148.5 billion which is approximately 1% of the entire United States annual GDP.

The wildfire-power system interaction can be visualized as shown in Fig.1.8, from the power generation level to the transmission and distribution levels. Several studies have captured different aspects of the wildfire power operational strategies and impact of wildfires on transmission and distribution grids [31–34]. The resilience of power systems to wildfires has also been studied [35–37]. In our work, we propose and hence introduce the wildfire resilience trapezoid as

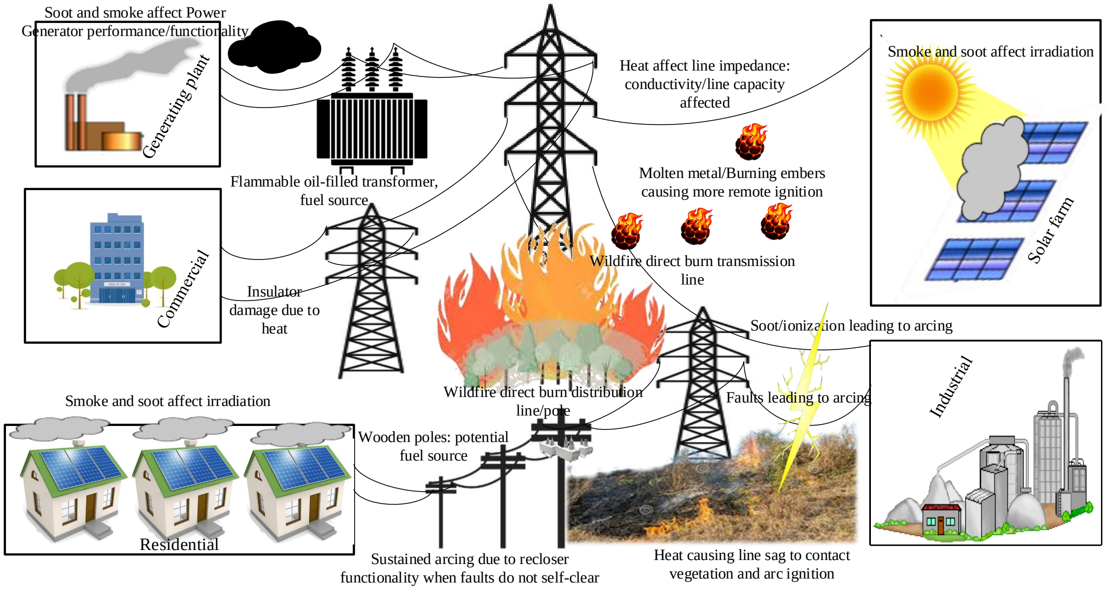

Soot and smoke affect Power Generator performance/functionality
Generating plant
Flammable oil-filled transformer, fuel source
Heat affect line impedance: conductivity/line capacity affected
Smoke and soot affect irradiation
Solar farm
Molten metal/Burning embers causing more remote ignition
Commercial
Insulator damage due to heat
Wildfire direct burn transmission line
Soot/ionization leading to arcing
Wildfire direct burn distribution line/pole
Faults leading to arcing
Industrial
Smoke and soot affect irradiation
Wooden poles: potential fuel source
Residential
Sustained arcing due to recloser functionality when faults do not self-clear
Heat causing line sag to contact vegetation and arc ignition

Figure 1.8: Illustrating the power system-wildfire interaction.

illustrated in Fig. 1.9, to comprehensively capture the different phases in which the power system lies before, during, and after wildfire threats/events. It also defines power system preventive, corrective, restorative, and adaptive actions utilized in each of these phases comprising the planning phase in which stakeholder take decisions on the structural attributes, such as grid hardening actions, that boost robustness of the grid and hence improve wildfire resilience. The wildfire analysis phase comprises of the preventive actions, such as vegetation management, that are preparatory and taken towards mitigating wildfire threats. When a wildfire threat is active, certain more stringent measures, e.g., public safety power shutoff, are taken in order to ensure that power equipment do not serve as ignition sources, nor aid to exacerbate the potential fire. When the threat of wildfires is realized, the stakeholders make further decisions towards firefighting which could include "Let-burn" strategies where power systems let a wildfire burn and rebuild infrastructure as opposed to more expensive fire fighting efforts. From when the wildfire threat is active to when the wildfire is suppressed is referred to as the wildfire progression phase. After suppression, post wildfire restoration and adaptation towards better system planning for improved wildfire resilience, follows.

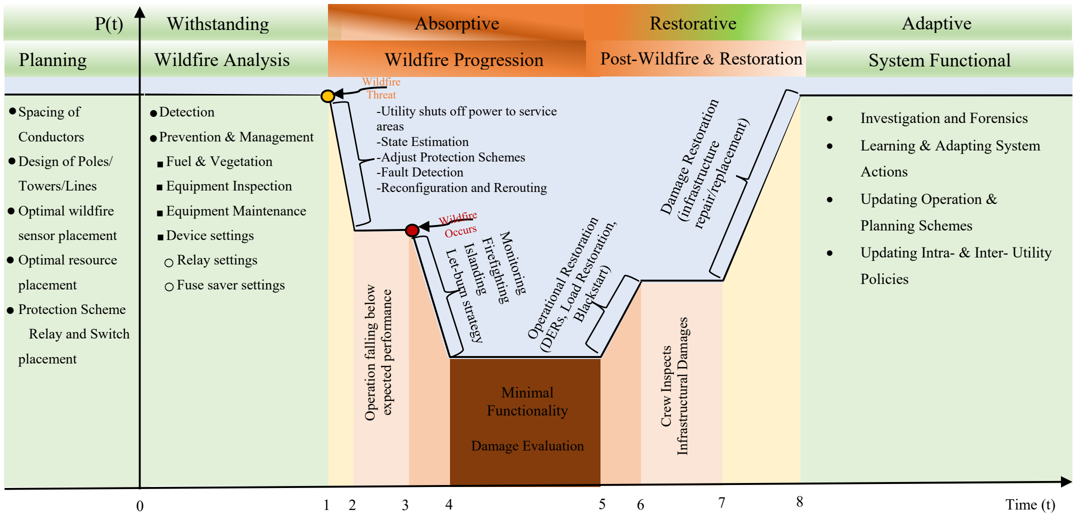

P(t)
Withstanding
Absorptive
Restorative
Adaptive
Planning
Wildfire Analysis
Wildfire Progression
Post-Wildfire & Restoration
System Functional
● Spacing of Conductors
● Design of Poles/ Towers/Lines
● Optimal wildfire sensor placement
● Optimal resource placement
● Protection Scheme Relay and Switch placement
● Detection
● Prevention & Management
■ Fuel & Vegetation
■ Equipment Inspection
■ Equipment Maintenance
■ Device settings
○ Relay settings
○ Fuse saver settings
Wildfire Threat
-Utility shuts off power to service areas
-State Estimation
-Adjust Protection Schemes
-Fault Detection
-Reconfiguration and Rerouting
Wildfire Occurs
Monitoring
Firefighting
Islanding
Let-burn strategy
Operational Restoration (DERs, Load Restoration, Blackstart)
Damage Restoration (infrastructure repair/replacement)
Operation falling below expected performance
Minimal Functionality
Damage Evaluation
Crew Inspects Infrastructural Damages
• Investigation and Forensics
• Learning & Adapting System Actions
• Updating Operation & Planning Schemes
• Updating Intra- & Inter- Utility Policies
0
1
2
3
4
5
6
7
8
Time (t)

Figure 1.9: The power system's wildfire resilience trapezoid. Performance $P(t)$ at different time phases, where the system is in normal performance until there is a wildfire threat (time 1) and the performance degrades to P(2) with preventive actions such as public safety power shutoff. With a wildfire ignition, there is further degradation in performance to P(4), where the system remains in a degraded state until wildfire is contained and restoration towards normal performance begins.

1.4 Contributions

This work proposes techniques to reduce the risk that accrues to the critical cyber-physical power system resulting from top cyber and physical threats. On the cyber side, the work presented in this dissertation follows the adversary process as a complete loop from adversary intrusion into the power system network to the realization of the adversary objective of injecting false data to deviate the system from normal operation. Hence, the techniques proposed reduce the system risk from adversary intrusion to attack realization. Furthermore, the work contributes a novel method for power systems towards automating the risk assessment process through the design and development of an emulation tool that automatically rebuilds the utility network in a virtual environment, allowing for several use cases that improve system resilience. On the physical threats, the work focuses on the high impact threat of wildfires which have plagued critical infrastructure on the territory, local, state, and federal levels. It proposes a spatio-temporal data-driven technique in modeling wildfire threats, better suited for risk reduction for the bulk power grid. Furthermore, the work presented in the dissertation designs and develops an important tool that comprehensively meets resilience needs in the (pre-event, event progression, and post event) pipeline of critical infrastructure response to the severe threat of wildfires.

1.5 Dissertation Outline

1.5.1 Cyber-Physical Component Ranking for Risk Sensitivity Analysis using Betweenness Centrality

Given the threat of adversary intrusion, this chapter proposes a framework for critical component ranking in power system risk analysis, which generates graphs of potential attack paths and traverses generated attack graphs to rank components according to their importance in reducing adversary impact on the power system. The framework proposes a metric which extends upon betweenness centrality and integrates into risk analysis, the services and security cost of communications between power system components, and the likelihood of component exploitation as an adversary medium to the target relays. The publication outcomes of this chapter are given below:

J1. Umunnakwe A, Sahu A, Narimani MR, Davis K, Zonouz S. Cyber-physical component ranking for risk sensitivity analysis using betweenness centrality. IET Cyber-Physical Systems: Theory & Applications. 2021 Sep;6(3):139-50.

C1. Umunnakwe A, Sahu A, Davis K. Multi-Component Risk Assessment Using Cyber-Physical Betweenness Centrality. In 2021 IEEE Madrid PowerTech 2021 Jun 28 (pp. 1-6). IEEE.

1.5.2 Graph Neural Networks Based Detection of Stealth False Data Injection Attacks in Smart Grids

Given that adversary has completed intrusion and thus poses a false data injection threat, we propose a Graph Neural Network (GNN) based FDIA detection model for smart power grids. We automatically represent the underlying graph topology and spatially correlate the smart grid measurement data to detect and hence, mitigate the risk associated with stealth cyber attacks, by raising alarms to the power system operator. Hence, the proposed GNN-based detection model is scalable and detects FDIAs in real-time by efficiently combining model-driven and data-driven approaches that incorporate the inherent physical connections of modern AC power grids and exploiting the spatial correlations of the grid measurements.

The publication outcome of this chapter is given below:

J1. Boyaci O, Umunnakwe A, Sahu A, Narimani MR, Ismail M, Davis KR, Serpedin E. Graph neural networks based detection of stealth false data injection attacks in smart grids. IEEE Systems Journal. 2021 Oct 20;16(2):2946-57.

1.5.3 OpenConduit: A Tool for Recreating Power System Communication Networks Automatically

The daily operations of critical infrastructures have long relied on computer networks, and often incorporate legacy devices and protocols with limited security functions. To study the risk associated with these systems, their architectures have to be replicated in a safe test environment. This chapter introduces the implementation of OpenConduit, a tool that automatically rebuilds and realistically replicates electric power system networks in an emulation environment in order to accurately and scalably automate risk studies. The objective targets the creation of the critical infrastructure's digital twin that enable use cases which improve resilience and enable risk reduction. Potential use cases enabling the tool's utility are also presented.

The publication outcome of this chapter is given below:

C1. Umunnakwe A, Wlazlo P, Sahu A, Velasquez J, Davis K, Goulart A, Zonouz S. OpenConduit: A Tool for Recreating Power System Communication Networks Automatically. In2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) 2022 Oct 25 (pp. 141-147). IEEE.

1.5.4 Data-Driven Spatio-Temporal Analysis of Wildfire Risk to Power Systems Operation

This chapter presents the resilience-oriented risk reduction to physical wildfire threats. Here, we propose a two-stage framework for assessing power system-wildfire risk using a data-driven model to predict wildfires which threaten portions of the transmission and distribution grid. The first stage of the framework estimates the spatio-temporal probability of potential wildfire ignition and propagation using a deep neural network (DNN) in combination with the wildfire physical spread model. The second stage assesses the wildfire risk in the power grid operation in terms of potential loss of load by de-energization, through combining geospatial information system data of the power grid topology and the stochastic spatio-temporal wildfire model developed in the first stage.

The publication outcomes of this chapter are given below:

J1. Umunnakwe A, Parvania M, Nguyen H, Horel JD, Davis KR. Data-driven spatio-temporal analysis of wildfire risk to power systems operation. IET Generation, Transmission & Distribution. 2022 Jul;16(13):2531-46.

C1. Umunnakwe A, Davis K. A Modeling Approach to Quantify Wildfire Risk in Power Systems Operations Using Data Availability and Deep Learning Techniques. In2022 IEEE Power & Energy Society General Meeting (PESGM) 2022 Jul 17 (pp. 1-5). IEEE.

1.5.5 A Self-Sufficient Low-Cost Mitigation Model to Improve Resilience in Power Utility Wildfire Response

This chapter builds on the previous one to present a coordinated risk management and comprehensive approach to improve resilience and economics in power utilities' wildfire response before, during, and after wildfires. The proposed self-sufficient low-cost wildfire mitigation model (SL-PWR) also detects and localizes wildfire occurrence, spread, and other wildfire-related using optimized artificial intelligence techniques. The SL-PWR's comprehensive nature informs power system resilience at the different phases of the resilience trapezoid, utilizing spatio-temporal wildfire potential probability maps, equipment layer information (e.g., equipment aging), vegetation layer information (e.g., vegetation-fuel correlation), and optimized UAV monitoring trees to obtain input images for training. The SL-PWR wildfire mitigation tool is the first of its kind that achieves effective response strategies, and rapidity via automation, in the complete pipeline from pre-wildfire, to wildfire progression, to restoration/recovery and adaptation. Results show that SL-PWR improves situational awareness and resilience during extreme threats to several critical infrastructure, primarily power grids.

The outcomes of this chapter are given below:

J1. Umunnakwe A, Davis K. A Data-Driven Automated Mitigation Approach for Resilient Wildfire Response in Power Systems. Submitted to the IEEE Open Access Journal of Power and Energy.

J2. Umunnakwe A, Davis K. An Optimization of UAV-Based Remote Monitoring for Improving Wildfire Response in Power Systems. Submitted to the IEEE Open Access Journal of Power and Energy.

1.5.6 Economic Analysis and Return on Investment: A Self-Sufficient Low-Cost Mitigation Model to Improve Resilience in Power Utility Wildfire Response

This chapter presents the detailed analysis of the economic viability, diverse functionality and utility of the proposed SL-PWR, and it's deployment advantages with respect to utility methods and existing wildfire mitigation tools. We conduct return on investment (ROI) of the SL-PWR model as opposed to conventional utility methods based on some economic benefits provided by the SL-PWR amongst many such as social benefits, environmental sustainability, operational/technical benefits, etc.

2. CYBER-PHYSICAL COMPONENT RANKING FOR RISK SENSITIVITY ANALYSIS USING BETWEENNESS CENTRALITY [*]

This chapter focuses on reducing the risk of the power system to the threat of adversary intrusion. According to Joy Ditto, president and CEO of Utilities Technologies Council, “In the face of imperfect protections, ... it comes back to how much situational awareness you have around your network, and if you know that you are going to have vulnerabilities but you can limit them or you can at least be aware when those vulnerabilities are being exploited, that is a good place to be” [39]. This chapter employs this strategy and enables risk reduction via a protection strategy by system topology and vulnerability impact awareness.

2.1 Introduction

Cyber threats can lead to data breaches, asset damage and power outages by exploiting control assets in the physical grid. As interactions between cyber and physical layers increase, the potential paths which a system adversary can exploit to reach critical devices also increase, making comprehensive monitoring more intractable for the system operator; this can have the unintended consequence of the grid becoming a target for cyber attacks [40]. In order to be prepared for these anomalies, the system operator usually performs contingency analysis as a risk monitoring tool to provide situational awareness of the power grid [41]. Different methods have been proposed to analyze power system risk to adversarial attacks. Researchers in [42,43] initially presented the concept of cyber-physical contingency analysis to identify high-risk elements using techniques based on Markov Decision Processes as well as reachability analysis of attack paths [44] and quantifying physical impact in power systems. Graph theory based analysis can be utilized to improve this cyber-physical contingency analysis by analyzing the system as a weighted graph, where priority can be assigned to edges/vertices with the most connection paths passing through [45]. Using the

[*] ©[2021] IET. Reprinted, with permission from, Sahu A, Davis K, Huang H, Umunnakwe A, Zonouz S, Goulart A., “Cyber-physical component ranking for risk sensitivity analysis using betweenness centrality,” in IET Cyber-Physical Systems: Theory & Applications, vol. 6, pp. 139-50, Sep 2021, doi:https://doi.org/10.1049/cps2.12010 [38].

graph theory approach, [46] estimates the impact of the cyber layer on the physical system through cost-effect analysis. In [47], graph multi-centrality features are utilized to detect attacks on the network. These measures can also be adapted to power system networks, using graph topology to detect anomalies in electric power grids [45, 48]. In [49], centrality and electrical characteristics are utilized to identify critical vertices. In [50], effective graph resistance is used as a metric to assess the robustness of power grids against cascading failure by identifying the best pair of connectivity vertices, while in [51], the authors rank the importance of the grid vertices and lines based on centrality measures and other characteristics.

In most of these power system risk studies, physical/electrical characteristics are investigated, while cyber vulnerabilities are not integrated. Communication networks can be penetrated through external connections, internal internet hosts, virus penetration, and more. Specifically, although the OT network is isolated from the IT by firewalls and DMZs, a collection of vulnerable web and remote access services can still be exploited to plant malware or worms [52].

Given the successful modeling of the cyber-physical power system in previous chapters, this chapter develops a cyber-physical risk assessment model that ranks cyber and physical components in the power system in order of importance towards minimizing adversary impact. This work is motivated by the nature of attacks [53, 54], which compromise control assets to create havoc. Thus, the work focuses on the adversarial process from the operators' host computers (e.g. via phishing emails) to the control network (relays). Rather than ranking discovered vulnerability by severity [55], the proposed model considers that the operator wants to rank the system components by importance toward reducing total system vulnerability. Furthermore, the model integrates the likelihood and cost of adversary exploitation [56] into cyber-physical risk analysis. As shown in Fig. 2.1, the proposed risk model utilizes the system connectivity, topology information, and user defined adversary and target component lists to generate attack graphs. Given the attack graphs, component ranking follows with detailed vulnerability scores (cost) of network communication links and the betweenness centrality of components (vertices), thus demonstrating the relative ease of compromising a communication link and the ease of reaching target assets from unique vertices.

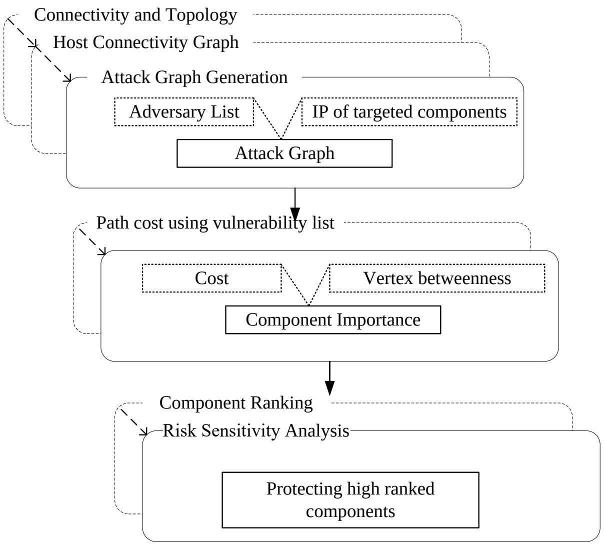

Connectivity and Topology
Host Connectivity Graph
Attack Graph Generation
Adversary List
IP of targeted components
Attack Graph
Path cost using vulnerability list
Cost
Vertex betweenness
Component Importance
Component Ranking
Risk Sensitivity Analysis
Protecting high ranked components

Figure 2.1: The proposed Component Ranking and Risk Sensitivity Analysis Model (CRSA).

The proposed model makes use of information flow, such as services and processes among system components, where the information flow and connectivity of the network are traced at a time when the system is in normal operation. Points of adversary intrusion are then modeled as hosts through which target relays may be reached after a series of vulnerability exploitation. Based on the results of the proposed approach, we demonstrate component protection to reduce overall system vulnerability.

The main contributions of this chapter are as follows.

- We propose a *component ranking and risk sensitivity analysis model* which integrates the cyber-physical network topology and standard industry vulnerabilities to model attack and defense from adversary and system operator perspectives simultaneously.

- We propose a cyber-physical betweenness centrality (CPBC) metric, that enables security-oriented risk awareness by ranking system assets according to their security tiers. We compare the proposed CPBC with the existing Betweenness Centrality (BC) metric to further illustrate attainable CRSA improvements.

- We develop an algorithm to protect critical components, while scalability is also illustrated using the Cyber-physical Situational Awareness (CyPSA) test systems.

2.2 Cyber Vulnerability Modeling

It is unlikely that an adversary will have access to all information required to carry out an attack on the power system, however, as with all high impact low probability events, the event probability approaches 0 until the event occurs and the probability is 1. Hence, in this model we expect that the adversary will inevitably gain system access while the system operator takes contingency measures to minimize adversary impact. We assume that the adversary will prioritize easily accessible paths which pose high impact on the system (e.g., access to more critical relays). Therefore, the adversary has access to the power grid topology information [57] and can carry out an attack based on component vulnerability and graph theory [58].

2.2.1 Attack Graph Generation

The goal of the attack graph is to provide details about the cyber-physical power network through dependencies among system components. The attack graph informs the current state of the system as well as the potential paths an adversary could take to reach target components given the possible points of intrusion, as adapted from Algorithms 2 and 3 detailed in [59], and is generated from the system connectivity and topology information.

2.2.1.1 The Connectivity Matrix

Attack graphs are generated using system connectivity matrix (CM) with pre-defined intrusion and target vertices. For realistic analysis, this work develops the CM from physical and cyber network interconnections of the synthetic CyPSA 8-substation model [60], which capture normal operation and communications, e.g., remote or secured shell (SSH) access.

2.2.1.2 Cyber Topology and Host Connectivity Generation

To generate the system topology and host connectivity, NMap generates a network mapping report which is spawned from control network hosts and provides host service details. The report is parsed using the NP-View application [61]. Based on the firewall's interface and object group configuration, NP-View generates the cyber topology as a JSON file having 2 primary features; `Device` and `Network` which have a list of all devices (hosts, relays, gateways with their IP address and unique ID), and a collection of the model's networks for the UCC, internet, vendor access and peer utility, respectively. The connectivity file is generated based on the access control list configured in each firewall [59].

2.2.2 System Vulnerability

The goal of this section is to explain the system security state. We assume that the adversary gains network access and will take a relative path of least resistance to reach relays in order to operate breakers. Ethernet connected relays may be discovered using port scanning tools such as NMap, and discovered relays can be identified using their IPs.

Connectivity characterization is stored in: 1) a source object; 2) a sink object; and 3) their security cyber cost (CC). A source and sink are vertices and may have more than one communication link (connectivity edge). For instance, an attack source vertex may leverage knowledge of required username and password to remotely access another sink vertex with hard-coded SSH credentials by exploiting the vulnerability `CVE-xxxx-xxxx` with a score, hence the path between the two vertices will be weighted on the cyber costs (CC) which are computed based on the Common Vulnerability Scoring System (CVSS) scores obtained from the National Vulnerability Database (NVD). Given these exploitable paths, the component ranking algorithm seeks to identify relatively easy access paths that the adversary can take to get to target assets. Once the paths are ascertained, vertices most common in these paths have high graph centrality and with consideration of their associated vulnerability types and scores, these vertices are noted as relatively critical for the adversary mission. The critical vertices (important components) are then sent to the system operator to be protected, as a collection of attacks can be prevented by patching system vulnerabilities. For instance, a Distributed Denial of Services (DDoS) can be avoided if vulnerable services or software are patched, uninstalled or filtered. Similarly, a Man-in-The-Middle (MiTM) attack targeting false command or data injection can be avoided, if an intruder is prevented from planting malware or creating botnets. We assume that once the critical component is protected, the service it provides is deterministically secure and available i.e. it becomes 100% secure.

2.3 Component Ranking Assessment

The cyber-physical network is a set of components that connect to one another for communication and/or control, and hence can be mathematically represented as a graph [62]. The ranking model is formulated given the cyber-physical attack graph G. The graph vertices represent system components such as hosts, routers, and relays. The edges represent links between the vertices e.g., service (ssh, tcp) running between two vertices. In particular, if data flows from object v_i to v_j, then object v_j becomes dependent on v_i and the dependency is represented by the network edge $e_{ij} = v_i \rightarrow v_j$. To capture this, we represent G as a pair of vertex and edge sets (V, E), with vertices, $V = \{v_1, v_2, v_3, ..., v_n\}$, and edges, $E = \{e_1, e_2, e_3, ..., e_m\}$ with individual weights $CC(e)$ $\rightarrow \mathbf{R}^+$.

2.3.1 Cyber-physical Interdependencies

Given the nature of historical attacks e.g., compromising operator computers to access control devices, our focus is on similar adversarial analysis. The cyber-physical interdependencies considered in this paper as follows:

- From one cyber vertex to another e.g., host-host, host-router link. This interdependency is the data flow or service between cyber vertices.

- From a cyber vertex to a physical vertex (relays), sending information/commands to relay.

2.3.2 Vertex Betweenness Centrality

Vertex betweenness centrality assigns ranking coefficients to vertices through which important components can be identified as those vertices with high coefficient values [63]. It gives insight to the influence of a vertex over the data flow between other vertices. Given the graph $G(V, E)$, the betweenness of a vertex v is the count of shortest paths between pairs of other vertices that run through v as below:

$$BC(v) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}}. \tag{2.1}$$

Equation (2.1) relies on the use of shortest path distance between the vertices which is computed using Dijkstra shortest path algorithm, where σ_{st} is the number of shortest paths from source vertex s to target vertex t, $\sigma_{st}(v)$ is the total number from the mentioned paths that pass through vertex v, and n is the number of vertices. Hence, vertices that occur on many shortest paths have relatively higher betweenness [51]. Different studies on cyber-physical vulnerability analysis using graph-theoretic algorithms including betweenness centrality, have been proposed towards contingency analysis [64]. However, utilizing just the BC metric for critical asset ranking in cyber-physical systems only takes into consideration the centrality positioning of a component in the network graph towards component importance, and hence less accurate results are often obtained.

To enhance accuracy in component ranking, we propose the CPBC for ranking system components towards risk assessment in the cyber-physical network. Specifically, the proposed metric incorporates the impending likelihood of components being compromised, directly or indirectly, in the attack graph as discussed in Section II. For instance, a vertex A, .e.g., an internet host, is affected directly by an adversary if he/she can successfully access that vertex via e.g., malicious emails. Alternatively, vertex B, e.g., a router, is indirectly compromised if it gets accessed by the adversary through A. In addition, the CPBC metric incorporates security vulnerability scores (CC) calculated as follows, using the lowest cost vulnerability to reach a particular vertex even though the attack graph retains all vulnerability IDs.

$$CC(e) = \min V_e \quad \forall e \tag{2.2}$$

We obtain vulnerability scores V_e from the NVD where the cost metric associated with realizing an attack edge is obtained from the CVSS with a script that extracts the exploitability sub-score using access complexity and authentication scores. The CC represents severity(operator-side)/vulnerability(adversary-side) of compromising a service between vertices.

2.4 Cyber-physical Betweenness Centrality Index

The objective of the CPBC index is to rank the cyber-physical power system components in order of protection importance to the power system operator. This importance stems from the potential adversary system impact through the compromise of a component given cyber-originated intrusions that target the introduction of malicious commands to relays through host computers in order to cause a physical-layer security event. In particular, the CPBC metric integrates the fact that important vertices have a greater chance to lie on multiple vulnerability-weighted shortest paths to the target relays, as illustrated in Fig. 2.2, while vertices with fewer services and lower CC will have relatively less importance. In Algorithm 1, the relative importance of a vertex due to its position in the network is obtained by defining internet and relay vertices as inputs. Then shortest paths from the possible adversary sources (internet) to targets (relay) are calculated. When these paths are obtained, the number of times a vertex occurs in these paths, $\sigma_{st}(v)$, can be determined. For the BC metric, this suffices for calculations as in equation (2.1), while the obtained $\sigma_{st}(v)$ is a

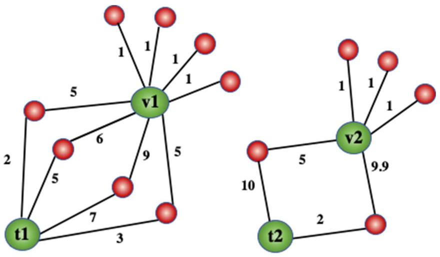


Figure 2.2: Visual aid for the cyber-physical betweenness centrality. The adversary at the red source vertices (with CC=1) will pass through $v1$ and $v2$ to get to their targets $t1$ and $t2$. As we observe, $v1$ provides about double the number of access paths from which the adversary can take the least cost path to $t1$. In addition, the cost of services associated with $v1$ is higher than $v2$ (29>17.9), hence it will cost more to the system operator if $v1$ is compromised. Thus, $v1$ will rank higher than $v2$, assuming they have same centrality in G.

Algorithm 1 Deriving Node Importance Given Betweenness Centrality in Attack Graph

```
Select IP of targeted relays, Physical_vertices
Select IP of Internet vertices, Cyber_vertices
function $node\_importance$(vertices)
    for relay in $Physical\_vertices$ do
        for host in $Cyber\_vertices$ do
            weighted shortest paths
            for short_path $S$ in $SPL$ do
                for $node$ in $vertices$ do
                    if vertex in short_path then
                        $unique\_node\_importance$ += 1
                    end if
                end for
            end for
        end for
    end for
return $node\_importance$, $\sigma_{st}(v)$,
end function
```

function of the proposed CPBC index, adequately capturing critical vertices:

$$CPBC(v) = \sum_{s\neq v\neq t\in V} \sigma_{st}(v) + \left(\varepsilon \times \frac{1}{\left(\frac{1}{\sum^{e_v} CC(e)} \right)} \right), \tag{2.3}$$

where $\sigma_{st}(v)$ is the number of shortest paths from source vertex s to target vertex t that pass through the vertex v with edges weighted on the communication link cyber costs, and e_v is the set of all edges to/from v, with cardinality of ε.

The key point is that this index performs risk analysis, allowing for models in which a vertex can be compromised without adversary having complete access to services being provided by that vertex since CC is summed for each compromised e_v. For instance, for the ranking of $v2$ in Fig. 2.2, the service represented by the edge with CC of 5 could be compromised with expected higher probability than that of CC 9.9, the CPBC index is formulated in such a way that this information

Algorithm 2 Asset Protection Using the Derived Cyber-Physical Node Importance

```
function $Generate\_Attack\_Graph, H$(G, L, sel_t)
    create empty $attackGraph, H$
    Get CC(e) (vuln_list) of $x$ ranked vertices
    for $vertex$ in $x$ do
        $v\_list$ = Get(vuln_list - y% of vuln_list)
        new_path = get_path($G$, $v\_list$)
        for adversary $a$ in $L$ do
            $d$,$p$ = djikstra_shortest_path($a$,$G$)
            for target $t$ in $d$ do
                if $t$ in $L$ then
                    $path$ = G($t$)
                    Add $path$ to $attackGraph, H$
                end if
            end for
        end for
    end for
return $new\_attackGraph, H$
end function
```

can be incorporated if so desired (e.g., if the model considered edges above a certain probability threshold to be compromised). In this case, if granular analysis of compromised vertex services is required, the CPBC index can also be utilized effectively. Another important advantage of this setup is that it allows for the grouping of vertices in security tiers with similar importance, and hence impact, on the overall system vulnerability. This will be further illustrated and discussed in our result analysis.

2.5 Model Evaluation: Risk Sensitivity Analysis

Risk sensitivity analysis proceeds with prioritized protection of ranked components while the impact of protection towards reducing the system's vulnerability is measured. The objective is to give the system operator enough information about the combination of components she chooses to protect in order to have a tractable number of possible adversary accessible paths in the case of an attack. As illustrated in Algorithm 2, the protection of the critical vertices follows with the removal of y% of the unique vertex's associated edges in the attack graph G. This generates a new attack graph, H, which is a sub graph of G, with number of attack paths less than or equal to

G. In particular, if a vertex is critical, it's protection should reduce the number of attack paths P accessible to the adversary.

The formulation of the protection algorithm is as follows. Let e_1 be the set of edges with links to a unique vertex $v1$ in the attack graph G, and e_{v1_c} be the set of edges with links to critical vertex $v1_c$ in the attack graph H. Then, the list of edges e_{v1_c}, associated with critical vertex $v1_c$, is defined as unique row entries with all but y% of the edges of the original set e_1, where $e_{v1_c} \in e_1 \in E$. Hence, within a row e_* (e.g., e_1, e_2,...) of E, the set of edges e_{y*}, from vertex $v*$ (e.g., $v1, v2$,...), not in e_{v*_c} is defined as:

$$e_{y*} = \frac{y}{100} \quad of \quad e_*. \tag{2.4}$$

This means that e_{v1_c} is a subset of e_1, where $y\%$ of the edges in e_1 are removed. So for $v1$,

$$e_{v1_c} = e_1 - e_{y1}. \tag{2.5}$$

Analysis for the new generated attack graph advances by calculating the impact of increased protection of important components on overall system attack paths as follows:

$$P_{Total} = \sum P(e_{v*_c}). \tag{2.6}$$

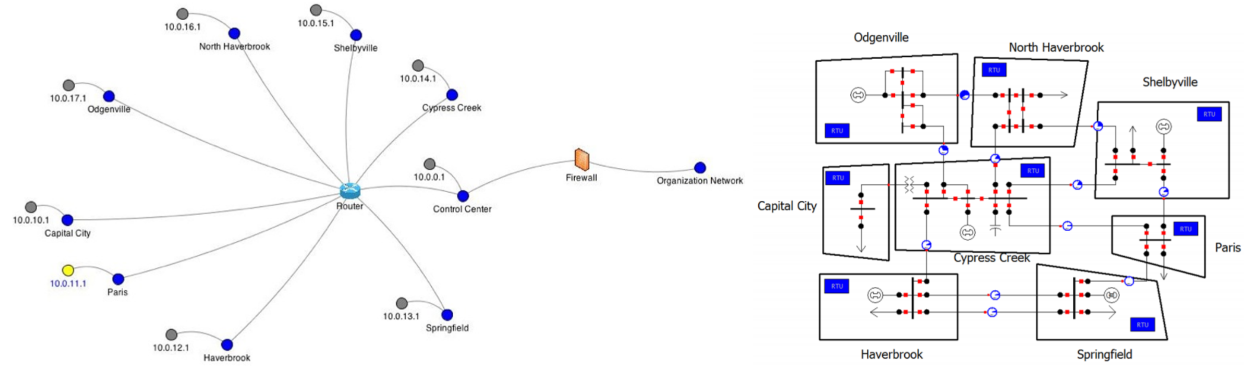


Figure 2.3: 8 substation cyber-physical test case [65].

Hence, equation (2.6) measures the improvement, i.e., reduction in paths accessible to adversary, of increased protection of critical vertices. This implies that protection of more critical vertices should relatively provide a higher improvement in overall system vulnerability with a reduced number of attack paths accessible to the adversary.

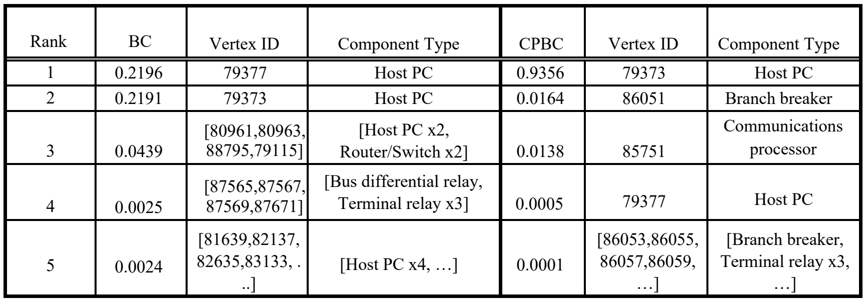
2.6 Simulation and Numerical Results

The CRSA model is implemented on the 8-substation test case, as shown in Fig. 2.3, and the extended cyber-physical IEEE 300 bus test cases with 78582 and 267762attack paths in G, respectively. These test cases are developed in our work [60] and publicly released with datasets for download [66]. The 300 bus test case is utilized to illustrate the computational complexity of the proposed model, as the case consists 4500 IP addressable devices with 1301 operational devices i.e., relays, and 2384 non-operational devices e.g., fault recorder, alarm systems, batteries. To illustrate the effectiveness of the proposed model, we consider the improvements offered by using the CPBC index in the risk sensitivity analysis compared to BC. The results are computed using a computer with an i7 1.80 GHz processor and 16 GB of RAM.

Table 2.1: Component ranking: 8 substation test case

Rank	BC	Vertex ID	Component Type	CPBC	Vertex ID	Component Type
1	0.1393	1896	Host PC	0.0652	1896	Host PC
2	0.0837	2010	Distance relay (SEL_421_*)	0.0583	[2018,2020,2004,2006]	[Overcurrent relay x2, Distance relay x2]
3	0.0686	1894	Host PC	0.0528	[2014,2016,1998,2000, 2002,2008,1996]	[Overcurrent relay x2, Distance relay x4, Host PC]
4	0.0490	1930	Overcurrent relay	0.0476	2012	Overcurrent relay
5	0.0460	[1875,1892,2026]	[Router/Switch,Host PC x2]	0.0304	1930	Overcurrent relay
6	0.0301	1881	Router/Switch	0.0282	[1920,1922,1924,1926, 1928]	[Overcurrent relay x5]
7	0.0213	[1882,1898,1900,1902, 2030]	[Local machine gateway,Host PC x3, Router/Switch]	0.0175	2024	Distance relay
8	0.0210	2029	Router/Switch	0.0105	[1938,1940,1942,1934, 1936,1932]	[Overcurrent relay x3, Distance relay x2, Host PC]
9	0.0178	[1920,1922,1924,1926, 1928]	[Overcurrent relay x5]	0.0067	2022	Host PC
10	0.0156	[1916,1918,1910,1912, 1914]	[Overcurrent relay x2, Distance relay x3]	0.0061	[2010,1877]	[Distance relay, Router/Switch]
11	0.0142	[2012,2014,2016,2018, 2020,1998,2000,2002, 2004,2006,2008]	[Overcurrent relay (SEL_451_*) x5, Distance relay x6]	0.0015	[1916,1918,1910,1912, 1914,1870]	[Overcurrent relay x2, Distance relay x3, Router/Switch]
12	0.0070	1996	Host PC	0.0013	1871	[Router/Switch]
13	0.0054	[1938,1940,1942,1934, 1936]	[Overcurrent relay x3, Distance relay x2]	0.0007	1878	[Router/Switch]
14	0.0049	2024	Distance relay	0.0005	1894	Host PC
15	0.0015	2022	Host PC	0.0003	[1898,1900,1902,2030]	[Host PC x3, Router/Switch]

Table 2.2: Component ranking: 300 Bus test case



Rank	BC	Vertex ID	Component Type	CPBC	Vertex ID	Component Type
1	0.2196	79377	Host PC	0.9356	79373	Host PC
2	0.2191	79373	Host PC	0.0164	86051	Branch breaker
3	0.0439	[80961,80963, 88795,79115]	[Host PC x2, Router/Switch x2]	0.0138	85751	Communications processor
4	0.0025	[87565,87567, 87569,87671]	[Bus differential relay, Terminal relay x3]	0.0005	79377	Host PC
5	0.0024	[81639,82137, 82635,83133, . ..]	[Host PC x4, …]	0.0001	[86053,86055, 86057,86059, …]	[Branch breaker, Terminal relay x3, …]

2.6.1 Cyber-physical Component Ranking

We implemented CRSA on the test cases with results as illustrated in Table 2.1 and Table 2.2, showing calculated and normalized values for the CPBC and BC indices. The first column in the table shows the rank of the vertices until such a rank where the decrease in overall system vulnerability is negligible. The second and fifth columns furnish the calculated and normalized values for the BC and CPBC indices respectively. The third and sixth columns furnish the unique identification (ID) for the vertices as ranked by the BC and CPBC respectively, while, the fourth and seventh columns presents the component type. For instance, Host PC with ID 1896, ranked 1 (most critical) by both the BC and CPBC,when protected, host 1896 drastically reduces adversary system impact by 12.95% as observed from Table 2.3.

2.6.2 Cyber-physical Risk Sensitivity Analysis

After component ranking, the vertices are protected as in Algorithm 2, by reducing the vulnerabilities associated with that vertex by 100%, hence deterministically patching the vulnerabilities. We choose 100% for the purpose of this evaluation in order to eliminate bias that can occur in the results due to randomly choosing different vulnerability types to remove. This leads to a new system attack graph H with total adversary-accessible attack paths less than or equal to that of the original attack graph G. Table 2.3 and Table 2.4 furnish the decrease in attack paths that component protection provides. The second column represents the total number of attack paths present in H. The third column furnishes the total percentage decrease in attack paths present in H, from

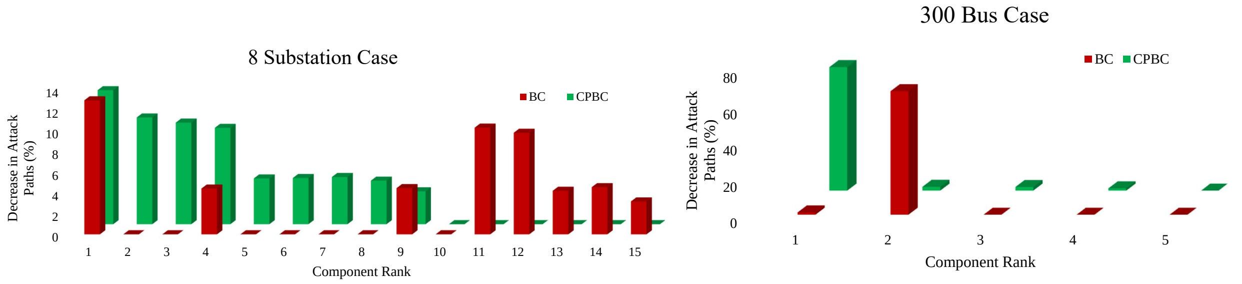


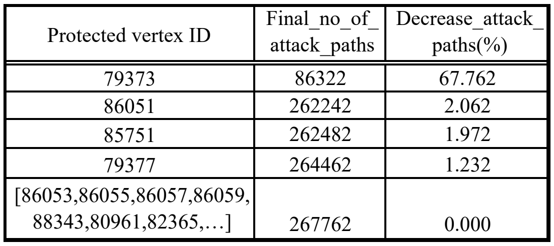
Figure 2.4: 8 Substation and 300 bus test cases: Visualizing the decrease in attack paths illustrated in Table 2.1 and Table 2.2, where the proposed cyber-physical risk framework demonstrates a steady decrease in risk (exploitable paths) with protection of components, from higher to lower ranked by the CPBC as opposed to the BC index.

that of G. In Fig. 2.4, the accuracy of the CRSA model is observed in the decreasing slope of the percentage adversary-accessible attack paths as the component ranks progress from 1-15 and 1-5, for the 8 substation and 300 bus test cases respectively. This sustained reduction, as opposed to the random decrease in ranking attained by using the BC metric, is preferable since component importance is proportional to percentage decrease in attack paths. Hence the decrease in attack paths attained by protecting a component of Rank 1 $>$ Rank 2 $>$ Rank 3 $>$ ... as illustrated in Fig. 2.4. Furthermore, we observe that the proposed CPBC ranking, as shown in Tables 2.1 and 2.2, calculates the same rank for vertices with equal decrease in number of attack paths accessible

Table 2.3: Actual component rank: 8 Substation case results. The protected vertex ID is associated with the components as mapped in Table 2.1

Protected vertex ID	Final_no_of_attack_ paths	Decrease_attack_ paths(%)
1896	68398	12.960
[2018,2020,2004,2006]	70469	10.324
[2014,2016,1998,2000,2002, 2008,1996]	70860	9.827
2012	71256	9.323
2024	74991	4.570
[1920,1922,1924,1926,1928]	75063	4.478
1930	75097	4.435
[1938,1940,1942,1934,1936, 1932]	75267	4.219
2022	76080	3.184
[2010,1894,1875,1892,1877, 1870,1871,1916, 1910, ...]	78582	0.000

Table 2.4: Actual component rank: 300 Bus case results. The protected vertex ID is associated with the components as mapped in Table 2.2



Protected vertex ID	Final_no_of_ attack_paths	Decrease_attack_ paths(%)
79373	86322	67.762
86051	262242	2.062
85751	262482	1.972
79377	264462	1.232
[86053,86055,86057,86059, 88343,80961,82365,...]	267762	0.000

to adversary. Hence, this additional component grouping functionality, not provided by the traditional BC metric, aids in simplifying and reducing computational burden during cyber-physical risk analysis as illustrated in Tables 2.3 and 2.4, where component sets with equal importance are provided to the system operator.

2.6.3 Complexity and Computational Efficiency

From Algorithm 1, we can compute the time complexity of the component ranking algorithm to be of the order of $O(I * R * Avg_{PL} * N)$, where I is the number of internet vertices, R is the number of relay vertices, Avg_{PL} is the average shortest path length which will depend on the graph density, and N is the total number of vertices. With approximation, we can consider the time complexity of the BC algorithm to be $O(N^4)$. The number of the internet and relay vertices as shown in Table 2.5 also influence the computation time, as the CPBC metric traverses, the attack graph starting from internet hosts and terminating in the relay vertices, hence adding to the time complexity of the CPBC ranking. Note that the time for the attack graph generation, an input to the proposed ranking model, increases with larger connected networks (9 minutes for the IEEE

Table 2.5: Computational Complexity

Test Case	Internet Hosts	Relays	Attack Paths	CPBC Time (s)	BC Time (s)
8 Substation	11	54	78582	7.6697	7.6
300 Bus	5	1300	267762	2024.62	1712

300 test case) as detailed in our previous work [59], while in this paper, we focus on the time complexity of the proposed ranking model.

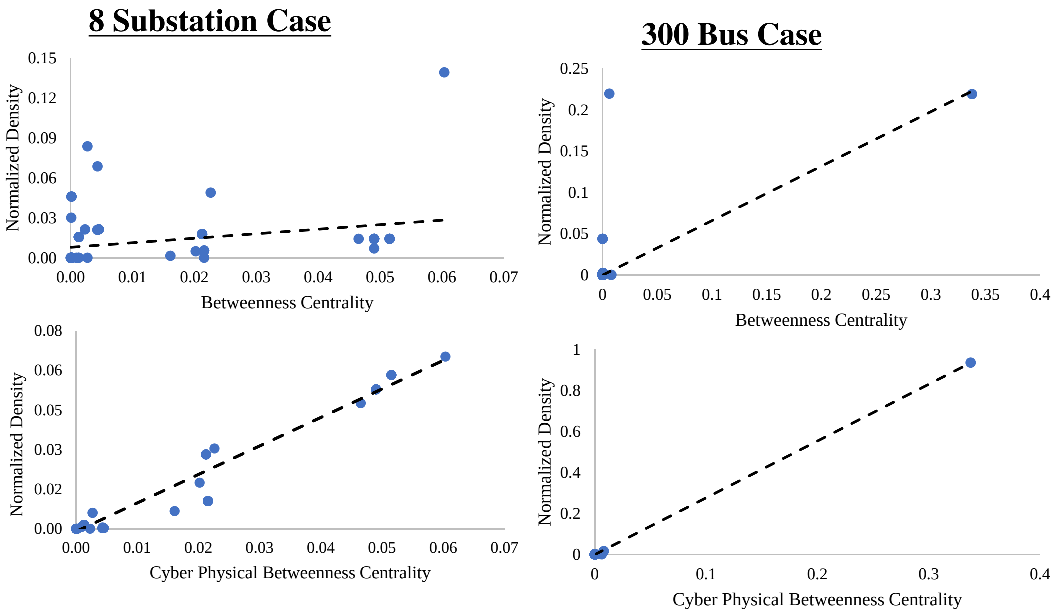


Figure 2.5: Vertex Density Analysis: Showing that the CPBC is more correlated to the graph node density than the BC in the 8 substation and 300 bus use cases.

2.6.4 Vertex Density Analysis

Vertex density is the relationship between the number of edges associated with a vertex and the total number of possible edges in the attack graph [67]. Hence, the vertex density holds information on the importance of a vertex [68]. Here, we show the improvements attained by the proposed CPBC index as opposed to the traditional BC metric using their correlations with vertex density as shown in Fig. 2.5 where we observe approximately linear relationships, however, with higher correlation between the vertex densities and the CBPC as opposed to the traditional BC metric.

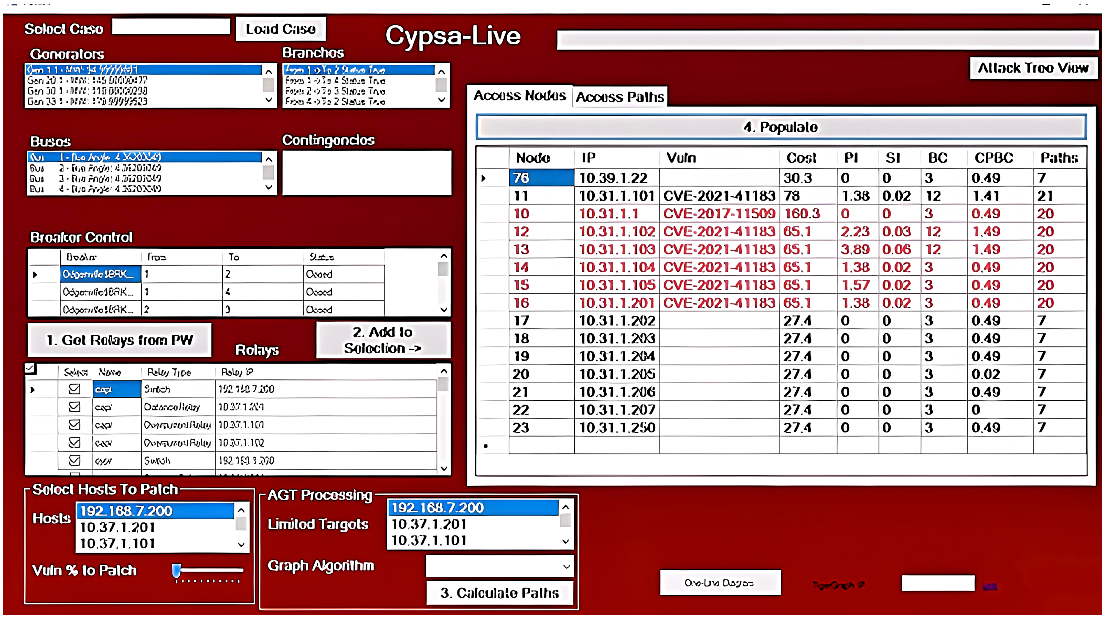
2.7 Conclusion

This chapter proposed a model for critically ranking system components, which integrates cyber-layer industry security vulnerability standards into the risk sensitivity analysis of the cyber-physical power system. The proposed model first leverages potential adversary intrusion vertices and targets to generate an attack graph which estimates potential attack paths. The model integrates cybersecurity costs and target reachability, via a proposed cyber-physical betweenness centrality index, to determine component criticality which is passed to the system operator for prioritized protection, enabling risk reduction to adversary intrusion.

2.8 Use Cases

2.8.1 Integrating CRSA to Dynamic and Online Risk Assessment

CRSA is currently incorporated into *CyPSA-Live*, a prototype solution of the power system security defense project, “Deep Cyber Physical Situational Awareness for Energy Systems: A Secure Foundation for Next-Generation Energy Management," with the objective to help energy delivery stakeholders own and maintain a threat-resilient dataflow pipeline from sensors to actuators. The *CyPSA-Live* application, shown in Fig. 2.6, enables situational awareness and risk mitigation to identify the most critical assets in the network. CRSA enables *CyPSA-Live*’s critical asset ranking



Breaker	From	To	Status
[illegible]	1	2	Closed
[illegible]	1	4	Closed
[illegible]	2	3	Closed

Select	Name	Relay Type	Relay IP
☑	[illegible]	Switch	192.168.7.200
☑	[illegible]	Distance Relay	10.37.1.201
☑	[illegible]	Overcurrent Relay	10.37.1.101
☑	[illegible]	Overcurrent Relay	10.37.1.102
☑	[illegible]	Switch	192.168.3.200

Hosts: 192.168.7.200, 10.37.1.201, 10.37.1.101

Limited Targets: 192.168.7.200, 10.37.1.201, 10.37.1.101

Node	IP	Vuln	Cost	PI	SI	BC	CPBC	Paths
76	10.39.1.22		30.3	0	0	3	0.49	7
11	10.31.1.101	CVE-2021-41183	78	1.38	0.02	12	1.41	21
10	10.31.1.1	CVE-2017-11509	160.3	0	0	3	0.49	20
12	10.31.1.102	CVE-2021-41183	65.1	2.23	0.03	12	1.49	20
13	10.31.1.103	CVE-2021-41183	65.1	3.89	0.06	12	1.49	20
14	10.31.1.104	CVE-2021-41183	65.1	1.38	0.02	3	0.49	20
15	10.31.1.105	CVE-2021-41183	65.1	1.57	0.02	3	0.49	20
16	10.31.1.201	CVE-2021-41183	65.1	1.38	0.02	3	0.49	20
17	10.31.1.202		27.4	0	0	3	0.49	7
18	10.31.1.203		27.4	0	0	3	0.49	7
19	10.31.1.204		27.4	0	0	3	0.49	7
20	10.31.1.205		27.4	0	0	3	0.02	7
21	10.31.1.206		27.4	0	0	3	0.49	7
22	10.31.1.207		27.4	0	0	3	0	7
23	10.31.1.250		27.4	0	0	3	0.49	7

Figure 2.6: Implementations of this work in the prototype tool for power system defense.

which assists users to take corrective measures such as installing software patches against vulnerabilities in the hosts (shown in bottom left of Fig. 2.6), manually operating the relays, or isolating the compromised network. The current functionalities of the *CyPSA-Live* include: 1.) Generating attack graph model in real-time by interacting with the NP-Live server [61], 2.) Interacting in real-time with the NVD to obtain cyber vulnerability severity rating, and impact scores, 3.) Extracting the list of possible CVEs, 4.) Patching the network vulnerabilities towards updating potential attack paths and ranking critical assets using the CPBC metric.

3. GRAPH NEURAL NETWORKS BASED DETECTION OF STEALTH FALSE DATA INJECTION ATTACKS IN SMART GRIDS [*]

3.1 Introduction

A smart grid consists of physical power system infrastructure and cyber communication network. Measurement data are acquired by physical devices and delivered to the Supervisory Control and Data Acquisition System (SCADA). The communication network transfers the measurement data to the application level where are processed and evaluated by the power applications [70]. The resilience of power system depends on the security of this cyber-physical pipeline [71]. Thus, integrity and trustworthiness of the measurement data play a critical role in ensuring proper operation of smart grids [72]. By breaking this integrity, cyber-physical attacks target smart metering devices to harm the underlying physical systems.

False data injection attacks (FDIAs) represent a significant class of cyber threats that modify power system state estimation (PSSE) by maliciously altering measurement data. In FDIAs, an attacker changes sensor data in such a way that a valid and misleading operating point converge in PSSE and the attack becomes unobservable [73]. Being unaware of the malicious data, the grid operator takes actions according to the false operating point of grid and consequently disrupts power system operation.

Stealth (unobservable) FDIA can easily bypass the bad data detection (BDD) systems. Therefore, FDIAs are one of the most critical attacks for today's smart power systems. FDIAs in power grids were first introduced a decade ago by [74], which showed that an attacker with enough knowledge of the grid topology can design an unobservable attack that satisfies the power flow equations and bypasses the BDD module. Influential reference [74] prompted an increased interest in detection of FDIAs [75–88]. Most of the works that deal with detection of FDIAs assume a linearized

[*] ©[2021] IEEE. Reprinted, with permission from, Boyaci O, Umunnakwe A, Sahu A, Narimani MR, Ismail M, Davis KR, Serpedin E., "Graph neural networks based detection of stealth false data injection attacks in smart grids," in IEEE Systems Journal, vol. 16, pp. 2946-57, Oct 2021, doi: 2946-57 [69].

DC model [74–77, 79, 80, 82, 84, 87]. In the DC state estimation model, bus voltage magnitudes are assumed to be known as 1 p.u. and branch resistances and shunt elements are neglected. Hence, estimation of bus voltage angles is reduced to linear matrix operations, and in general it helps to analyze the grid at some extent. Although the linearized DC model is fast and simple, ignoring voltage magnitudes and reactive power components does not reflect the actual physical operation of the grid [16]. Therefore, the DC models can not validate that the FDIAs being tested are stealthy because PSSE and BDD tools employing AC power flow modeling can easily detect these attacks without using extra detectors. In addition, only a few works exploit grid topology information into their detection model [78, 89, 90] together with graph signal processing techniques to detect FDIAs. Although innovative and powerful, these methods manually design spectral filters, an operation which is not scalable since it requires manual and custom filter design steps. Scalability is an essential feature that has to be considered when designing detectors. Except a few highly scalable designs [91, 92], the majority of the proposed detectors for FDIAs are designed for small scale systems such as IEEE 14 [79, 80, 82, 83] or IEEE 30 [85, 87]. Therefore, extensibility issues may arise when deploying small-scall detectors at large-scale networks.

Survey [93] classifies the FDIA detection algorithms into two categories: model-based methods [79–83] and data-driven methods [84–88]. In general, model-based algorithms require first to build a system model and estimate its parameters to detect FDIAs. Since there is no independent system to be trained, model-based methods do not need historical datasets; nevertheless, threshold finding, detection delays and scalability aspects restrict applicability of model-based methods [93]. On the contrary, data-driven models do not interfere with the system and its parameters, yet they necessitate historical data and a training process in order to reduce the detection time and increase scalability.

Due to the superiority of machine learning (ML) methods along with the increasing volume of collected historical data samples, ML-based detectors have been proposed to identify FDIAs in smart grids [84, 85, 87, 88]. Undirected graphs can be used to capture the smart grid topology; buses and branches of the grid can be represented by nodes and edges of the undirected graph, respectively. The Graph Neural Network (GNN) architecture, in particular, immensely benefits from this architectural matching promise [94, 95]. Due to GNN's highly efficient modeling capability in non-Euclidean data structure, they are adopted in numerous areas such as social networks, physical systems, and traffic networks [95]. Despite their potential, to the best of our knowledge, no study has explored GNNs to detect FDIAs. In this chapter, we propose a GNN-based stealth FDIA detection model for smart power grids. To fully model the underlying complex AC power system and dynamism of the measurements data, we decided to use a hybrid model; while system topology is integrated into our model by the help of GNN graph adjacency matrix, historical measurement data are modeled by the GNN spatial layers. These features enable to take advantage of the benefits of both model-driven and data-driven approaches and hence better detect and mitigate FDIAs.

The contributions of this chapter are summarized as follows:

- We properly model the inherent cyber system: due to topology and distribution of smart measurement devices, meter readings are correlated in the smart grid measurement space; hence, ignoring the location of the meter data and assuming independent and identical distribution of meter readings may not be accurate for a data-driven model. Therefore, we use GNN to match the cyber and physical layers of the grid.

- We design a stealth FDIA attack methodology to test our detector: the main goal of any FDIA detector is to be able to detect stealth attacks since observable attacks can be easily detected by BDD systems. Therefore, we develop a Stochastic Gradient Descent (SGD) based stealth FDIA detection algorithm to exploit the possible weak points of the grid and assess the performance in realistic conditions. It is experimentally verified that the designed attacks can easily bypass classical BDD algorithms; however, they are detected by the proposed GNN detectors.

- We propose a scalable and real-time FDIA detector as an early warning/prediction system prior to the PSSE: since PSSE outcome is directly used by various EMS, the integrity of the measurements should be preserved. In addition, the proposed detector is efficiently extensible to larger networks. Moreover, as detection delays can be very critical for power grids, possible attacks should be detected as quickly as possible. Employing the standard IEEE 14, 118, and 300 bus test cases, we demonstrate that the proposed method is linearly scalable in parameter size and detection time.

3.2 GNN Based Detection of FDIA

3.2.1 False data injection attack scenario

First, active and reactive power injections P_i, Q_i at buses and active and reactive power flows P_{ij}, Q_{ij} on branches are read by RTUs. Next, as a man in the middle, an attacker attempts to inject false data to the original measurements $z_o = [P_i, P_{ij}, Q_i, Q_{ij}]$ before the grid operator receives them. Then, using $\boldsymbol{z_a}$, the operator estimates the state variables and runs the BDD block to indicate a possible attack. In parallel, the defender runs the GNN-based detector when it receives the measurements and hence predicts the probability of attack to warn the operator. In order not to raise suspicion from the operator, the attacker needs to design a stealth $\boldsymbol{z_a}$ that can bypass the BDD mechanism.At the same time, the attack strength should be strong enough to cause intended consequences or damages to the grid. In this regard, s/he initially estimates the state variables of grid in the target area , where security of the meters is compromised. Then, s/he searches a set of measurements $\boldsymbol{z_a}$ in the measurement space that serves the intended aim.

FDIAs require that an adversary know the parameters and topology of the targeted portion of the system and is able to tamper the measurement data before the operator uses them in PSSE [70, 74]. Since accessing information and hardware all over the grid is neither easy nor realistic, we use a realistic 'local' attack model to test our system. Due to the lack of open source, AC power flow based stealth FDIA generation algorithms to fully test the detection system, we propose a generic, localized AC stealth FDIA generation method using the stochastic gradient descent algorithm. Herein scenario, the attacker focuses on a target area of the grid where the measurements s/he wants to inject the false data are located. To specify this area, it is assumed that s/he found an entry point p in the cyber layer and can manipulate the measurements up to the $r-$neighbor of p. Since generation buses and zero-injection buses would be too risky to change, s/he skips those buses even if they are in their active target region [96–99]. Moreover, s/he avoids to attack the power flow measurements if this alternation leads to violate the KCL at the bus that the line is connected to [100]. To find a stealth attack vector in , the attacker tries to minimize the objective function:

$$\begin{aligned} &\min_{\check{\boldsymbol{x}}} \lambda_z ||h(\check{\boldsymbol{x}})_i - h(\hat{\boldsymbol{x}})_i||_2 - \lambda_x ||\check{\boldsymbol{x}}_j - \hat{\boldsymbol{x}}_j||, \forall i \in \mathcal{T}_z, \forall j \in_x \\ &\text{s.t. } h(\check{\boldsymbol{x}})_k = h(\hat{\boldsymbol{x}})_k,\ \check{\boldsymbol{x}}_l = \hat{\boldsymbol{x}}_l,\ \forall k \notin T_z,\ \forall l \notin_x \\ &\quad \tau_m^{min} < ||\check{\boldsymbol{x}}|| < \tau_m^{max},\ \tau_a^{min} < \angle(\check{\boldsymbol{x}}) < \tau_a^{max}, \end{aligned} \tag{3.1}$$

where $\hat{\boldsymbol{x}}$ denotes the honest state vector, $\check{\boldsymbol{x}}$ stands for false data injected state vector, λ_z and λ_x are weighting factors associated with loss terms, ${}_z$ and ${}_x$ denote the targeted measurements and state variables, τ_m^{min} and τ_m^{max} denote the minimum and maximum values of the magnitude of $\check{\boldsymbol{x}}$, and τ_m^{min} and τ_m^{max} represent minimum and maximum values of the angle of $\check{\boldsymbol{x}}$, respectively. In essence, s/he searches a vector $\check{\boldsymbol{x}}$ in the state space of the grid by only targeting some $\boldsymbol{x} \in_x$ so that the corresponding measurements $\boldsymbol{z_a} = h(\check{\boldsymbol{x}})$ resemble the original measurements $\boldsymbol{z_o}$ in the measurement space of the grid restricted by ${}_z$. Note that the objective function in (3.1) consists of two competing losses. While the first part $||h(\check{\boldsymbol{x}})_i - h(\hat{\boldsymbol{x}})_i||_2$ aims to minimize the measurement differences in ${}_z$, the second part $||\check{\boldsymbol{x}}_j - \hat{\boldsymbol{x}}_j||$ maximizes the attack power injected into the state variables in ${}_x$. The trade-off between these objectives is directly related to detection risk and attack power since deviation from the original state variables increases the probability of being detected. Consequently, an attacker can increase the attack power at the expense of higher risk of being detected. The attacker aims to maximize the assault power by minimizing the detection risk. To do that, s/he first defines a free complex variable $\check{\boldsymbol{x}}_j \in$ in the vicinity of original estimated values by probing them with a small Gaussian noise. Using the SGD algorithm, s/he calculates the gradient of the state variables with respect to the joint loss defined in (3.1) and updates them iteratively at each step until there is no improvement in the loss. Recall that s/he only updates a state variable if it is in the active insecure area. Eventually, s/he decides whether to inject this obtained false data to the related measurements in the cyber layer of the grid, according to the final loss value obtained during the iterations. In a sense, this individual latent vector search can be interpreted as 'training' in the machine learning terminology [101]; however, it is very specific to the corresponding time slot and should be repeated for each case in order to minimize the detection risks. Note that this generic algorithm can be tailored according to the modeled electric grid and capabilities of the attacker.

3.2.2 Detection of Attacks Using Graph Neural Network

The architecture of the proposed GNN-based detector is depicted in Fig. 3.1. It contains one input layer to represent bus power injection measurements, L hidden Chebyshev graph convolution layers to extract spatial features and one output dense layer to predict the probability of the input sample being attacked. In this layered structure, X^0 denotes two channel input tensor $[P_i, Q_i] \in^{n\times 2}$, X^l represents the output tensor of hidden layer $l \in^{n\times c_l}$, $y \in$ designates the scalar output of the neural network, $1 \leq l \leq L$, and c_l stands for the number of channels in layer l. Particularly, a GNN hidden layer l takes $X^{l-1} \in^{n\times c_{l-1}}$ as input and produces $X^l \in^{n\times c_l}$ as output. Different from the hidden graph layers, dense layer outputs y in classical feed-forward neural networks by feeding with the inputs $X^L \in^{n\times c_L}$. In this multi-layer architecture, each Chebyshev

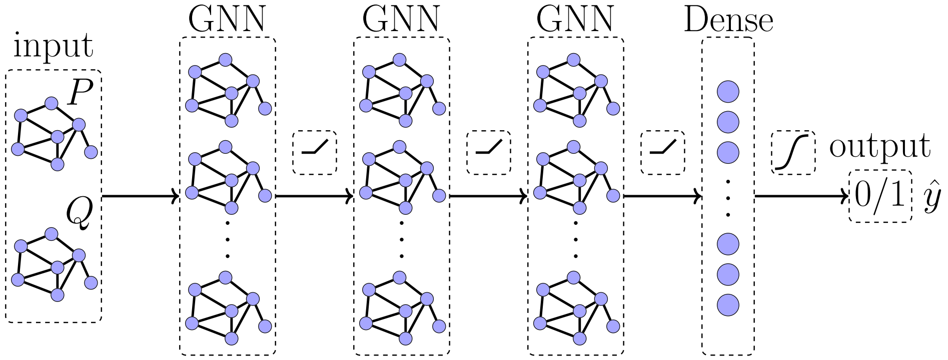


Figure 3.1: Architecture of the proposed GNN based detector [69].

layer l for $1 \leq l \leq L$ transforms its input X^{l-1} by first applying graph convolution operation, then adding a bias term and finally employing a nonlinear rectified linear unit function (ReLU) defined as ReLU$(x) = \max(0, x)$ to generate X^l as,

$$X^l = \text{ReLU}(\theta^l *_X^{l-1} + b^l), \tag{3.2}$$

where $\theta^l \in^{K \times c_{l-1} \times c_l}$ denotes free Chebyshev coefficients and $b^l \in^{c_l}$ represents bias term of the layer l . The output of the dense layer is computed by $y = \sigma(W^L X^L + b^L)$, where $W^L \in^{n \times c_L}$ denotes the weights of each feature, $b^L \in$ represents the bias term and σ designates the nonlinear sigmoid operation: $\sigma(x) = 1/(1 + e^{-x})$.

3.3 Experimental Results

3.3.1 Data Generation

It is arduous to find publicly available power grid data due to privacy issues, hence synthetic data are generated using Pandapower [102] for several test cases including IEEE 14, 118, and 300. Data generation steps are summarized in Algorithm 3. To make the data as realistic as possible, we first downloaded ERCOT's 15 minutes interval backcasted actual load profiles [103]. Next,

Algorithm 3: Data Generation: Scaling ERCOT Data to the IEEE Test Cases

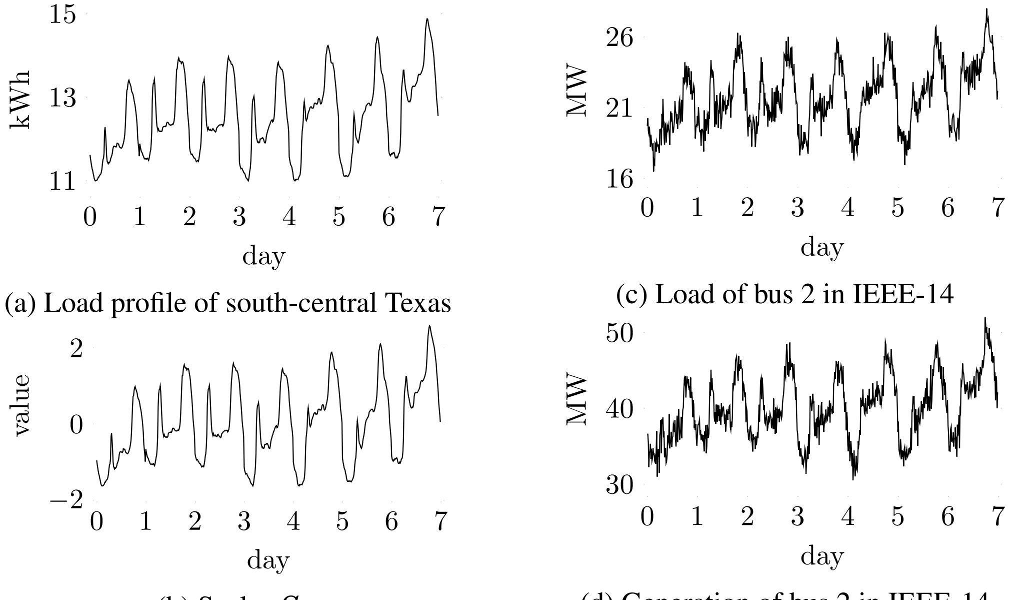
```
Input  : normalized scaler $\boldsymbol{S}$
Output: $\boldsymbol{Z_n}, \boldsymbol{X_n}$ for each test system $n$
$N \leftarrow [14,\ 118,\ 300]$ $T \leftarrow [1$ to $9600]$ $k,\ \sigma_s \leftarrow 0.1,\ 0.03$ $\sigma_n \leftarrow 0.01$
Function Generate($sg,\ t$):
    foreach $bus \in sg.genbus \cup sg.loadbus$ do
        $bus.scale \leftarrow (1 + k \times \boldsymbol{S_t},\ \sigma_s)$
    $\boldsymbol{z_o} = sg.PF()$ $\boldsymbol{z_o} \leftarrow (\boldsymbol{z_o},\ \boldsymbol{z_o} \times \sigma_n)$, $\hat{\boldsymbol{x}} \leftarrow sg.PSSE(\boldsymbol{z_o})$ return $\boldsymbol{z_o},\ \hat{\boldsymbol{x}}$
Function Main:
    foreach $n \in N$ do
        $\boldsymbol{Z_n},\ \boldsymbol{X_n} \leftarrow [\,],\ [\,]$ $sg \leftarrow$ SG$(n)$ foreach $t \in T$ do
            $\boldsymbol{z},\ \boldsymbol{x} \leftarrow$ Generate$(sg,\ t)$
            $\boldsymbol{Z_n}[\boldsymbol{t}],\ \boldsymbol{X_n}[\boldsymbol{t}] \leftarrow z,\ x$
        $\boldsymbol{Z_n}.save(),\ \boldsymbol{X_n}.save()$
```

we arbitrarily selected the 'BUSHILF_SCENT' profile which corresponds to south-central Texas having a high load factor. Then, we normalized the time series data to zero mean and unit variance 'scaler' vector $\boldsymbol{S}$ so that it can be easily adapted to each test system. Having obtained $\boldsymbol{S}$, we run the Main function of the Algorithm 3 where a smart grid object sg is created for each test system having n bus and Generate function is called for each timesteps t. In Generate function, the scaling parameters of generator and load buses are assigned to a sample drawn from a normal distribution with $1 + 0.1 \times \boldsymbol{S_t}$ mean and 0.03^2 variance, where $\boldsymbol{S_t}$ denotes the value of $\boldsymbol{S}$ at time-step t. Due to the properties of normal distribution, the scaling operation provides practically more than $\pm 20\%$ dynamic range on average with respect to the static case. We limit the scaling range between 0.7 and 1.3 for the convergence of power flow solutions. As a next step, AC power flow solutions are calculated, and the measurements considered to have 1% noise are read. Finally, PSSE is conducted, and estimated state variables are returned along with original meter values to the Main function. In Fig. 3.2, the scaling process formulated with line 7 in Algorithm 3 is demonstrated for one week period (7×96 samples). Please note that $\boldsymbol{S}$ is just a normalized version of the south-central Texas load profile. Next, the load and generation values of buses are multiplied with a value sampled from a distribution $(1 + k \times \boldsymbol{S_t},\, \sigma_s)$ which has $1 + k \times \boldsymbol{S_t}$ mean and σ_s standard deviation at time t. Namely, they follow the patterns in $\boldsymbol{S}$ by deviating around their static values defined in their test systems.

3.3.2 Attack Generation

After generating honest data samples, we focus on malicious data samples in this subsection, where the attack generation steps are summarized in Algorithm 4. The algorithm gets original measurements matrix $\boldsymbol{Z_n} \in^{T \times m}$ and estimated state variable matrix $\boldsymbol{X_n} \in^{T \times n}$ and produces their attacked version as well as corresponding sample vector $Y_n \in^{T}$, where 0 and 1 in $\boldsymbol{Y_n}$ represent honest and malicious samples, respectively. As can be seen from Algorithm 4, Main function simply creates the smart grid and attacker objects, fetches the current sample and calls Generate function for each system having n buses at each time-step t.

Generate function, in contrast, simulates a 'smart' intruder capable of entering the cyber layer



(a) Load profile of south-central Texas

(c) Load of bus 2 in IEEE-14

(b) Scaler $\boldsymbol{S}$

(d) Generation of bus 2 in IEEE-14

Figure 3.2: An example scaling process for bus 2 in the IEEE-14 bus test system [69].

of the grid, computing an unobservable attack vector and deciding to insert the false data into the measurement devices according to the 'quality' of the attack. In this regard, since it is not realistic to assume that an attacker can inject false data at every time step due to practical reasons, Generate function first models the attack frequency by a r.v. $f \sim (0, 1)$ where $f > \tau_{freq}$ means the attacker has successfully entered the system. To attack roughly 15% of total time-steps on average, τ_{freq} is selected as 1. Second, it models the target area of the attacker by help of a r.v. $p \sim \mathcal{U}(1, n)$ and a predefined attack radius r. To this end, it calls a breadth first search (BFS) method of the attacker object to model the target area defined by a set of measurements captured by the attacker denoted by ${}_z$ and a set of state variables intended to inject the false data. In fact, all the measurements and state variables located up to r-distance neighbor of the bus p are assumed to be in ${}_z$ and ${}_x$ except the generator buses and zero-injection buses. Then, it calls the attack method of the attacker to compute and insert z_a if the method returns a $loss$ value smaller than threshold τ_{loss}. The attacker's assault method solves the nonlinear and non-convex minimization (3.1) in the Tensorflow [104] library. As a first step, it defines a free trainable vector tuple to represent the new complex state variables $\breve{\boldsymbol{x}}$ which constitutes the 'fake' operating point at the end of attack: voltage

Algorithm 4: Generation of Malicious Attack Data Samples

```
Input  : $\boldsymbol{Z_n},\ \boldsymbol{X_n}$ for each test system $n$
Output: $\boldsymbol{Z_n},\ \boldsymbol{X_n},\ \boldsymbol{Y_n}$ for each test system $n$
$N \leftarrow [14,\ 118,\ 300]$ $T \leftarrow [1$ to $9600]$ $\sigma_n \leftarrow 0.005$ $\lambda_z,\ \lambda_x \leftarrow 1,\ 1$ $\eta,\ E \leftarrow 0.001, 1000$
  $\tau_{freq},\ \tau_{loss} \leftarrow 1,\ 0.1$ $R_{min} \leftarrow \{14:2,\ 118:3,\ 300:6\}$ $R_{max} \leftarrow \{14:3,\ 118:4,\ 300:8\}$
Function attacker.attack($\boldsymbol{z_o},\ \hat{\boldsymbol{x}},\ _z,\ _x$):
    $\boldsymbol{trainable\ V}$ : $0.9 < \boldsymbol{V} < 1.1$
    $\boldsymbol{trainable\ \theta}$ : $-\pi < \boldsymbol{\theta} < +\pi$
    $\boldsymbol{V},\ \boldsymbol{\theta} \leftarrow \text{abs}(\hat{\boldsymbol{x}}),\ \text{angle}(\hat{\boldsymbol{x}})$
    foreach $j \in_x$ do
        $\boldsymbol{V_j} \leftarrow \boldsymbol{V_j} + (0,\ \sigma_n^2)$
        $\boldsymbol{\theta_j} \leftarrow \boldsymbol{\theta_j} + (0,\ \sigma_n^2)$
    foreach $epoch \in E$ do
        $\check{\boldsymbol{x}} \leftarrow \boldsymbol{V}e^{j\boldsymbol{\theta}}$ $\boldsymbol{z_a} \leftarrow h(\check{\boldsymbol{x}})$ $L_z \leftarrow \sum_i ||\boldsymbol{z_{ai}} - \boldsymbol{z_{oi}}||_2,\ \forall i \notin_z$
        $L_x \leftarrow \sum_j ||\check{\boldsymbol{x}}_j - \hat{\boldsymbol{x}}_j||,\ \forall j \notin_x$
        $L \leftarrow \lambda_z L_z - \lambda_x L_x$
        foreach $j \in_x$ do
            $\boldsymbol{V_j} \leftarrow \boldsymbol{V_j} - \eta \frac{\partial L}{\partial \mathbf{V_j}}$
            $\boldsymbol{\theta_j} \leftarrow \boldsymbol{\theta_j} - \eta \frac{\partial L}{\partial \boldsymbol{\theta_j}}$
    $\check{\boldsymbol{x}} \leftarrow \boldsymbol{V}e^{j\boldsymbol{\theta}}$ $\boldsymbol{z_a} \leftarrow h(\check{\boldsymbol{x}})$ return $\boldsymbol{z_a},\ L$
Function Generate($attacker,\ \boldsymbol{z_o},\ \hat{\boldsymbol{x}}$):
    $y,\ \boldsymbol{z} \leftarrow 0,\ \boldsymbol{z_o}$ $f \sim (0, 1)$ if $f > \tau_{freq}$ then
        $p \sim \mathcal{U}(1, n)$ $r \leftarrow \mathcal{U}(R_{min}[n],\ R_{max}[n])$ $_z,\ _x \leftarrow attacker.BFS(p, r)$
          $\boldsymbol{z_a},\ loss \leftarrow attacker.attack(\boldsymbol{z_o},\ \hat{\boldsymbol{x}},\ _z,\ _x)$
        if $loss < \tau_{loss}$ then
            $y,\ \boldsymbol{z} \leftarrow 1,\ z_a$
    $\check{\boldsymbol{x}} \leftarrow sg.PSSE(\boldsymbol{z})$
    return $\boldsymbol{z},\ \check{\boldsymbol{x}},\ y$
Function Main:
    foreach $n \in N$ do
        $\boldsymbol{Y_n} \leftarrow [\,]$ $sg \leftarrow \text{SG}(n)$ $attacker \leftarrow Attacker(n)$ foreach $t \in T$ do
            $\boldsymbol{Z_n}[\boldsymbol{t}],\ \boldsymbol{X_n}[\boldsymbol{t}],\ \boldsymbol{Y_n}[\boldsymbol{t}] \leftarrow \text{Generate}(attacker,\ \boldsymbol{Z_n}[\boldsymbol{t}],\ \boldsymbol{X_n}[\boldsymbol{t}])$
        $X_n.save(),\ Z_n.save(),\ Y_n.save()$
```

magnitude $\boldsymbol{V}$ is limited to $0.9 < \boldsymbol{V} < 1.1$ p.u. and voltage angle $\boldsymbol{\theta}$ is limited to $-\pi < \boldsymbol{\theta} < \pi$. Next, it initializes the jth elements of this tuple in the vicinity of their original variables by adding a small Gaussian white noise $(0,\ \sigma_n^2)$ if $j \in_x$ to ignite the optimization. This small proximity could play a vital role because SGD may fail to reduce the objective function if the initial point is not balanced [101]. A $\check{\boldsymbol{x}}$ too close to $\hat{\boldsymbol{x}}$ might result to no update at all in optimization variables $\boldsymbol{V}$ and $\boldsymbol{\theta}$, whereas a $\check{\boldsymbol{x}}$ too distant to $\hat{\boldsymbol{x}}$ might get stuck in a secluded region of and produce a highly suspicious $\boldsymbol{z_a}$. Thus, $\sigma_n = 0.005$ is found to be accurate according to the minimization loss. Then, for each epoch, it obtains $\boldsymbol{z_a}$ using $h(\boldsymbol{x})$ and consequently calculates loss term L_z as a root mean squared error between $\boldsymbol{z_a}$ and $\boldsymbol{z_o}$, and L_x as a mean absolute error between $\check{\boldsymbol{x}}$ and $\hat{\boldsymbol{x}}$. Eventually, it calculates gradients of total loss $L = \lambda_z L_z - \lambda_x L_x$ with respect to optimization variables $\boldsymbol{V_j}$ and $\boldsymbol{\theta_j} \in_x$ and updates corresponding terms in the reverse direction of gradients by scaling the gradients with learning rate η before starting the next epoch. Lastly, it returns $\boldsymbol{z_a}$ and final loss L to Generate function and halts.

3.3.3 Attack Detection

In order to immediately predict the attack probability in our models instead of waiting for PSSE result, we only use measurement values in our detectors. Moreover, since $P_i + jQ_i = \sum_{k\in\Omega_i} P_{ik} + jQ_{ik}$, node values can represent branch values as summation in their corresponding Ω_i and the proposed GNN-based detector accepts features in its nodes, we decide to use only P_i and Q_i as input to our models. PSSE and BDD modules, on the contrary, continue to receive every available measurement to operate as depicted.

Having decided to input features $[P_i, Q_i]_n \in^{9600\times n\times 2}$ and output labels $\boldsymbol{Y_n} \in^{9600}$ for $n \in \{14, 118, 300\}$ bus test systems where 0 denotes honest and 1 denotes malicious samples of $\boldsymbol{Y_n}$, we partition the first 60% of the samples for training the proposed detectors, the next 20% for validating and tuning the hyper-parameter of the models, and the last 20% for evaluating the performances of the detectors. Then, we standardize each split separately, with a zero mean and a standard deviation of one, to have a faster and more stable learning process [105].

As a next step, we implement the GNN-based FDIA detector having a multi-layer Chebyshev graph convolution layer in its hidden layer and one dense layer on top of that as depicted in Fig. 3.1. We add a bias term and ReLU activation functions between graph convolutional layers and sigmoid activation functions at the last dense layer to increase the detector's nonlinear modeling ability [105]. As for weighted adjacency matrix $\boldsymbol{W}$, we use the magnitude of complex sparse

Ybus matrix of the corresponding grid, which models the relation between nodes, determine the graph Laplacian L and scale it to obtain $\tilde{L}$. All free unknown parameters defined in the model are computed by a supervised training using cross-entropy loss:

$$L(\hat{y}, W_\theta) = \frac{-1}{N} \sum_{n=1}^{N} y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i), \tag{3.3}$$

over the training set where N denotes the number of samples in the training set, W_θ represents all trainable parameters θ_l and b_l for $1 \leq l \leq L$ along with W^L and b^L in the model, and y_i and $\hat{y}_i$ stand for true and predicted class probability for sample i, respectively. Training samples are fed into the model as mini batches having 64 samples with 128 maximum number of epochs in addition to the early stopping where 16 epochs are tolerated without any improvement in the cross entropy loss of validation set. All the implementation was carried out in Python 3.8 using Pandapower [102], Sklearn [106], and Tensorflow [104] libraries on Intel i9-8950 HK CPU 2.90GHz with NVIDIA GeForce RTX 2070 GPU.

3.3.4 Comparison with Other Methods

To compare our GNN-based models with the available detectors, we train, validate and test these models similar to our proposed detector using our dataset [69]. The detection rate (DR), false alarm rate (FA), and F1 score of each model for each test system are analyzed. The BDD system falls behind every other model as it simply predicts each sample as malicious, and this results in 100% FA rate for each test system. Non-NN based approaches such as DTC and SVM, in contrast, enhance the FA and perform better than BDD by an F1 score range between 67.91% - 85.97% due to their nonlinear modeling capabilities. The NN-based family surpasses the non-NN based models in general, except the MLP where it achieves comparable results with SVC and DTC. The RNN-based detector yields 86.33%, 83.87%, and 71.08% F1 score for IEEE 14, 118, and 300 bus systems, respectively. Only CNN and GNN based detectors reach the 90% F1 range. Nevertheless, GNN outperforms CNN models by 3.14%, 4.25% and 4.41% in F1 for IEEE test cases with 14, 118, and 300 buses, respectively. Our experiments point out that architectural differences in the NN family play a vital role in terms of detection performance, as graph data requires topology-aware models such as GNN to better reflect the adjacency relations of the measurement data.

3.4 Conclusion

In this chapter, we address the detection of stealth FDIA in modern AC power grids. To that end, we first developed a generic, locally applied, and stealth FDIA generation technique by solving a nonlinear non-convex optimization problem using SGD algorithm and made available the labeled data to the research community. Second, we proposed a scalable and real-time detection mechanism for FDIAs by fusing the underlying graph topology of the power grid and spatially correlated measurement data in GNN layers. Finally, we tested our algorithms on standard test beds such as IEEE 14-, 118-, and 300-bus systems and demonstrated that the proposed GNN detector surpasses the currently available methods in literature by 3.14%, 4.25% and 4.41% in F1 score, respectively.

3.5 Use Cases

3.5.1 Attack Data Provision for Risk Assessment

Critical infrastructure data is sensitive and thus arduous to obtain, often requiring long legal procedures and non-disclosure agreements. If permission is granted, the data transfer process may take several months, as there has to be a very secure hand-off, where third party applications are avoided and data transfer is preferably in-person. This difficulty translates to attack data which is even more so a matter of system security since this data exposes system vulnerabilities. Furthermore, since attacks are low frequency events, it is difficult to obtain the required quantity of study data for learning and training models that reduce risk. Hence, beyond the risk reduction to FDIA threats discussed in this chapter, the stealth FDIA detector proposed is intended for integration in the Cyber Physical Resilient Energy Systems (CYPRES) Next Generation Energy Management [65] such that the attack datapoints generated from FDIAs can be used for risk assessment studies in our emulation models for different use cases.

4. OPENCONDUIT: A TOOL FOR RECREATING POWER SYSTEM COMMUNICATION NETWORKS AUTOMATICALLY [*]

This chapter introduces continually improving efforts towards automating the modeling of the cyber-physical power system for risk assessment in next-generation energy management. The synthetic model of the test system in Fig. 4.1, is designed and implemented in our work [52, 108] which introduces the prototype solution of the power system security defense project, *“Deep Cyber Physical Situational Awareness for Energy Systems: A Secure Foundation for Next-Generation Energy Management,"* with the objective to help energy delivery stakeholders own and maintain a threat-resilient dataflow pipeline from sensors to actuators. The work discussed in this chapter designs and implements a tool [107,109] for next generation risk assessment which provides digital twins of cyber-physical infrastructure. A digital twin is a virtual model of a physical system which spans the system’s lifecycle and uses real-time data/traffic from the system’s network of sensors to simulate behavior and monitor operations [110]. The aim of the OpenConduit tool is to develop the power system’s digital twin to enable risk assessment and resilience studies by automating accurate virtual recreation of the power system network and traffic flow.

4.1 Introduction

Electric utilities incorporate legacy devices and protocols with limited security functions as part of the heterogeneous mix of technologies comprising large-scale cyber-physical power systems. The daily operations of critical infrastructures have long relied upon computer networks which attract adversarial actions. Adversaries can leverage vulnerabilities associated with communication protocols used by physical systems to create anomalies e.g., Ukraine’s power grid attacks [111] and the Colonial pipeline incident which shut off roughly 45% of the East Coast of United States supply of fuel [112]. The rise in adversarial attacks on critical infrastructure has heightened global

[*] ©[2022] IEEE. Reprinted, with permission from, Umunnakwe A, Wlazlo P, Sahu A, Velasquez J, Davis K, Goulart A, Zonouz S., “OpenConduit: A Tool for Recreating Power System Communication Networks Automatically,” in IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 141-147, Oct 2022, doi: 10.1109/SmartGridComm52983.2022.9960996 [107].

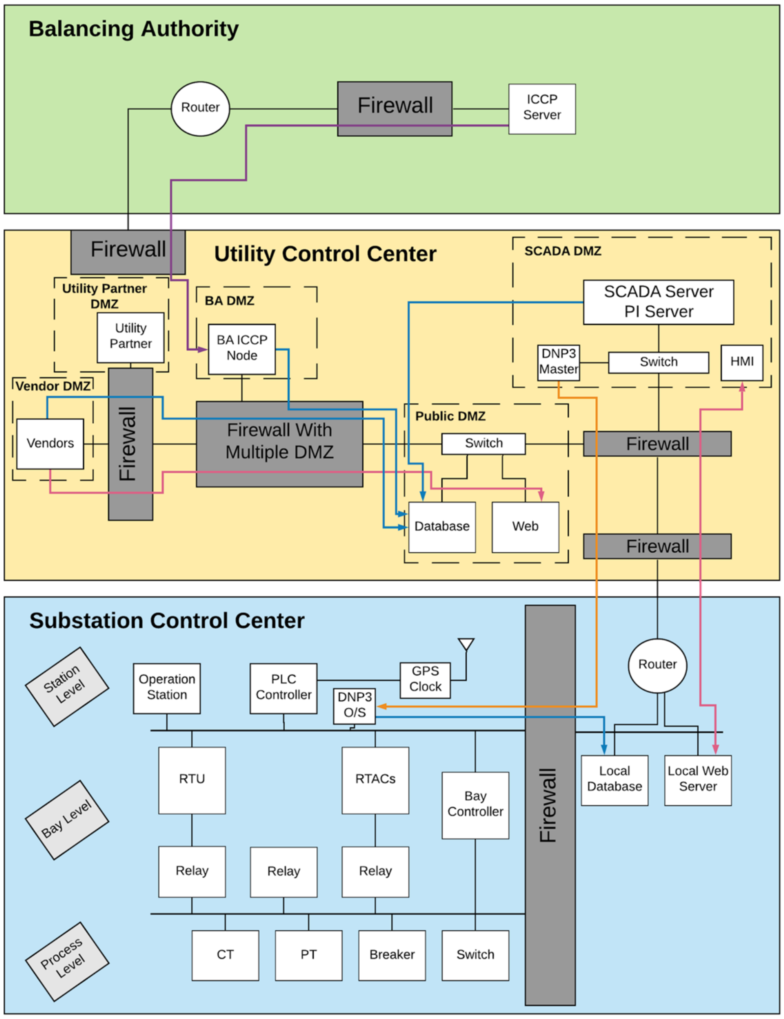


Figure 4.1: Hierarchical model of the synthetic communication network. Reprinted from [52,109].

attention to advance state-of-the-art critical infrastructure defense capabilities by fueling research to harden device and network security in CPSs.

Substantial research is directed toward developing test environments for critical infrastructure, to study systems without disrupting operations, ideally to promote detection of adversarial actions before they morph into attacks [113]. Building, connecting, and evaluating simulators and emulators [114–116] are important for network security research and experimentation. Virtual testbeds are gaining attention as cost-efficient means for performing scalable and realistic research [117, 118]. The simulator/emulator testbed environment can be built on machine virtualization tools such as VMware's vSphere server virtualization software [119], and Sandia's minimega, a set of open-source tools used to launch and manage VMs [120]. Relevant examples of emulators include Emulab [121] proven in [122] to uphold performance in scientifically rigorous experiments, DETER which targets the provision of a national cyber security experimentation resource [123, 124], and the National Cyber Range developed by DARPA as a test environment to assess advanced security threats [125].

However, there is a disconnect between network models used by research groups and the actual network topologies used in industry. These modeling differences lead to discrepancies between study results and what is attainable in the field. To address this, OpenConduit is designed to achieve automated and realistic replication of electric power system networks in an emulation environment by interpreting industrial networks' configuration data in CORE. CORE has been used to develop other testbed tools, such as the SCORE (Smart-Grid CORE) [118] that co-emulates a smart grid communication and power network. In these works, network topologies are manually added into the CORE GUI which is limiting and cumbersome for large-scale systems. OpenConduit overcomes these limitations by automating the process of rebuilding the network from just the system's configuration files, improving experiment scalability and accessibility for larger systems.

To the best of our knowledge, OpenConduit is unique in its ability to automatically recreate system networks, services, and datasets toward a realistic emulation platform from easily obtainable configuration files. OpenConduit emulates operational networks such that an application/program in the testbed can be directly mapped with the real system devices, e.g., network nodes can run services such as firewalls from the actual system and can route packets, using real or simulated industry network traffic. Scalably recreating these networks in emulation enables researchers to study many operational use cases and evaluate effects of network changes, anomalous cyber-physical events, and reconfigurations.

The main chapter contributions are as follows:

1. OpenConduit is introduced, as a tool which reads, parses and converts real system configuration files to simulated environments automatically. Hence, eliminating the possibility of

human errors that occurs in typical manual model designs nowadays. Additionally, it enables the emulation of large systems which otherwise would be a hassle for researchers with manual implementation.

2. OpenConduit enables fast and automatic emulation which is useful in cases where the underlying real system is reconfigured. In cases like this, the model gets updated in real-time accurately and in a timely manner.

3. OpenConduit captures, emulates and integrates both the cyber and physical dynamics as a true cyber-physical platform. This allows OpenConduit to continuously compare the dynamical evolution of the underlying real system with the emulated environment to vet the validity of its generated models in real-time.

4.2 OpenConduit Architecture

The OpenConduit architecture is illustrated in Fig.4.2, showing the recreation of the virtual nodes and their services in CORE. The nodes are able to generate and replay traffic from the packet captures. The applications employed include: NP-View, Wireshark, NetworkX, and CORE. The NP-View software by Network Perception performs compliance and security audits of firewalls within a utility network using the Critical Infrastructure Protection North American Energy Reliance Corporation (NERC-CIP) standards [61]. The compliant configurations serve as input files for OpenConduit to generate an emulated version of the communication network. Wireshark is an open source traffic sniffer that facilitates packet analysis, of captured local area network traffic (`.pcap` files) from the network interfaces of real systems, to generate traffic in the emulated network [126]. In this work, we use Scapy Python package [127] to process and modify the fields in the data packets that are captured from real devices using Wireshark. NetworkX is a Python package used for creating the structure and dynamics of a communication network in graph form [128] by applying graph theory principles. The NetworkX library is used in OpenConduit to rebuild the network in a graph form, with detailed node attributes like device type, IP, location, default gateway, and links with attributes like dataflow and bandwidth. CORE is a real-time network em-

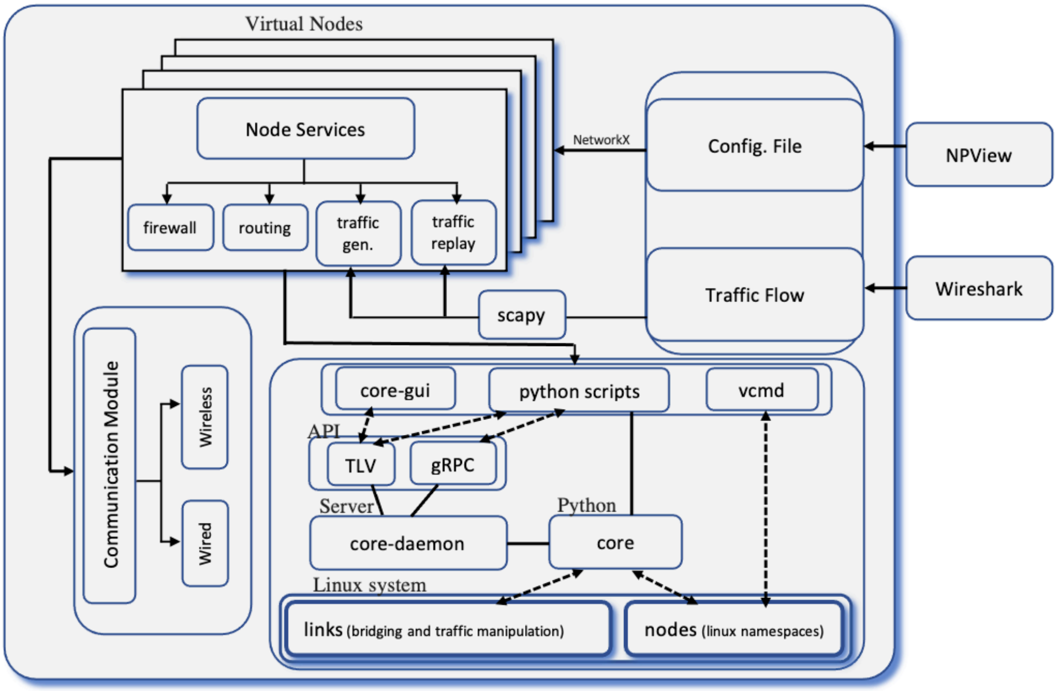


Figure 4.2: OpenConduit Architecture [107].

ulator that allows users to create communication devices such as switches, routers, computers, and custom network devices that run programs either as clients or servers [129].

4.2.1 Interaction with CORE

OpenConduit runs on CORE which runs on Linux OS. Users can execute configurable target services on the virtual CORE nodes. The virtual nodes are linked using virtual interfaces and Linux Ethernet bridging. The linking of these nodes forms the network that runs on sessions, which are managed by the core-daemon with different states: `definition` using GUI drawing scripts; `service configuration`; `instantiation` to create nodes, links, and interfaces; `run-time` to run interactive shells and generate traffic; `data collection`; and `shutdown` to tear down instantiated nodes and links. OpenConduit uses CORE's *gRPC* application program interface (API) to remotely add nodes and links to a session. The session will contain all the nodes and links connected as specified by the OpenConduit Python script. In the `core-daemon`, data packets are sent over links and handled using traffic control in the `core-gui`, which communicates with the `core-daemon` using the TLV API [130].

4.2.2 OpenConduit Workflow

OpenConduit has six steps as shown in Fig. 4.3. First, `PARSE` takes the files from NP-View and parses them into graph-readable form with attributes, services, connections, and geo-positional data. Also, NP-View files contain firewall rules that are parsed and translated into Linux *iptable* rules. Then, `FILTER` obtains details on the nodes and links of the graph, such as IP address and subnet mask. `CREATE` then builds the network topology from the attributes, adding the components into the CORE session with state set to `configuration`. Next, `ASSIGN` assigns different services to the nodes. For instance, host PCs are assigned default gateways, routers are assigned default routes, and *iptable* rules are assigned to edge routers. Then, `UPLOAD` uploads traffic to

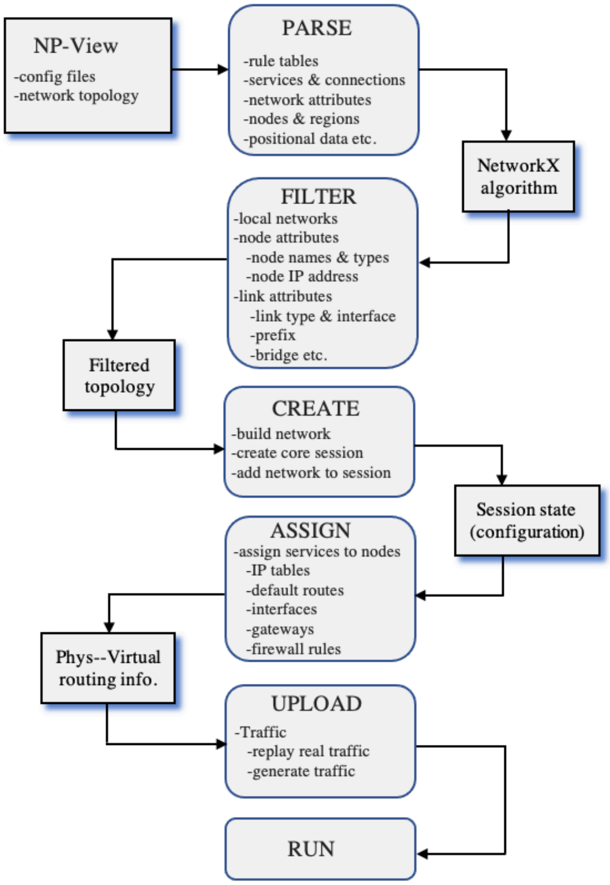


Figure 4.3: The workflow of the OpenConduit architecture [107].

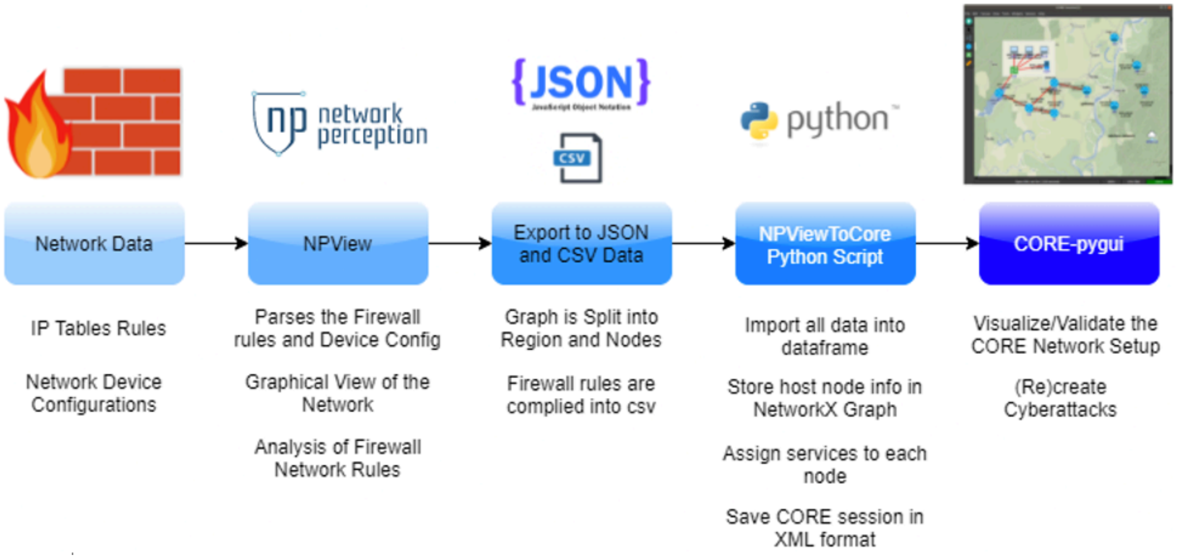

{JSON}
CSV
python
np network perception
Network Data
NPView
Export to JSON and CSV Data
NPViewToCore Python Script
CORE-pygui
IP Tables Rules
Network Device Configurations
Parses the Firewall rules and Device Config
Graphical View of the Network
Analysis of Firewall Network Rules
Graph is Split into Region and Nodes
Firewall rules are complied into csv
Import all data into dataframe
Store host node info in NetworkX Graph
Assign services to each node
Save CORE session in XML format
Visualize/Validate the CORE Network Setup
(Re)create Cyberattacks

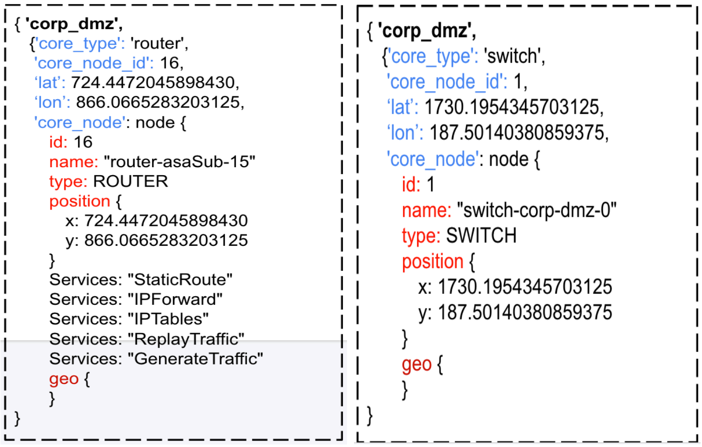
Figure 4.4: OpenConduit's NP-View to CORE pipeline. Reprinted from [107, 109]

the network. The traffic can be a real utility traffic or synthetic traffic that is based on real traffic statistics. Finally, the emulated system can be `RUN`, and different control commands can be sent to the nodes.

4.2.3 Network Model Extraction

The software pipeline as in Fig. 4.4 is discussed as follows. Three NP-View output files serve as configuration input for OpenConduit: `Network Topology Map`, `Asset Inventory`, and `Rule Tables`. `Network Map` specifies node/region information used to determine the local area network (LAN), such as substation or UCC network. The `Asset Inventory` file has the IP address of end-nodes, and `Rule Tables` are translated into Linux *iptables* to be configured in CORE's emulated firewalls.

The node attributes are stored in the NetworkX graph. Fig. 4.5 shows examples of attributes of a router and a switch. Nodes that belong to different regions are established using `Network Map` data. The data is formatted using developed algorithms such as Regional-Subset Algorithm, Adaptive Subnetting Algorithm, and Node Specific Allocation, discussed in [107].



```
{ 'corp_dmz',
   {'core_type': 'router',
    'core_node_id': 16,
    'lat': 724.4472045898430,
    'lon': 866.0665283203125,
    'core_node': node {
      id: 16
      name: "router-asaSub-15"
      type: ROUTER
      position {
        x: 724.4472045898430
        y: 866.0665283203125
      }
      Services: "StaticRoute"
      Services: "IPForward"
      Services: "IPTables"
      Services: "ReplayTraffic"
      Services: "GenerateTraffic"
      geo {
      }
}
```

```
{ 'corp_dmz',
   {'core_type': 'switch',
    'core_node_id': 1,
    'lat': 1730.1954345703125,
    'lon': 187.50140380859375,
    'core_node': node {
      id: 1
      name: "switch-corp-dmz-0"
      type: SWITCH
      position {
        x: 1730.1954345703125
        y: 187.50140380859375
      }
      geo {
      }
}
```

Figure 4.5: Attributes of nodes in the network stored as dictionaries in the NetworkX graph [107].

4.3 Evaluation

4.3.1 Conformity

OpenConduit is verified to conform with the power system network when the emulated network is visualized as shown in Fig. 4.6. First, the evaluation is done using the small-scale network, Fig. 4.1, with a total of 36 nodes including four routers and five firewalls with *iptables*, interconnected via switches which have the network address information.

4.3.2 Scalability

Next, the scalability of OpenConduit is evaluated using a real utility network of a partner utility that provided configuration files and traffic details, redacted for sensitivity reasons. The utility network consists of 166 nodes at a plant location. OpenConduit was able to scale up to automatically recreate 150 PC nodes, 12 switches, four routers, and a firewall. The custom script for adding default routes was automatically added to each of the PC nodes, allowing the PC nodes to communicate with one another, avoiding the need for manual updates before each session. The execution time and resource usage are also studied using the `psutil` Python package [131]. OpenConduit and the emulation are run on VMware's vSphere with Ubuntu Linux (64-bit). While execution time averages 59 seconds (Fig. 4.7), memory usage can be seen to increase as the storage

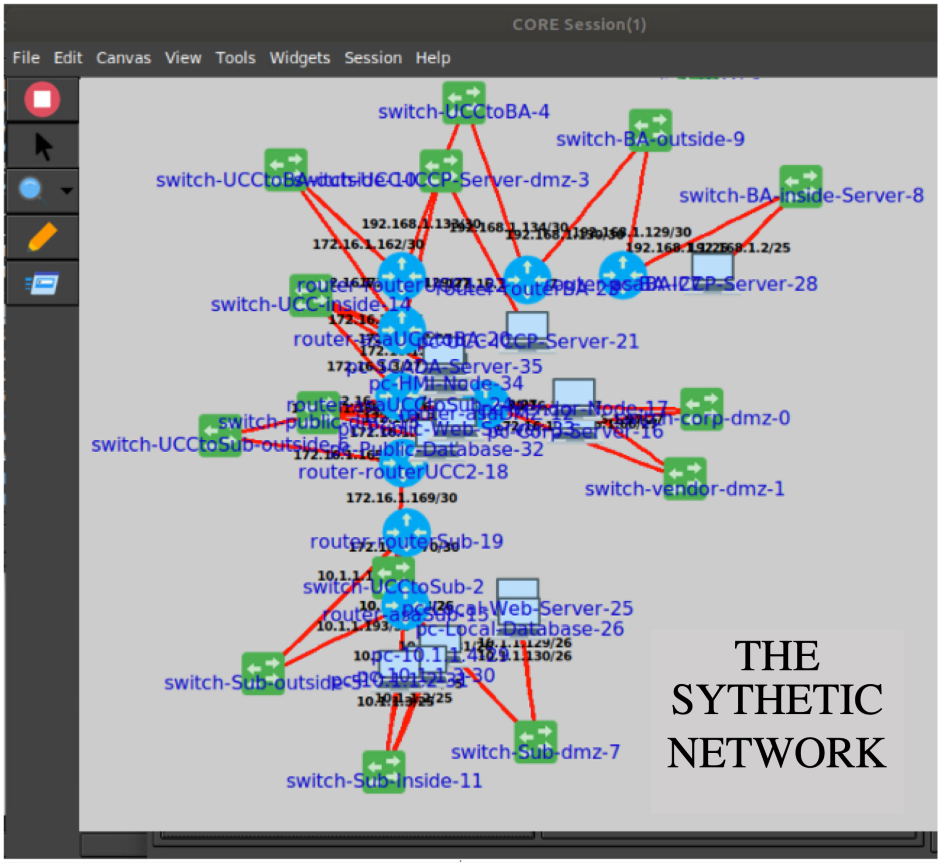


Figure 4.6: The results of OpenConduit in recreating the synthetic network [107].

of node attributes increases.

4.3.3 Functionality

The functionality of the nodes, links, and interfaces added in the re-built network are tested at runtime. We collected packets running through a node for five minutes, with about 9000 packets captured via the `eth0` interface.

4.3.4 Integrability

Services executing in emulated nodes can be ported to real devices/testbeds on Linux platforms. Hence, it is possible to integrate processes like IP forwarding for packet routing in the emulated node into Linux-based devices in a real system.

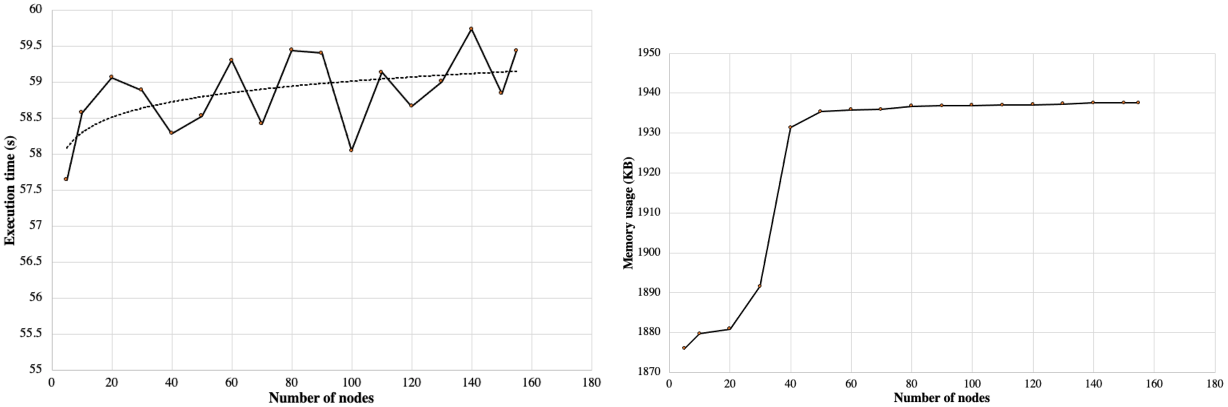


Figure 4.7: Execution time and memory usage for the emulated utility network [107].

4.3.5 Information Security

Security in data handling is crucial. OpenConduit protects sensitive industry data while enabling more realistic datasets for researchers. Toward this, a custom script extracts attributes from real traffic data to generate traffic on the emulated nodes. The packet attributes stored are limited to traffic type based on transport layer protocol, time interval between packets, packet size, and source and destination addresses, stored in JSON format ensuring that the emulation does not expose any sensitive information about the industry data. With the extracted packet attributes, the custom script on the node generates data traffic, which facilitates generation of larger datasets with more realistic networking constraints.

4.4 Conclusion

In this chapter, we have presented the design and implementation of OpenConduit, a tool to automatically recreate industry networks from configuration files. Designed for power systems, the tool is applicable to any network. The main function is to automate, in a scalable implementation, an organization's networks within an emulation environment.

4.4.1 Use cases

4.4.1.1 Power Network Digital Twin

A digital twin is a virtual representation of an object or system that spans its lifecycle, is updated from real-time data, and uses simulation, machine learning and reasoning to help decision-making. Digital twins are needed in critical infrastructure risk analysis since the operations of such systems have catastrophic effects when tampered with. Hence, such systems need a sandbox which can be used to learn about the system, its vulnerabilities, and the impact of such vulnerabilities. Hence, the OpenConduit tool meets this need by providing a digital twin for critical infrastructure network risk analysis by studying different scenarios including attack scenarios. As illustrated in the results, Fig. 4.8 created by OpenConduit is the digital twin of the small-scale test network. This usecase demonstrates how OpenConduit improves system resilience as well, by providing "Redun-

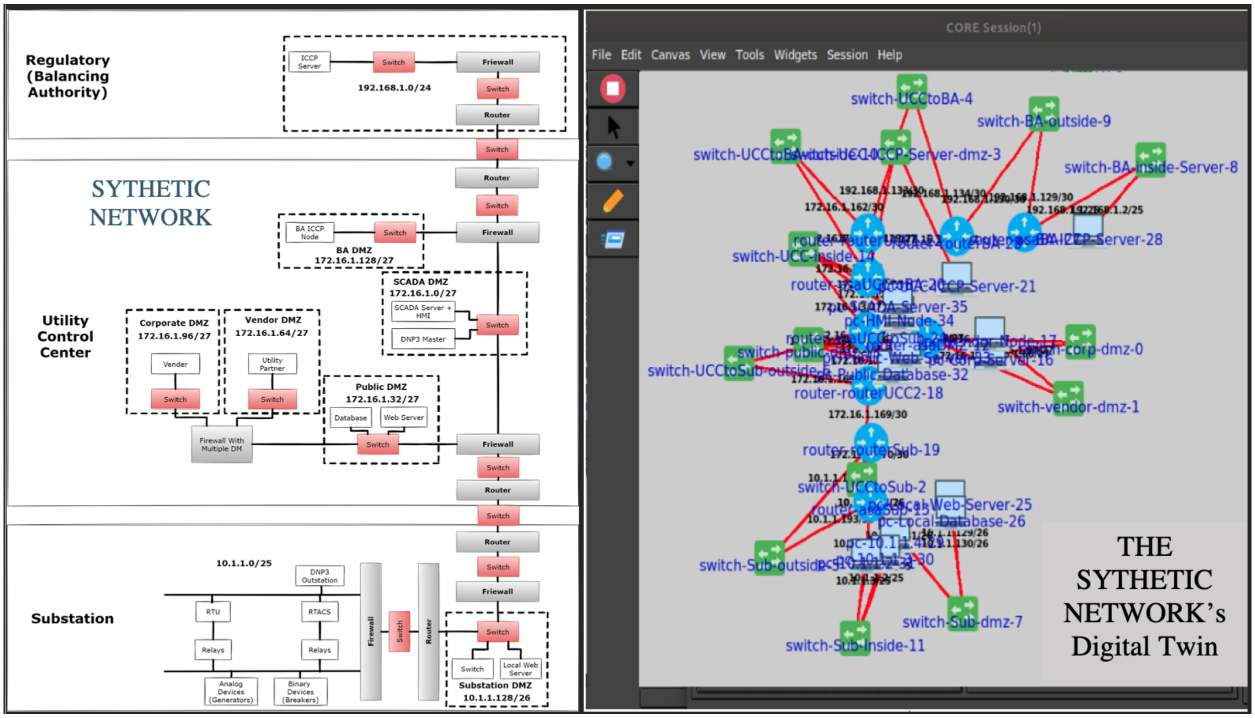


Figure 4.8: The Digital Twin of the synthetic network recreated by OpenConduit.

dancy", achieved through the duplication of the network and it's services. For instance, the virtual digital twin can be used for programs that train employees on different attack scenarios and effective response strategies. Real-time information provided by digital twins enable the optimization of system processes where arising issues can be tackled in real-time, ensuring peak performance and reduce downtime. Additionally, this tool can provide to power systems the remote monitoring capability, hence, fewer trusted personnel could be granted access to the actual system.

4.4.1.2 Cyber Deception

Cyber deception is proactively defending the power network by leading the adversary to less risky, no-true-damage-impact environment with the aim of learning the adversary's objective from the attack tools, methods, and behaviors. According to [132], cyber deception is a set of planned, deliberate, and controlled actions to conceal the network, create uncertainty and confusion in the adversary's mind, delay and manipulate his efforts to establish situational awareness, and to influence and misdirect perceptions and decision processes, thereby causing them to take or not take actions that are beneficial to the defender's security posture. The value of cyber deception lies in: 1.) revealing the power system's security posture, risks and functionality likely to be attacked, and 2.) leading the adversary intentionally through the network in order to reveal adversary motives, intentions, and techniques. With these values, the power system can obtain important information including: OpenConduit enables the cyber deception use case where the rebuilt network can be setup as a honeypot for the power system network as shown in Fig. 4.9, where the tap interface can be used to connect the virtual network created by OpenConduit to the real power system network, allowing the virtual network serve as a honeypot since it is emulated with network-authenticity capabilities including reflection of active network data such as DNP3 traffic from the SCADA server to the substation relays, user interaction and network presence.

4.4.1.3 Proactive Intrusion Response and Decision Making

OpenConduit facilitates dynamic risk assessment in real-time emulation, where threat scenarios of a false data injection attack which may use techniques such as Address Resolution Protocol

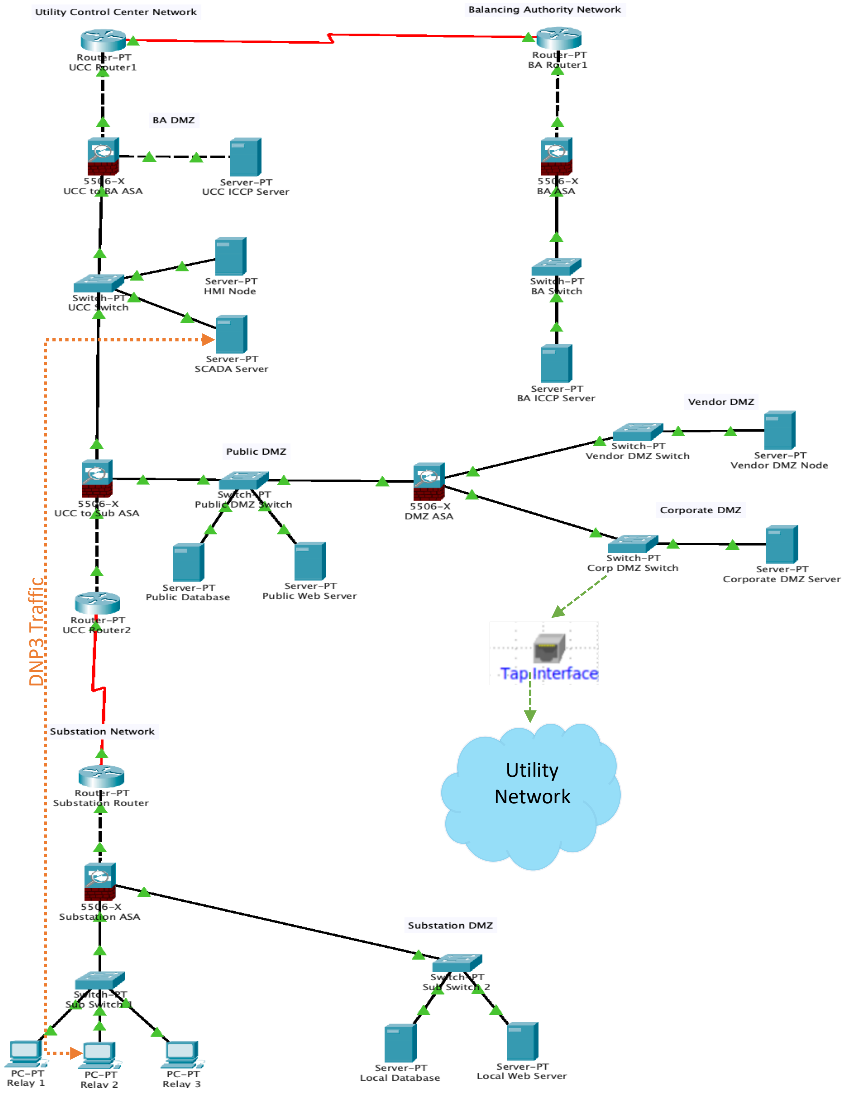


Figure 4.9: Cyber deception usecase: A network automatically built by OpenConduit can serve as a cyber deception network for power systems. The built network can be connected from CORE to the power utility network and serve as a honeynet, running similar but false-payload traffic e.g., DNP3 traffic used in SCADA.

(ARP) spoof-based Man-in-The-Middle (MiTM) attack, communication loss via Denial of Service (DoS), etc., can be studied by collecting traffic and sensor data from different nodes in the emulated network. The patterns in these attacked network can be modeled towards proactive detection, using adversary indicators, to learn about adversary objectives and motivations.

1. Adversary Information: The emulated honeynet can be used to obtain information such as

adversary identity, motive, techniques, objectives, knowledge level of the network (which can guide investigations from internal adversaries), capacity of exploitation.

2. System Information: The emulated honeynet can expose information such as zero-day network vulnerabilities, how different vulnerabilities that can be leveraged by adversary, risk and impact of adversary intrusion or attack, efficacy of current security controls and compliance.

These information can aid the system stakeholders to implement risk frameworks that enable informed decision making. For instance, OpenConduit provides a digital view of the power system network, where anomalies and faults can be identified and flagged for operator action proactively, rather than waiting until the system breaks down.

5. DATA-DRIVEN SPATIO-TEMPORAL ANALYSIS OF WILDFIRE RISK TO POWER SYSTEMS OPERATION [*]

This chapter initiates the studies, designs, and implementations developed towards the resilience-oriented risk reduction for the critical cyber-physical power system to the physical threat of wildfires.

5.1 Introduction

The increasing magnitude and frequency of power outages induced or motivated by wildfires affects the operation of critical services and leads to lost opportunity costs [134]. The United States suffers considerable economic loss from wildfire events. In California in 2018 alone, wildfire events cost the U.S. 0.7% of the country's GDP, while Butte County where the Campfire occurred suffered indirect losses of approximately 50% of its GDP [135] on a single wildfire event. This is a slippery slope given that multiple wildfire events can occur in the same wildfire season (e..g., in the same day, week, or months). The California Department of Forestry and Fire Protection estimates damages from the 2018 Woolsey and Camp fires to be about \$4 and \$11 billion respectively [136] with Campfire responsible for about 84 deaths [137]. Additionally, wildfire threats in October 2018 and 2019 led Pacific Gas and Electric (PG&E) to shut off power to a sizeable number of customers in extreme risk areas of northern California leading to lost opportunity costs when no wildfires occurred [138]. Subsequently, the 2020 Zogg fire saw PG&E facing 31 criminal charges, including manslaughter, for the utility's role in the fire that claimed 4 lives and destroyed more than 200 building properties [139]. More recently, the 2021 Dixie fire was caused by the blowing of two fuses when a Douglas fir fell on a PG&E line [140]. The fire gulped more than \$630 million in suppression efforts and led to tangible losses including damages to approximately 1500 residential and commercial property, injuries and fatalities [141].

[*] ©[2021] IEEE. Reprinted, with permission from, Umunnakwe A, Parvania M, Nguyen H, Horel JD, Davis KR., "Data-driven spatio-temporal analysis of wildfire risk to power systems operation," in IET Generation, Transmission & Distribution, vol. 16, no. 13, pp. 2531-46, Jul 2022, doi: https://doi.org/10.1049/gtd2.12463 [133].

In response to wildfire threats, utilities have significantly invested on wildfire monitoring systems and analytical tools, which generally rely on observations from remote automated weather stations to evaluate current weather conditions [142] that are disseminated and retrieved [143] from many sources such as Synoptic's Mesonet API. These data are then used to estimate and strategize for optimal operation in the face of wildfire threats, but with room for improvements. In fact, the decisions of a utility to shut off power to more than sixty thousand northern California customers in 2018 and nearly a million in 2019, was controversial [144]. It may be, however, impossible to assess if this was an overestimation of impact and utility resources ("conservative"), but the passing of the California Senate Bill 901 required states investor-owned utilities with the California Public Utilities Commission to file wildfire mitigation plans, increasing research on the topic [145].

Studies on wildfire prediction and estimation [146–148] have mainly focused on numerical quantification [149] and fire scale [150], often using techniques such as regression [151], in an effort to aid mitigation. In [152], wildfire variables are studied to predict spatial patterns of ignition producing national-level ignition risk maps. To aid pre-wildfire planning, [153] implements fire danger mapping system based on numerical weather prediction and derived moisture content of live fuels. Historical data for vegetation, climate and locational features have been utilized in [154] to predict the risk of wildfire ignition. However, these region-specific wildfire models are simply aggregated over space or time with approximated/linear and spatially constant effects [155]. Hence, their accuracy can be affected by the limited integration of the non-linear influence of variables, and similarly, do not fully utilize recent wildfire monitoring investments of grid utilities. Wildfire risk prediction has also been done where model performance using machine learning approaches have been evaluated [156]. Artificial intelligence techniques have also been effective for wildfire analysis and outperform conventional statistical methods [157–159]. Additionally, interactive maps have been garnering literary and industry application to supply information on wildfires in real-time. For instance, in [160], a real-time fire prediction system is developed for visualizing wildfire risk at specific locations based on a machine learning model.

Although these methods prove effective, they generally have not been designed to integrate with the power grid operations. The effect of this on the power system side is the assumption of already progressing wildfires, while geographical uncertainties of spatio-temporal variables are often assumed [33] and not investigated. For instance in [161], energy dispatch is optimized assuming an already progressing wildfire. The same progressing wildfire assumption is applied in[162] to dynamically change thermal ratings of power lines and in [148] to optimize resource preparation.

Conventionally, electric power utilities have often performed fundamental analysis to indicate wildfire threat alert on coarse resolutions of spatial areas while not utilizing the richness of historical data, evident in indices such as the Fire Potential Index [163]. This index, for instance, utilizes a linear summation of present weather variables and fuels to provide threat levels (extreme, elevated, normal) for predefined regional-scale threat areas. This may arguably lead to over-estimation of risk, over-allocation of operational resources, and consequently "conservative" risk analysis for utilities.

This chapter develops a deep learning based framework for analyzing the expected spatio-temporal impacts of stochastic wildfire threat on the power grid. The proposed framework, as shown in Fig. 5.1, integrates a detailed spatio-temporal wildfire analysis model to evaluate system risk. The model incorporates information from real databases towards potential wildfire ignition maps, as the spatio-temporal wildfire "readiness" of a location does not necessarily imply an ignition until a fire source is applied. Therefore, a model is proposed to estimate the spatio-temporal probability of a potential wildfire ignition which can be applied to power transmission and distribution systems. The advantage in modeling potential ignitions pre-wildfire is to prepare for critical scenarios and proceed with optimal strategies to better mitigate risks arising from extreme wildfire events, thereby reducing the propensity of outages and power shutoff to customers. As wildfires can be caused by power equipment failure or by exogenous causes (human, natural events), the applications of the estimation result are twofold. First, it provides spatio-temporal risk for proactive de-energization against potential power system failure-induced wildfire [33]. Second, it generates a spatio-temporal spreading model for optimal grid operations against potential exogenous wildfires

[148]. In summary, the main chapter contributions are as follows:

- We develop a comprehensive spatio-temporal wildfire risk analysis framework using a data-driven deep learning approach that efficiently incorporates publicly-available historical data for estimating wildfire ignition risk and its impact on power grid.
- Novel quantitative risk metrics that capture potential effects of fuel, vegetation, and wind speed, on wildfire propagation are proposed, while the weighted impacts of wildfire predictive variables are furnished to aid utility operations and stakeholder strategy.
- The framework provides information to utilities towards optimizing grid operation, i.e., proactive de-energization to prevent endogenous power system failure induced wildfire and the response strategy e.g., “let-burn”, against exogenous wildfire threats.

5.2 Overview of the Proposed Model

Wildfires are influenced by a number spatial and temporal factors that can be unique in different geographical locations which can lead to inaccuracies in prespecified mathematical models. Hence,

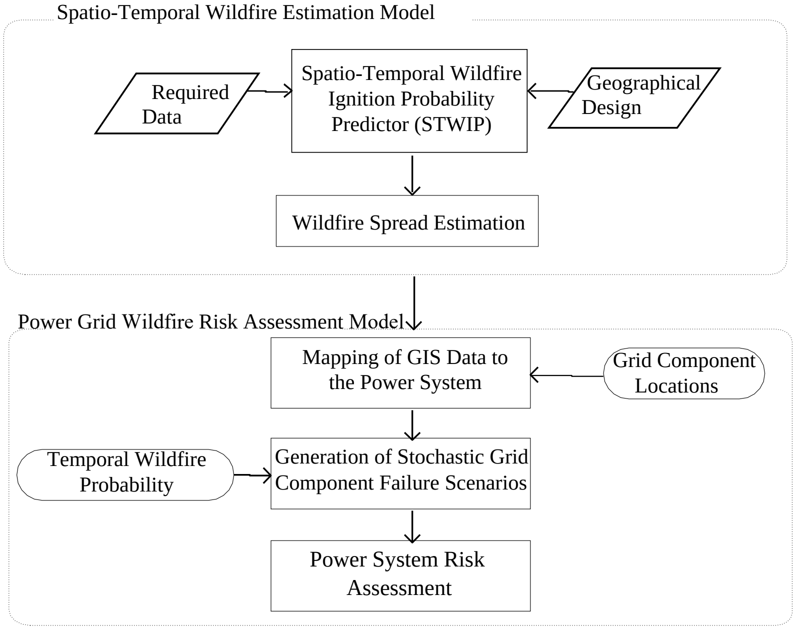

Spatio-Temporal Wildfire Estimation Model
Required Data
Spatio-Temporal Wildfire Ignition Probability Predictor (STWIP)
Geographical Design
Wildfire Spread Estimation
Power Grid Wildfire Risk Assessment Model
Mapping of GIS Data to the Power System
Grid Component Locations
Temporal Wildfire Probability
Generation of Stochastic Grid Component Failure Scenarios
Power System Risk Assessment

Figure 5.1: Structure of spatio-temporal wildfire risk assessment model

the objective of the proposed framework is to drive operational strategy with data-driven situational awareness to wildfire. As in Fig. 5.1, the framework consists of two sequential stages. First, the *spatio-temporal wildfire estimation model* predicts the probability of potential wildfire ignition, utilizing the spatio-temporal wildfire ignition probability predictor model (STWIP), and estimates potential wildfire spread, producing important parameters such as ignition probability maps and the rate of spread of potential ignitions to critical power components. These parameters are then passed to the proposed *power grid wildfire risk assessment model*, which aims to optimize power system operations and risk assessment such that outage cost is minimized. The risk assessment model optimizes power system operations by GIS-enabled mapping of these parameters to the power network and generating wildfire threat scenarios. Part of the risk assessment model also includes proposed power system-wildfire metrics that enable optimal operational strategies such as choosing mitigation vs. restoration ("let-burn").

5.2.1 Geographical Structure of the Model

A spatial location is a point i with geospatial coordinate $i.loc$ defined by a latitude and longitude *(lat,lon)* at any location in a grid cell. The grid cells here are 3km $\times$ 3km polygons which have uniform past spatio-temporal wildfire characteristics and a centroid. Each grid centroid also has geospatial coordinates $g_c.loc$. For instance, the past spatio-temporal characteristics of a historical sample ignition occurred in i is obtained by its association with $g_c.loc$ of the grid cell $g \in G$ in which it is situated, since the centroid is processed to bear the characteristics of g. Each grid has a set of historical wildfire ignition events with geospatial coordinates $i.loc$. These historical events, which form sample points in the training data, have a set of variables, $\mathbf{x} = [x_1, x_2, ..., x_D]$, obtained for their unique $i.loc$ and dates of ignition. Here, D denotes the dimensionality. These wildfire-informative variables are referred to as Wildfire Predictor Variables (WPVs) and are usually sourced from weather stations geographically situated at locations of interest. Their interactions and correlation can be modeled towards wildfire prediction. They can vary spatially and/or temporally, are indicative of wildfire occurrence, and are often called explanatory variables [164].

5.2.2 Data Requirements

The proposed framework proceeds with data pre-processing and integration (solid green arrows), feature extraction and training the predictor (solid black arrows), these precursors are as illustrated in Fig. 5.2 and discussed as follows.

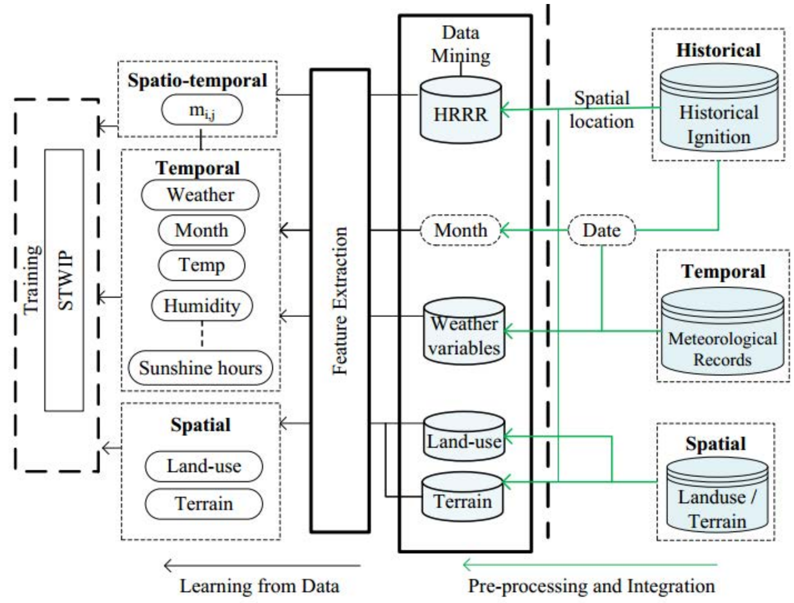


Figure 5.2: Spatio-temporal wildfire prediction model

5.2.2.1 Data Pre-processing

This stage proceeds with obtaining the grid centroids together with spatial data e.g., land-use and terrain data, from databases such as the National Oceanic and Atmospheric Administration's High Resolution Rapid Refresh (HRRR) model [165]. The temporal probabilities, π_j of wildfire ignition, as shown in Appendix A.4, are also calculated in this stage from the US Geological Survey historical ignition data and can be used as a feature to improve estimation. This assumption of a same climate period is enabled by the similarity in the data distribution over the historical period of analysis as illustrated in Appendix A.2, Fig. A.1. Also in this phase, the python scrapper is coded to request and clean meteorological data for unique spatial locations on days of interest. These days of interest depend on user applications but for this work, meteorological variables on historical ignition and non-ignition days are duely processed for training/validation of the predictor while forecasted meteorological variables are requested for days that wildfire potential is to be predicted.

5.2.2.2 Data Integration

The next phase is data integration which proceeds in two levels. The first is the spatial integration, where $i.loc$ of historical ignitions are associated to $g_c.loc$ to obtain the past ignition characteristics of g. The goal here is to enable spatial locations in the training data inherit wildfire attributes of the grid cell in which they are located. The second occurs after feature extraction during integration into python's pandas dataframes in preparation for training. This dataframe is a two dimensional data structure with columns of multivariate data. The month in which the training ignition sample occurred is incorporated as a feature to account for temporal relation of features, and is also critical to the utilization of only one fundamental deep network.

5.2.2.3 Feature Extraction

5.2.2.3.1 Past Spatio-Temporal Ignition: This feature captures sequential changes in characteristics of spatial wildfire ignition over time and is crucial in the capability of the predictor to use one fundamental deep network. It is calculated from the historical wildfire database and is the initial (historical) ignition probability of a spatial location in the same climate period. To this end, we compute the past wildfire ignition probability $m_{g,j}$ of a grid cell g in period j of our comprehensive year. Since this attribute is inherited by all i in grid cell g, we refer to this attribute as $m_{i,j}$. Specifically, because the climate pattern of the multiple-year-dataset is assumed constant, the conditional probability of an ignition occurring in grid cell i given the study area, is used to calculate $m_{i,j}$ given that grid cells are a subset of the studied geographical area as in (5.1).

$$m_{i,j} \approx \frac{n_{g,j}}{N}, \tag{5.1}$$

where $n_{g,j}$ is the total number of wildfires occurred in cell g in period j, and N is the total number of wildfires that occurred in the multiple year period. Assuming constant climate, the multi-year period (e.g., 1996-2016) can be modeled as a comprehensive year. As mentioned earlier, in order to enhance the computation of $m_{i,j}$ considering the scarcity of historical ignitions in some grid cells, the Monte Carlo population technique is employed in pre-processing the original dataset to further populate grid cells.

5.2.2.3.2 Temporal Meteorological Features: Wildfire occurrence is influenced by non-linear and complex meteorological features which are temporally related. Temporal meteorological input includes temperature, rain, humidity, sunshine hours. The choice of these features are informed by indices such as the Angstrom, Nesterov, and Canadian Forest Fire Weather Index as well as the US Fire Danger Rating System [166].

5.2.2.3.3 Spatial (Static) Features: These features characterize spatial locations for same climate periods and are influential to wildfire occurrence [167]. Spatial data of land-use and terrain can be obtained from sources such as the HRRR model which have standard grid points that can serve as grid centroids and enable division of the studied geographical area into grid cells with the same spatial and spatio-temporal features. Historical ignition events that fall within a grid cell are used to obtain $m_{i,j}$ of the respective cells which are in turn inherited by the sample points i within g, during training.

In addition, the past ignition probability and ignition month are also included as spatio-temporal and temporal features respectively. Additional details can be found in Appendix A.1 and A.3.

5.2.2.4 Data construction

Here, we discuss the logic behind constructing the training data as there is little to none pre-existing for wildfire analysis. Since training samples are based on historical ignition/non-ignition days, the dates (dd/mm/yy) and corresponding $i.loc$ are extracted from the historical ignition database and are utilized to automatically request training sample variables. Once the features are extracted from obtained variables, this training sample point is assigned with a classification label 1, meaning the historical status of ignition was active for the sample. Next, the feature data are requested for the same $i.loc$ and another (dd/mm/yy) prior to the active ignition date, when no wildfire ignitions were reported to have occurred and this is labelled a 0, meaning that the historical status of ignition was inactive for the sample. In particular, the ignition label for a training sample is defined as:

$$Ign = \begin{cases} 1, & \text{if} \quad ign_{(j)}\ recorded \\ 0, & \text{if} \quad ign_{(j-n)}\ \neg recorded \end{cases} \tag{5.2}$$

where Ign is the historical wildfire ignition status in day j, and $n = \{1, 2, ..., 30\}$ depending on any day in the given month and year where an ignition was not recorded. This process constitutes the dataframe for training the STWIP. For the 0-labelled samples, dates prior to ignition (1-labelled sample) of an $i.loc$, are chosen since historical ignition could have significantly tampered with temperature, fuel and vegetation, rendering later dates deceptive for use as 0-labelled training samples. It is worth noting that although we assume true absence points, these 0-labelled samples are pseudo-absence points since it is unknown if ignition could not occur (there was no potential for ignition) or simply did not occur (there was no source of ignition) in that historical date and $i.loc$.

5.3 Spatio-Temporal Wildfire Estimation Model

After data construction, the dataframe is fed into STWIP as input data following some transformations discussed herein. The input data is cleaned, missing values are filled with an average of their nearest neighbors. A major part of training data processing includes rescaling the features to have the properties of a standard normal distribution ($\mu = 0, \sigma = 1$). The need for rescaling arises as features are multivariate with different units. Also, since feature magnitudes in instance $\mathbf{x}_i$ play a role in the updates applied to the weights during gradient descent, rescaling becomes important. This standardization is implemented using the Z-score as follows:

$$z = \frac{x - \mu}{\sigma}. \tag{5.3}$$

Then STWIP predicts the expected ignition potential of a spatial location in period j as discussed further.

5.3.1 Spatio-Temporal Wildfire Ignition Probability Predictor

The aim is to train a neural network with the problem objective formulated as follows. Given a collection of sample points i with geospatial coordinates $i.loc$ of *(lat,lon)* $\in$ historical ignition data, where features of the sample point i are known, we aim to predict the potential of a wildfire ignition at periodic intervals. We propose a model based on supervised learning of spatial, spatio-temporal and temporal features to capture complex and non-linear interactions between WPVs using a deep neural network (DNN). The DNN is the prediction algorithm of the STWIP and unlike traditional methods of wildfire estimation with simple logistic regression [151, 168], the DNN is capable of modeling non-linear correlations between the WPVs as illustrated in (5.4), and can update the network's basis functions in specific input space directions.

$$\widehat{y} = \sigma\left(\sum_{h=1}^{H} w_{oh}^{T} h\left(\sum_{i=1}^{D} w_{hi}^{T} * x_i + w_{h0}\right) + w_{o0}\right), \tag{5.4}$$

where **w** is the vector of adjustable weight parameters, with input variables x_i, σ is a threshold function, and $\{i, h, o\}$ represent the input, hidden, and output layers. By adjusting the weight vector through different training epochs the predicted labels are mapped closer to the target labels, estimating the probability of potential wildfire ignition, $\pi_{i,j}$, as follows:

$$\pi_{i,j} = f(\mathbf{x}). \tag{5.5}$$

The STWIP architecture is a three layer fully connected network as shown in Fig. 5.3, utilizing the Adam optimizer, ReLU activation, and softmax activation at the output layer. The hidden layers' (12,3) neurons, respectively, are chosen to avoid over-fitting and enhance prediction accuracy.The data input, **x**, is fed into the input layer. The output layer consists of two neurons that output probabilities of potential ignition/non-ignition in one hot encoded format. The network is trained and minimized over the cross-entropy loss. The trained STWIP is illustrated in Algorithm 6 in Appendix A.5.

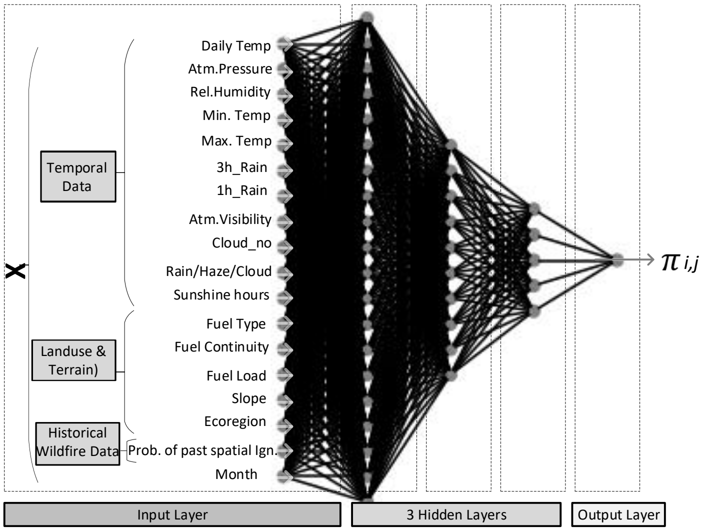


Figure 5.3: The STWIP training model. Predicting the probability of ignition $\pi_{i,j}$ in a location i at time j using a set of spatio-temporally engineered input features $\mathbf{X}$.

5.3.2 Wildfire Spread Estimation

In modeling wildfire behaviors including spread, software such as Prometheus and Burn-P3 have been developed, but however, may require predefined inputs such as initial ignition grids from all historical fires, the different ecoregions, percentage of escaped fires and more, which may not be readily available to the user. In literature, models such as the FLAME [169] have been developed to rely on observable field assessments to consider areas of high fire spread rates. In [170, 171], the developed model seeks to attain the fire front using a variation of the Thomas Equations shown in (5.6) and (5.7).

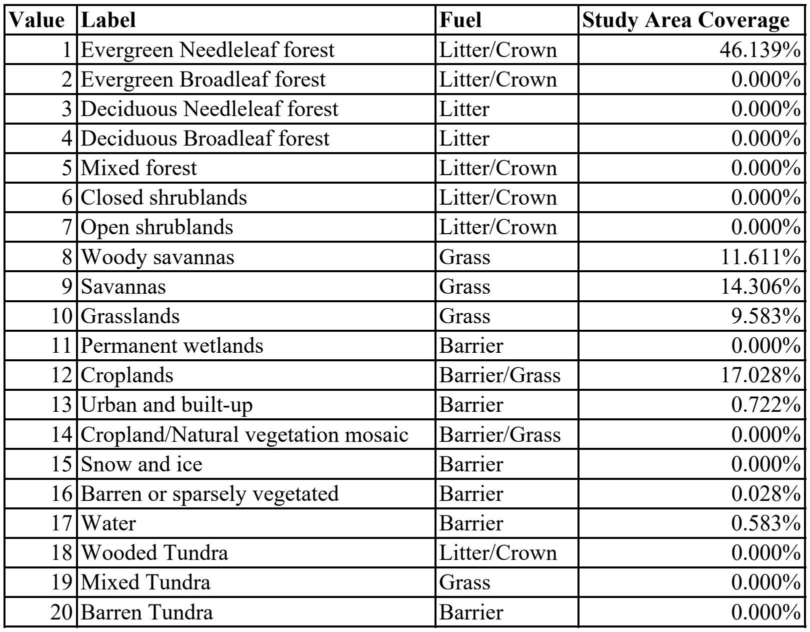
$$V^f = \frac{k(1+V_w)}{\rho_b} \tag{5.6}$$

$$r^f_{i,j,\omega,t} = r^f_{i,j,\omega,t-1} + V^f_{\omega,t}\ \Delta t\ cos(\phi^{\omega}_{i,j,\omega,t}) \tag{5.7}$$

where V_w is wind speed, k is fire-type parameter, ρ_b is the bulk density, r^f is the radius from the initial ignition point to the fire boundary, and ϕ^w is wind direction.

However, if a wildfire ignites in a cell i in period j, its spread rate depends on surrounding fuel types and wind speed, which can be captured by the wildfire-fuel spread characteristics. Hence, we adapt an approximate radial spread rate using the FireLine Assessment MEthod [169], that can be determined by assessing the fuel type and wind speed at each HRRR grid point nearest to the potential wildfire ignition location. In this paper, instead of arbitrary values of spread rates, practical datasets that adapt the considered geographical area to different fuel types is utilized.

Table 5.1: Mapping service area vegetation to fuel type for wildfire spread estimation



Value	Label	Fuel	Study Area Coverage
1	Evergreen Needleleaf forest	Litter/Crown	46.139%
2	Evergreen Broadleaf forest	Litter/Crown	0.000%
3	Deciduous Needleleaf forest	Litter	0.000%
4	Deciduous Broadleaf forest	Litter	0.000%
5	Mixed forest	Litter/Crown	0.000%
6	Closed shrublands	Litter/Crown	0.000%
7	Open shrublands	Litter/Crown	0.000%
8	Woody savannas	Grass	11.611%
9	Savannas	Grass	14.306%
10	Grasslands	Grass	9.583%
11	Permanent wetlands	Barrier	0.000%
12	Croplands	Barrier/Grass	17.028%
13	Urban and built-up	Barrier	0.722%
14	Cropland/Natural vegetation mosaic	Barrier/Grass	0.000%
15	Snow and ice	Barrier	0.000%
16	Barren or sparsely vegetated	Barrier	0.028%
17	Water	Barrier	0.583%
18	Wooded Tundra	Litter/Crown	0.000%
19	Mixed Tundra	Grass	0.000%
20	Barren Tundra	Barrier	0.000%

The study area is mapped, by a consulted fire expert, Robert Ziel [172], to three common fuel types namely crown, litter, and grass as illustrated in Table 5.1 which also shows the coverage of each fuel type in our study area in northern California. Hence, this paper considers three common vegetation/fuel types (crown, litter, and grass) with spread rates modeled as a function of wind speed, W, as in (5.8) and as shown in Fig.5.4. Note that in the case of multi-fuel types such as litter and crown, the fuel type with higher spread rate was chosen. Constant but atypical wind speed directed towards the power system components is assumed, in order to account for the worst case scenarios of wildfire spread in the spatio-temporal assessment.

$$\begin{aligned} \omega_{\text{grass}} &= 14.4(W)^{1.232}, \\ \omega_{\text{crown}} &= 4.87(W)^{1.146}, \\ \omega_{\text{litter}} &= 1.03(W)^{1.213}. \end{aligned} \tag{5.8}$$

Armed with the potential rate of spread of the wildfire, utilities are able to optimize operations based on parameters such as expected distance and the time it takes a potential ignition to reach critical grid components.

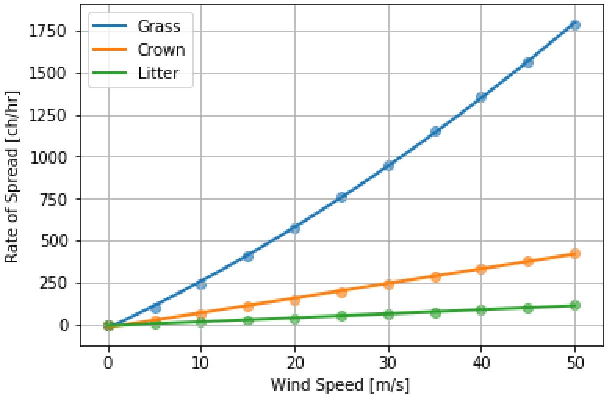


Figure 5.4: Rate of Spread as a function of wind speed (1 ch/hr = 0.005588 m/s)

5.4 Power Grid Wildfire Risk Assessment Model

This section presents the proposed model for the power grid risk assessment, utilizing the outputs of wildfire estimation model presented in Section 5.3. The wildfire potential ignition map (ignition probability map), produced by the STWIP, aids in proactive de-energization to prevent endogenous fires caused by power system failure [33] while the spread estimation aids improvement in adaptive operation of power grid against exogenous wildfires [148]. Specifically, a set of grid component outage scenarios are first generated by incorporating the output parameters of the first stage estimation model with GIS information of the power grid. In particular, given $\pi_{i,j}$, scenarios are sampled given the distribution of the wildfire potential ignition map and potential ignition locations, generating expected scenarios for the power system risk assessment model. Note that the granularity of $\pi_{i,j}$ can be improved to hourly depending on user application. In this paper, we estimate the hourly probabilities from $\pi_{i,j}$ as follows:

$$(1 - p_{i,h})^H = (1 - \pi_{i,j}) \tag{5.9}$$

where $p_{i,h}$ is the hourly probability of potential wildfire ignition in i, and H is the cardinality of hours in day j. Based on these scenarios, three risk metrics, namely, critical response time, scenario based damage cost, and expected damage cost are calculated to assess risk.

5.4.1 Power Grid Outage Scenario Generation

We aim to generate the outage scenario of grid component c at time t of operational day j of the year. Assume that the wildfire ignition happens at time $t^* = 0$, and we aim to assess the operation of power grid for the subsequent 24 hours after the potential incident. In other words, the utility operator's thought process is: "if the potential wildfire occurs given scenario, s, and I have knowledge of the spread rates given s, I should estimate what component outages can be induced or motivated by this fire so I can be better prepared for such scenarios". Let π_s denote the probability of occurrence of scenario s corresponding to a set $\mathcal{I}_j^s$ of potential ignition locations of day j. The spreading rate ω_i^s of the ignition in location i in scenario s is obtained by using the spread model presented in Section 5.3.B with the corresponding values of forecast wind speed and fuel types around i. The GIS data of the power grid is mapped into the considered area. The characterization of a wildfire induced (exogenous) grid outage scenario is illustrated in Fig. 5.5. In particular, the component (e.g., transmission line) is assumed to be damaged if the potential fire crosses its safety zone defined by Δ_c and the status of power grid component c is characterized by a scenario dependent parameter $\delta^s_{c,t}$ as:

$$\delta^s_{c,t} = \begin{cases} 0, & \text{if } \min\limits_{i \in I^s_j} D^i_c - \omega^s_i \Delta t > \Delta c \\ 1, & \text{if } \min\limits_{i \in I^s_j} D^i_c - \omega^s_i \Delta t < \Delta c \end{cases} \tag{5.10}$$

where $\Delta t = t - t^* = t$ $(t^* = 0)$ is the potential duration of the wildfire spread, D^i_c is the Euclidean distance from the potential ignition point i to the grid component c, and $\omega^s_i \Delta t$ is the spreading radius of the wildfire from its ignition point. Note that (5.10) considers potential wildfire ignition with spread closest to component c, since multiple ignition points can possibly occur in a scenario s, which was reportedly the case in the infamous Campfire. Also, when a component is on outage ($\delta^s_t = 1$), we assume it continues to be out until the end of the considered operation horizon. The value of Δ_c can be adapted from numerical determination of the Acceptable Safety Distance [173], which furnishes a detailed thermodynamics of wildfire effect on system components, informed by flame characteristics and a vulnerability threshold. The safety distance is informed by flame characteristics and a vulnerability threshold, and is the distance between the transmission line and the fire at which the thermal radiative flux is less than a given threshold, Φ_{thresh}. The threshold value is set to the vulnerability of transmission lines. The safety adapted distance is determined by the following correlation:

$$D_x(opt) = D\left(1 - exp\left(-p_{thresh}\tfrac{2L}{l_f}\right)\right), \tag{5.11}$$

where p_{thresh} is a pre-determined empirical parameter for each Φ_{thresh}, l_f is the flame length, $2L$ is the width of fire, and

$$D = \frac{l_f cos\gamma\sqrt{-4\Phi^2_{thresh} + (BT^4_f \varepsilon\tau)^2}}{2\Phi_{thresh}} + I_f sin\gamma, \tag{5.12}$$

where τ is the atmospheric transmissivity, ε represents flame emissivity, B is the Boltzmann constant, and T_f is the average temperature of the flame.

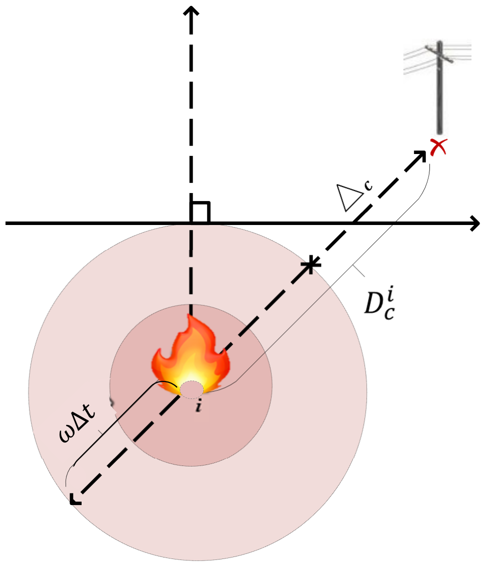


Figure 5.5: Wildfire-induced outage scenario generation. The power component (e.g., transmission line) is assumed to be damaged if the estimated spread crosses its safety zone defined by Δ_c and the status of power grid component c is characterized by a scenario dependent parameter calculated based on D_c^i and $\omega_i^s \Delta t$.

5.4.2 Metrics for Power Grid Wildfire Risk Assessment

The following metrics are developed to aid utility decision making process and operational strategies in the wake of a wildfire threat. Note, since the metrics are used for a particular operation day j of the grid, we omit the notation j from hereon for simplifying the notation.

5.4.2.1 The Critical Response Time ($\overline{\Delta t}$)

This metric furnishes the time period within which utility operators can make operational changes to minimize economic damages before power shutoff is absolutely necessary. It is a function of the distance from the potential wildfire ignition point i to power system component c (see Fig. 5.5), and the wildfire rate of spread ω_i^s as follows:

$$\overline{\Delta t} = \min_{\forall i \in I^s, s \in \mathcal{S}} \frac{D_c^i - \Delta_c}{\omega_i^s}. \tag{5.13}$$

Note the importance of this metric since aspects of vegetation, fuel, and velocity of wildfire spread, based on the spreading model in (5.8), is incorporated into a time measure for optimizing utility actions pre-wildfire. The metric inadvertently provides a time estimate before the potential ignition will pose a risk, and serves in two ways depending on application. First, if $\overline{\Delta t}$ is $<<$ threshold (utility defined, associated with Δ_c), then ignitable location is close to the power system component, ignition is possible within Δ_c and components should be de-energized to avoid being sources of ignition for endogenous wildfires. Secondly, if $\overline{\Delta t}$ is $>>$ threshold i.e., distance of potential ignition is far enough from component, the utility can afford to wait pre-wildfire and not cut off power to customers, say H hours before actual ignition, which is mainly where revenue is lost during wildfire threats [144]. Also for the latter depending on the critical time, utilities can operate and strategize before any potential exogenous wildfire fronts induce component outages.

5.4.2.2 The Scenario based Damage Cost

The operational damage cost of a particular scenario s is the result of the optimal response of the power grid against the realized outage scenario. The operational damage cost includes losses in revenue accruing to the power utility due to lost opportunity costs arising from load curtailment, including power shutoff to customers and intended unavailability of power components, e.g., power lines, from wildfire threats. In the case of the power transmission grid, such scenario based damage cost can be defined as the optimal value of the following security constrained optimal power flow as below:

$$\text{cost}_s = \min \quad \sum_{t \in T} \sum_{b \in \mathcal{B}} \text{VOLL}_{b,t} \text{LC}^s_{b,t}. \tag{5.14}$$

$$\text{s.t.} \quad P^s_{l,t} = \frac{\left[\theta^s_{b,t} - \theta^s_{b',t}\right]}{x_l}(1 - \delta^s_{l,t}), \ \forall l = bb' \in \mathcal{L} \tag{5.15}$$

$$P^s_{g,b,t} - P_{d,b,t} + \text{LC}^s_{b,t} = \sum_{bb' \in \mathcal{L}} P^s_{bb',t}, \tag{5.16}$$

$$0 \leq \text{LC}^s_{b,t} \leq P_{d,b,t}, \ \forall b \in \mathcal{B}, \forall t \in \mathcal{T} \tag{5.17}$$

$$(1 - \delta^s_{g,b,t})\underline{P}_{g,b} \leq P^s_{g,b,t} \leq (1 - \delta^s_{g,b,t})\overline{P}_{g,b}, \quad \forall g \in \mathcal{G}, \forall b \in \mathcal{B}, \forall t \in \mathcal{T} \tag{5.18}$$

$$-(1 - \delta^s_{l,t})\overline{P}_l \leq P^s_{l,t} \leq (1 - \delta^s_{l,t})\overline{P}_l, \quad \forall l \in \mathcal{L}, \forall t \in \mathcal{T} \tag{5.19}$$

$$\underline{\theta}_b \leq \theta^s_{b,t} \leq \overline{\theta}_b \quad \forall b \in \mathcal{B}, \forall t \in \mathcal{T}, \tag{5.20}$$

$$P^s_{g,b,t} - P^s_{g,b,t-1} \leq RU_{g,b}, \ \forall g \in \mathcal{G}, \forall b \in \mathcal{B}, \forall t \in \mathcal{T}, \tag{5.21}$$

$$P^s_{g,b,t-1} - P_{g,b,t} \leq RD_{g,b}, \ \forall g \in \mathcal{G}, \forall b \in \mathcal{B}, \forall t \in \mathcal{T}. \tag{5.22}$$

where $\mathcal{B}$, $\mathcal{L}$, $\mathcal{G}$, and $\mathcal{T}$ denote the set of transmission buses b, transmission lines l, generators g, and time slots t. The objective function (5.14) is to minimize the load curtailment cost over all the sets of buses and the scheduling horizon where $\text{LC}^s_{b,t}$ denotes the load curtailment in bus b in time t in scenario s and $\text{VOLL}_{b,t}$ denotes the value of loss load. The optimization is subject to the following constraints. The DC power flow constraints of the transmission lines l connecting bus b and b' is captured in (5.15) where the scenario based outage status of the line l is represented by a binary parameter $\delta^s_{l,t}$. In particular, if the line is potentially damaged by the modeled wildfire, i.e., $\delta^s_{l,t} = 1$, there is no power flow on the line. Power balance constraint in bus b is captured in (5.16) where the power $P^s_{g,b,t}$ generated by g in b, minus the bus power demand $P_{d,b,t}$, plus load curtailment $\text{LC}^s_{b,t}$, equals the total power flowing out of b. Additionally, the load curtailment at any bus must remain within the limitations of the total demand at that bus, which is presented in (5.17). The power generated by g is constrained by its minimum and maximum capacity as in (5.18). The power flow over the line l is constrained by its thermal capacity $\overline{P}_l$ as in (5.19). On a similar note, the upper and lower limit constraints of the bus phase angle $\theta^s_{b,t}$ are described in (5.20). Furthermore, the limitations $RU_{g,b}, RD_{g,b}$ of the generators' ramping up and down rates are furnished in (5.21) and (5.22) respectively. Note that our framework can also apply to power distribution network where DC power flow constraints are replaced by the DisTFlow model considering line outage status [174].

5.4.2.3 The Expected Power System Damage Cost

The expected damage cost of power systems [175] for a given set of wildfire motivated outage scenarios S is calculated as:

$$ECOST = \sum_{s \in \mathcal{S}} \pi_s \times \text{cost}_s, \tag{5.23}$$

where cost_s is obtained by solving the optimal response of the power grid against the wildfire motivated outage scenario s, e.g. solving optimization problems (5.14)-(5.22) for the case of transmission networks. Hence, the $ECOST$ metric, in addition to estimated infrastructure damage costs, can aid utility decisions of wildfire mitigation vs. restoration, i.e., informing the important question: should the utility use the "let-burn" strategies, since oftentimes the utility is burdened with the economic decision of either fighting wildfires or employing the "let-burn strategy" where the wildfire is allowed to burn and damages are rebuilt/restored [176]. If the firefighting costs are greater than the expected damage costs (operational, infrastructural and otherwise), the utility could utilize the "let-burn" strategy.

5.5 Numerical Results

5.5.1 Simulation Setup

We consider an area covering approximately $200km^2$ in northern California and spanning latitudes $38°49'17.616''N$ to $40°46'7.14''N$, and longitudes $120°11'52.8''W$ to $122°43'55.2''W$. The chosen area reflects homogeneous climate yet spatially diverse in fuel and vegetation as illustrated in Fig. A.2 detailed in Appendix A.3. The STWIP was trained and validated using a 70% and 30% split training data of 10,900 samples, and compared to other data-based conventional baselines [177, 178] including decision tree, boosted decision tree, and linear regression. We first provide the wildfire estimation results over the studied area to illustrate the effectiveness of the first stage of the framework, i.e., the STWIP model.

5.5.2 Wildfire Estimation Analysis

The performance analysis in Fig. 5.6 shows the average accuracy for training and validation of the STWIP was (98.31% and 97.0%), while the boosted decision tree was (93.27% and 92.0%), both outperforming other baselines. Also, the proposed STWIP achieves the best performance with an Area Under the Receiver Operating Characteristic curve (AUC) of 0.995. Note that the AUC describes the model trade-off in terms of sensitivity and specificity. This performance is followed again by the boosted + tree algorithm with an AUC of 0.965 and the regression with an AUC of 0.903 respectively.

Next, we test STWIP with the 2018 year, comparing results with the actual wildfire occurrence currently available in [179]. In the test data we use the 15^{th} day of the month as it is representa-

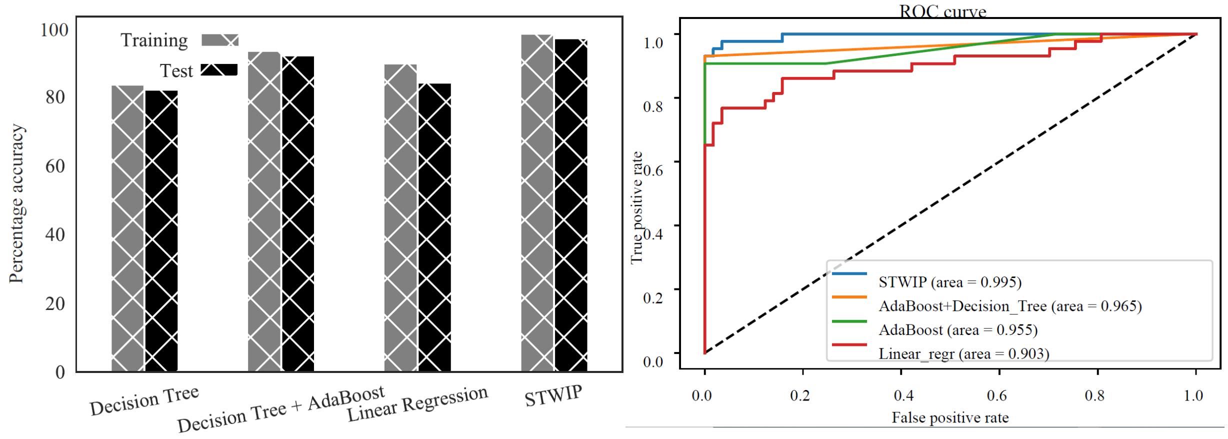


Figure 5.6: Comparison of STWIP performance to that of other machine learning baselines in terms of accuracy and Area Under the Receiver Operating Characteristic curve (AUC) scores, trained on 20 years of data till 2016 and tested on the 2018 wildfire year.

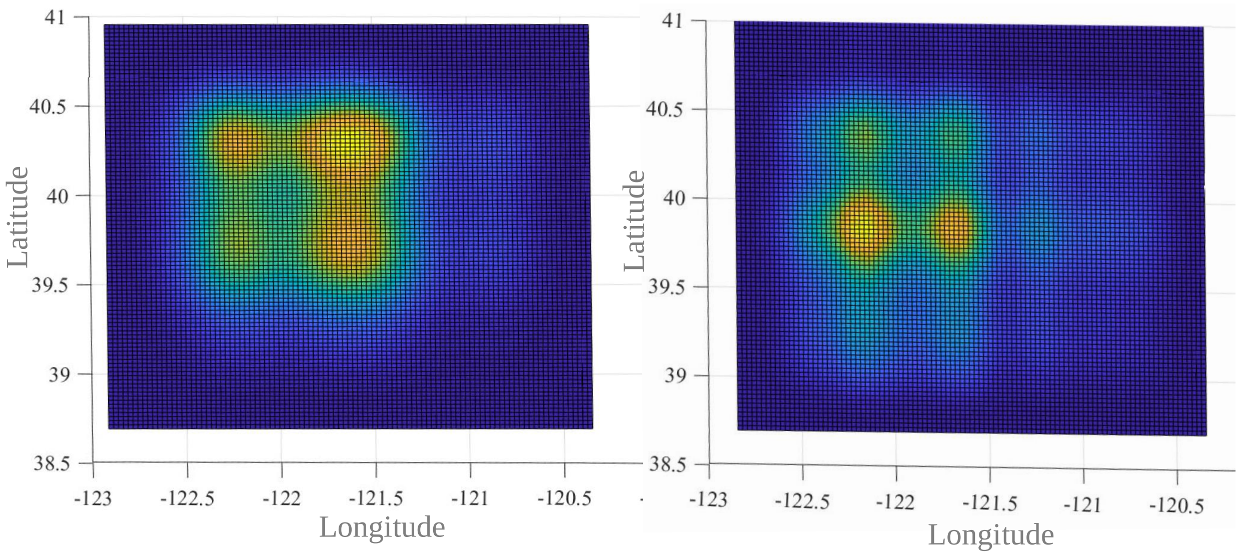


Figure 5.7: Test Year Results: Actual (left) vs. predicted spatial ignition pattern for 2018 wildfire year around Paradise California.

tive of its wildfire characteristics. Thus, we seek to obtain similar patterns of spatial density and temporal distribution. Results in Fig. 5.7 show that predicted hotspots are similar to the actual

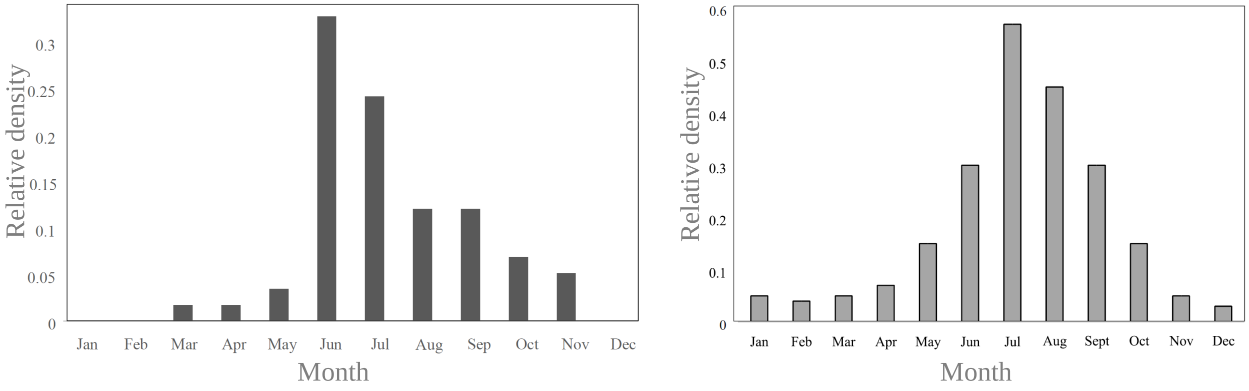


Figure 5.8: Test Year Results: Actual(left) vs. predicted temporal ignition pattern 2018 wildfire year around Paradise California.

historical test year, clustered between latitudes and longitudes (39° 30’ 00” N , 122° 30’ 00.0000”

W) and (39° 30’ 00.0000” N , 121° 30’ 00.0000” W). The central valley area of northern California has less ignition clusters, which is attributed to limited elevation and fuel. Similarly, the temporal results are analyzed monthly as furnished in Fig.5.8, showing that the estimated temporal distribution well follows the test year’s actual temporal wildfire distribution (approximately Gaussian). Hence, by employing the STWIP for analysis as opposed to the conventional utility predefined fire threat areas and fire threat levels as detailed in Appendix A.6.1, power systems can further improve wildfire forecast and analysis towards actual expectations.

The percentage weighted impact of WPVs on the wildfire ignition status is presented in Fig 5.9. In particular, the WPVs are evaluated based on their weighted influence on wildfire occurrence. Terrain and temperature, and cloud type and historical ignition, have the highest and least influence, respectively. Also, humidity seemingly influenced daily wildfire ignition maps produced by the predictor especially in the central valley of northern California. This suggests which measurement types (sensors in monitoring corridors) that the power utility should invest for enhancing situational awareness against wildfire. The performance of STWIP is further underlined as linear methods such as regression do not well capture terrain which is indeed a high impact feature [180].

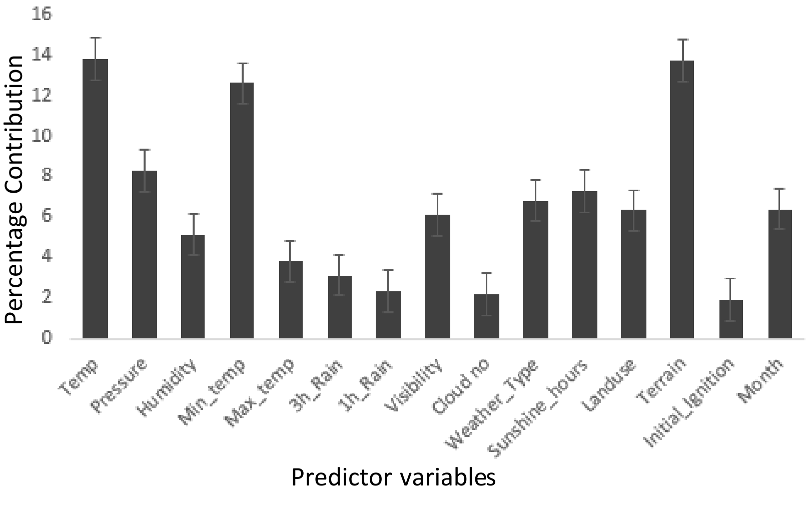


Figure 5.9: STWIP furnishes the influence of variables on wildfire occurrence enabling stakeholder decisions in power system operation and planning.

5.5.3 Illustrating Wildfire Aware Power Grid Operation Analysis

Conventionally, utility often uses region-scale and deterministic threat level analysis as previously discussed, and detailed in Appendix A.6.1. In this situation as further illustrated by Fig.

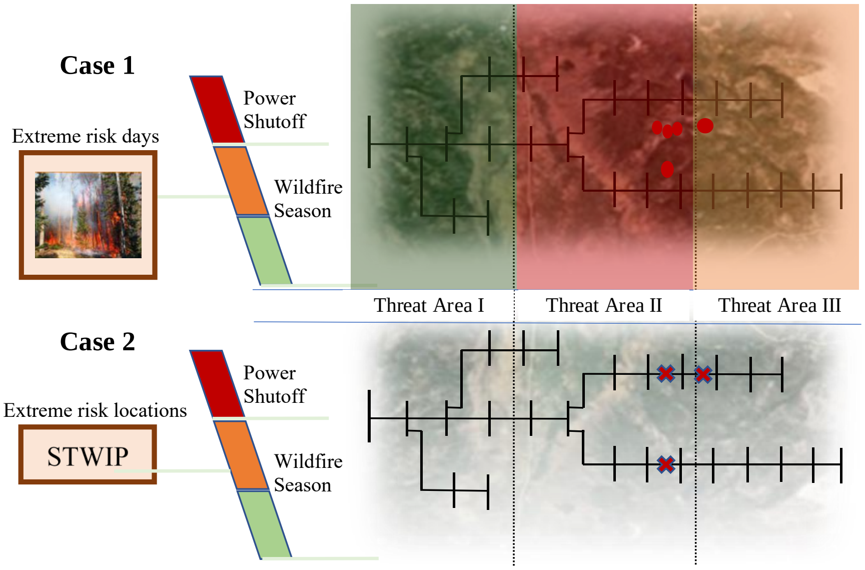


Figure 5.10: Illustration of spatial granularity risk assessment afforded by the STWIP as opposed to conventional power system use of wildfire threat areas and zones.

5.10, as seen in the "conservative" utility case, the utility will have an extreme alert in the red area since there are more wildfire threats as opposed to the elevated threat area (orange highlight). The customers in the area with extreme alert will have their power shut off for the duration of the wildfire threat, including customers up north (relatively farther) from the wildfire threat cluster. The magnitude of the shut off can be visualized given the size of the predefined threat areas in a sample utility wildfire awareness issue as shown in Fig. A.5 in Appendix A.6.1. However, the potential ignition map and spread parameters provided by the first stage estimation model can be used to analyze the risk of over de-energization motivated by power component failure-ignited wildfires and the risk of outages induced by exogenous wildfire. With the granularity in spatial detail of the wildfire potential probability maps, the spread model, and the proposed risk assessment, the utility can optimize the time before shut off is necessary in exogenous fires, and also emulate the distance between a potential ignition location (ignitable location) and the power equipment in endogenous/equipment-induced wildfires. The analysis is conducted on a 24-bus test system mapped to span the length and breath of the studied area as detailed in Appendix A.6, however, this analysis can be done on any transmission or distribution system given complete system details. We consider two case studies which deviate from the power system normal operation when there are no wildfire threats. In case 1, the test system is simulated with the current conventional "conservative" utility approach of threat area and levels detailed in Appendix A.6.1. In this case, all the power components located in the pre-defined elevated threat area as illustrated in Appendix A.6.1 are intentionally outaged whether or not they are in the direct vicinity of high wildfire potential. This simulates current utility procedure to prevent endogenous wildfires [144]. In case 2, the wildfire analysis and test system de-energization is based on the wildfire potential ignition map produced by STWIP as described in Section 5.4 aiming to improve spatial granularity and optimize (shorten) the time span of utility de-energization. Simulation data is based on Nov. 10, 2018. The VOLL is set to 1000 $/MWh. Details of the components that are out of service in the three case studies are shown in Table 5.2.

5.5.3.1 *Assessing risk of outages induced by exogenous wildfire*

For exogenous wildfire induced outage risk analysis, the probabilistic ignition map is used to generate wildfire ignition scenarios and simulated spreading pattern, thus modeling exogenous wildfire-induced damages on power grid components. The expected damage cost, ECOST, as illustrated in Fig. 5.11, represents the aggregate analysis for one operational year of the test system in the studied area. It shows that the power system is highly vulnerable during summer time from

Table 5.2: Wildfire-motivated De-energization: Scenario of public safety power shutoff aided by STWIP (case 2) vs. conventional utility methods (case 1).

Case Study	Transmission Line Outages	Generator Outages
Case 1	L1-4, L6-8, L14, L19, L24-33	G1-4, G15-29
Case 2	L4, L8, L19, L23-24, L28, L31-33	None

June to September, and quite low during winter time from December to March. However, the risk of wildfire induced outage still exists during non-summer times, which can be explained by the impacts of the time independent WPVs such as landuse and terrain. Hence, an efficient allocation of utility wildfire monitoring resources should be based on spatio-temporal analysis of wildfire occurrence, e.g., monitoring grid and vegetation should be done more frequently during high risk period.

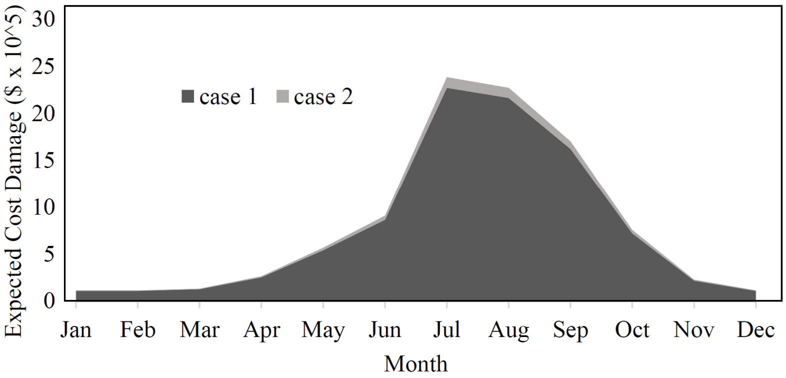


Figure 5.11: Enabling power system infrastructure planning using the expected damage cost from exogenous fires over the period of one year. There is wildfire risk during non-summer months as well.

5.5.3.2 Enhancing de-energization decision for power component failure-ignited wildfires

Wildfires can be ignited by electric power line faults that cause arcing in a high-heat release of energy. Such incidents are majorly caused by ignitable vegetation contacting power lines. Indeed, the correlation between the wildfire ignition probability map and electric power failures motivates the use of proactive de-energization of equipment as a preventive measure [33]. We aim to illustrate the improvements in de-energization using the proposed STWIP, which is more granular and stochastic, over conventional utility approach. The proposed framework aids in enhancing de-energization and estimating the potential cost of wildfire occurrence as detailed further.

The total system energy consumption, total loadshed, and loadshed-bus localization of the three

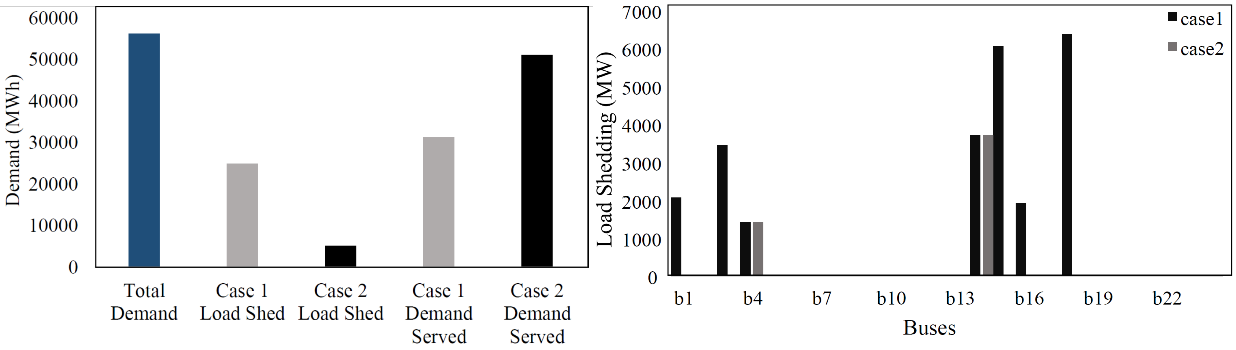


Figure 5.12: Demand served and load shedding results for cases 1 and 2. The spatially detailed STWIP enables more load buses to be served and generally meets more customer demand, as opposed to conventional utility methods, during wildfire threats.

cases are shown in Fig. 5.12. The total energy demand of the system is 54358.679 MWh, with case 1 supplying 29449.051 MWh due to large amounts of load shedding, 45.8%, resulting from the conventional threat area and threat level methods. Relative to case 2, the power grid response avoids a large amount, 19798 MWh, of unnecessary load shedding. Hence, a more detailed wildfire potential ignition map provided by the proposed granular analysis results in less conservative shutoff, i.e., only components in the high wildfire vicinity are proactively de-energized to prevent component failure-caused wildfire [33]. Table 5.3 presents load shedding cost, and generation cost

Table 5.3: Costs for cases 1 and 2 ($)

	Load Shedding Cost ($)	Generation Cost ($)
Case 1	181,591.25	537,969.01
Case 2	37,263.75	537,991.32

for all cases. For the normal system operation, there are no load shed costs and generation costs are $568,084.40 The total costs for case 1 is high due to the amount of load shed and the increase in production of expensive online generators.

In addition, the framework aids improve the resilience of the system by spatio-temporally informing the disaster progression phase of the resilience trapezoid as illustrated in Fig 5.13, hence reducing the “dip” in the resilience curve [7]. Specifically, in case 1, a large and sudden drop of

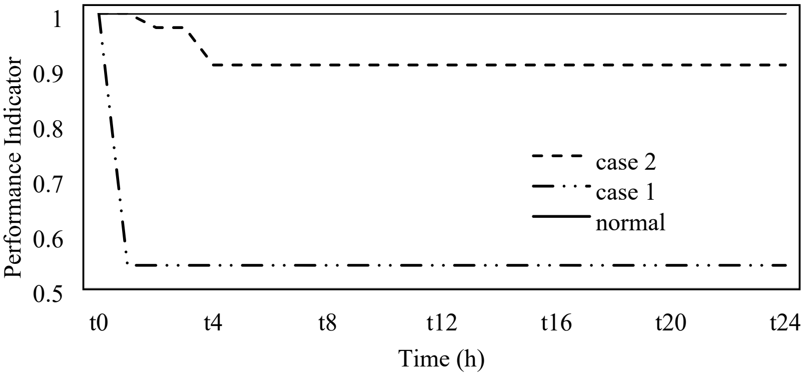


Figure 5.13: Profile of load served during wildfire threats as a resilience performance indicator. STWIP enhances resilience as de-energization is enabled by a granular spatio-temporal map, as opposed to conventional utility methods which shut-off power to entire predefined wildfire threat zones given the threat of a wildfire.

the percentage load served (performance indicator) is observed. This is because without spatio-temporal analysis, the utility performs conservative forced outages as soon as a wildfire threat is observed in their pre-defined regional threat areas, which in this simulation is set to the beginning of the scheduling horizon at $t^* = 0$. The percentage load served in case 2 is observed to reduce over time. This is possible due to the improved granularity provided by spatio-temporal analysis where expectations of wildfire parameters such as distance, spread rate, and the critical response time have been pre-estimated as discussed in Section 5.4.2.1. Hence, with a grasp of the expected critical response times, the utility operations have increased and informed time flexibility in forcing component outages.

5.6 Conclusion

This chapter proposed a comprehensive spatio-temporal framework for power system wildfire risk analysis including two sequential models. The first model estimates the granular and spatio-temporal potential wildfire probability and spread based on influential parameters such as vegetation and fuel, wind speed, geographical and meteorological variables, while the second model leverages the estimated probabilistic ignition maps in order to analyze system risk from exogenous wildfire and to enhance power system de-energization in mitigating endogenous fires induced by power equipment failures. Numerical results show that lower forced electricity outages to customers can be achieved by increased granularity in spatial locations in utility service areas. Hence, the framework significantly improves utility de-energization decision compared to the current "conservative" threat area approach In addition, the framework aids to improve system resilience and utility revenue and prioritize resource allocation given increased localization of high wildfire potential.

6. A SELF-SUFFICIENT LOW-COST AND AUTOMATED MITIGATION MODEL TO IMPROVE RESILIENCE IN POWER UTILITY WILDFIRE RESPONSE

6.1 Introduction

In the previous chapter, the spatio-temporal wildfire ignition predictor (STWIP) is proposed to study and produce the wildfire potential map of the study area with the probability for wildfire threat. The STWIP model is also integrated with the SL-PWR (pronounced *ES-EL-POWER*) model proposed in this chapter as illustrated in Fig. 6.1, whereby the output of the STWIP is used by the SL-PWR to optimize the UAV operation.

This chapter further develops an intelligent and novel self-sufficient and low-cost model (SL-PWR) to guide and improve resilience in the wildfire response of power utilities. Specifically, the SL-PWR model consists of 4 major modules including 1.) the vegetation module, 2.) the power equipment module, 3.) the wildfire module, 4.) the burnt equipment module, which are active in all the resilience phases of the system including pre-wildfire (wildfire analysis), wildfire progression, and restoration phases. The modules are also made up of sub-modules which consist of CNNs that extract spatial details for detection, classification, estimation, and localization. As shown in Fig. 6.1, the SL-PWR model receives granular mapped spatio-temporal information of wildfire potential in a given service area which has been divided into grid cells with grid centers located at $g_c.loc$ with a latitude and longitude (Lat, Lon) at which UAVs can be situated to monitor that particular grid. SL-PWR uses the $g_c.loc$'s with extreme/elevated wildfire ignition probabilities to optimize the trips of the UAV to these grids to monitor and capture input images for important analyses in the comprehensive resilience enhancement provided by the proposed mitigation model.

The SL-PWR model performs analysis in real time with computation time that can be easily integrated into power system operations in order to prevent wildfire occurrence and mitigate impact. This is achieved via automated vegetation management and equipment monitoring or in the case where wildfires occur, hasten the resilient response of the power utilities' mitigation resources by providing information on the fire type (e.g., fire accompanied by thick smoke will induce additional precaution in the area during evacuation or firefighting), fire area, fire location and spread. The proposed model also aids in transparent inventorying during post-wildfire restoration e.g., instead of contracting manual road crews to take inventory of damaged equipment which the system operator will be blind to, the SL-PWR can aid transparency, in that the system operator will be able to visualize and estimate damage cost through the images captured and analyzed by the "Burnt Equipment Detection and Estimation Module" and can hasten and automate the process.

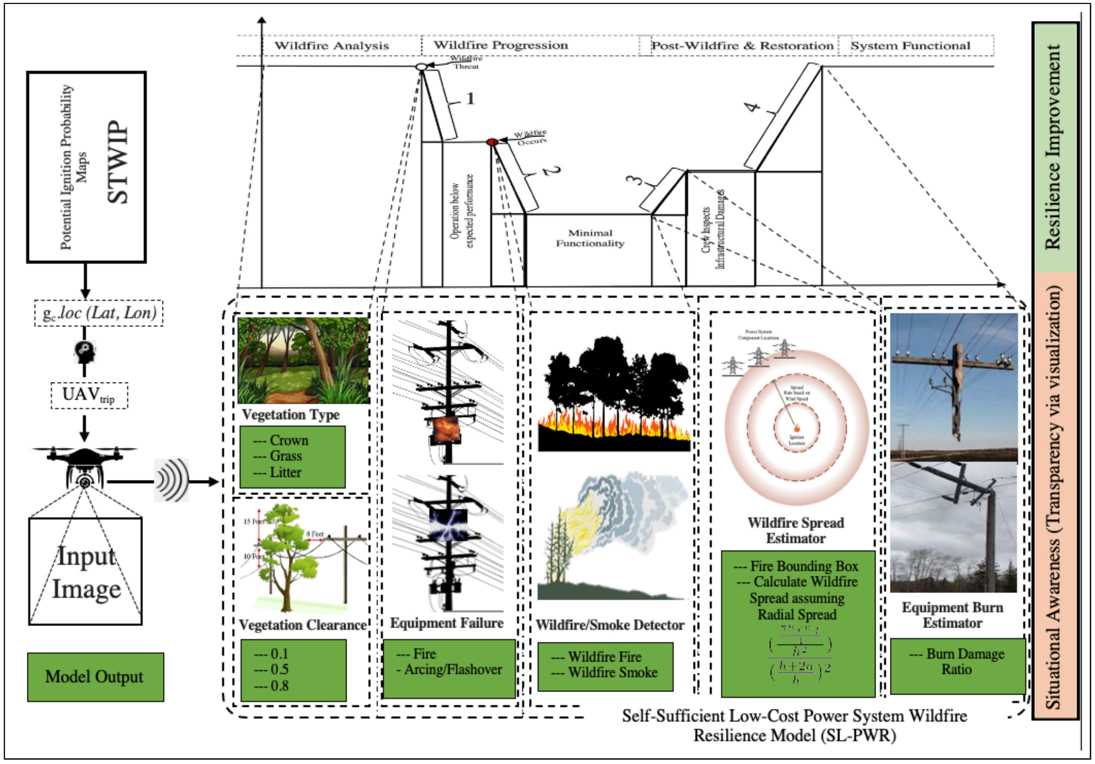


Figure 6.1: The Self-Sufficient Low-Cost Power System Wildfire Resilience (SL-PWR) Model.

6.2 Methodology of the SL-PWR Model

6.2.1 The Structure of the CNN

The CNN is the fundamental network used in obtaining spatial attributes used to train the SL-PWR model. It is a deep learning algorithm that takes in an input image and assigns learnable parameters (weights and biases) to various aspects/elements of the image so as to differentiate one image from another. It is a multi-layer neural network that consists of convolution layers, pooling layers and fully connected layer. The convolution layer(s) are made up of N @ $F \times F$ filters which basically translates to a matrix of weights called feature maps. In order to generate these feature maps, the filters (a pre-defined matrix initialized with height and width parameters) travel left to right on the input image/map, stepping in strides of predefined width and taking the dot product of the applied filter/kernel and the image/feature map area overlapped by the filter, after which it moves downward with step size of a predefined stride height and repeats the step across the image (i.e., from left to right). The CNN operator at each layer is completes the following function.

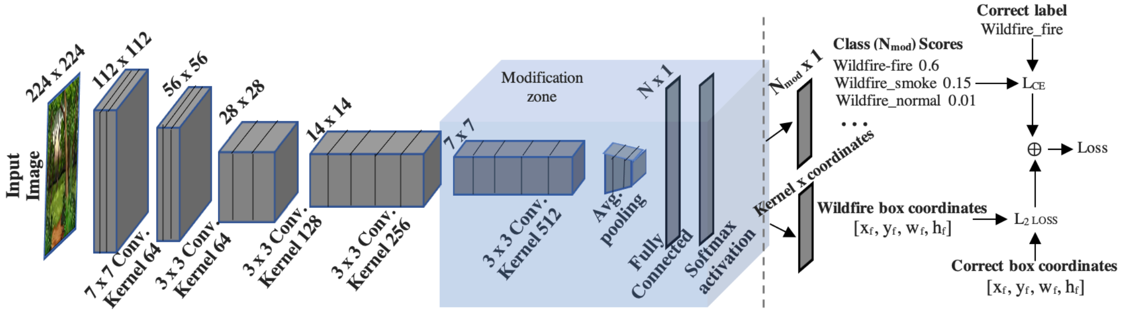


Figure 6.2: ResNet-18 architecture: Illustrating the modification zone for the classification and wildfire localization problems

$$Y_{ij}^{\widehat{x}\widehat{y}} = A\left(b_{ij} + \sum_{\widehat{p=0}}^{F-1}\sum_{\widehat{q}=0}^{F-1}\omega_{ij}^{\widehat{p}\widehat{q}}X_{i-1}^{(\widehat{x}+\widehat{p})(\widehat{y}+\widehat{q})}\right) \tag{6.1}$$

where the layer under consideration is i, j is the feature map under consideration in layer i, $Y_{ij}^{\widehat{x},\widehat{y}}$ is the output located at position $(\widehat{x},\widehat{y})$ in feature map j and layer i, $A(\cdot)$ represents the layer's activation function, b_{ij} is the bias term, ω_{ij}^{pq} denotes the weights/value of the convolution filter ($F \times F$), at position (p,q), associated with layer i and feature map j. In the event where the filter size and stride would leave certain parts of the input unattended, padding can be applied. This creates the output volume from each convolution layer given the filter size, padding, and stride, according to (6.2),

$$Out\_Vol = \frac{(I - F + P)}{S} + 1 \tag{6.2}$$

where I is the input volume of the $I \times I$ image, F is the kernel size (volume of the filter, $[F < I]$), P is the padding and S is the stride. Hence, by convolving the filters with the input image and carrying out non-linear transformations using activation functions, N feature maps are created. The activation function adopted in the proposed model is the ReLU (Rectified Linear Unit) function as in 6.3.

$$A(x) = max(0, x) \tag{6.3}$$

The pooling layer(s) performs it pooling operation by obtaining the average or maximum value of the elements of the feature map where its window slides, given the kernel size (height and width) of the filter and the strides. Hence, this layer extracts the dominant features, a dimensionality reduction of sorts which also helps to improve computational efficiency. Together, the convolutional layer and the pooling layer form the i^{th} layer of the CNN. The fully connected layer is one that learns the non-linear combinations of these high-level features as transformed by the convolutional layer, hence, learning a non-linear function. It takes in the elements of the feature maps feeding directly into it and then flattens these elements towards the output which could be classification or regression type. The flattened elements are then fed into a feed-forward neural network, learning the parameters (ω, b) by minimizing the negative log-likelihood given the training input as in (6.4).

$$L(\omega, b) = -\sum_{I_k} \ln p(I_k | I_k; (\boldsymbol{\omega}, \mathbf{b})) \tag{6.4}$$

where I_k is the correct (target) class label for the input image under consideration. This objective is optimized by applying applying stochastic gradient descent with back propagation using the chain rule as in (6.5), to training iterations over several epochs.

$$\omega_i^{n+1} = \omega_i^n - \mu \frac{\partial L}{\partial Y_{N_i}^n} \cdot \frac{\partial Y_{N_i}^n}{\partial Y_{(N_i-1)}^n} \cdots \frac{\partial Y_i^n}{\partial \omega_i^n} \tag{6.5}$$

where μ is the learning rate, N_i is the total number of layers in the network, Y_i^n is the output of layer i during iteration n. With this process, the model is then capable of distinguishing dominant and less-superior features in the input images, further classifying them using the Softmax function, an adaptation of the Sigmoid function used for multi-class classification, which takes in the vector of R real numbers and normalizes them into a probability distribution of N probabilities which are proportional to the input exponentials as in (6.6),

$$p(c|I_k;(\boldsymbol{\omega},\mathbf{b})) = \frac{e^{f_c(I_k;(\boldsymbol{\omega},\mathbf{b}))}}{\sum\limits_{d=1}^{N} e^{f_d(I_k;(\boldsymbol{\omega},\mathbf{b}))}} \tag{6.6}$$

where $f_c(I_k;(\boldsymbol{\omega},\mathbf{b}))$ is the scores from each of the multiple classes of interest c $\in \{1,\cdot\cdot\cdot,N\}$ transformed into conditional probabilities using the Softmax function which applies the exponential function to the elements of its input vector and divides the obtained value by the sum of the exponentials of all elements (normalization) which ensures the output components sum up to 1. In order to test the CNN model after the training process described above, the output layer then predicts the label $\widehat{I}$ of the image input I using the argmax of the Softmax-transformed probabilities as in (6.7).

$$\widehat{I} =_{c\in\{1,\cdots,N\}} p(c|I;(\boldsymbol{\omega},\mathbf{b})) \tag{6.7}$$

The proposed SL-PWR consists of sub-modules which are built fundamentally based on the Residual Neural Network (ResNet18).

6.2.1.1 The ResNet18 CNN Model

ResNet18 has been widely applied to different image vision and classification problems as it provides a solution to the issue of vanishing gradients, which occurs as continuous multiplication during back-propagation makes the gradients infinitesimal as neural networks get deeper [181]. As illustrated in Fig.6.3, the block tries to learn an output, say G_x. The residual block allows the network to directly learn $F(x) = G(x) - x$, such that the target output is $F(x) + x$ hence avoiding depreciating performance that having too many convolutional layers would have introduced. For instance, in the block in Fig.6.3, the residual mapping function is as in (6.8), while the output of the block after the second ReLU activation is as furnished in (6.9).

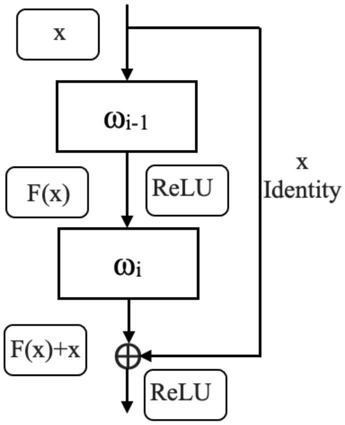


Figure 6.3: Implementation of the identity shortcut connection via the residual block to avoid the depreciating performance of having many convolutional layers.

$$F = \omega_i \sigma \left(\omega_{i-1} x \right) \tag{6.8}$$

$$Y = F(x,_i) + x \tag{6.9}$$

where σ is the ReLU activation function. Given the "identity shortcut connection", the network can skip one or more layers in order to avoid performance degradation birthing different variants including the ResNet18 and ResNet34 proposed in [181]. In this work, we employ the ResNet18 model as its performance is comparable with other networks [182] such as the ResNet34 but with relatively faster convergence. The architecture of the ResNet18 model employed in this paper is as shown in Fig.6.2. This architecture is then adapted as required for the different sub-models of the proposed model.

6.2.1.2 Loss Functions

Since stochastic gradient descent (6.5) is used in training neural networks, a loss function has to be selected during model design and configuration. In this work, the loss functions are chosen according to the classification type/output requirements of the specific model.

6.2.1.2.1 L1 Loss: This represents the average of all absolute differences between the true value $y^{(i)}$ and the predicted value $\widehat{y}^{(i)}$. Also called Mean Absolute Error (MAE), it measures the average of residuals in the dataset. We use the L1 loss for illustrations because it is not affected by the outliers as the L2 Loss Function is.

$$Acc_1 = \frac{1}{N}\sum_{i=1}^{N} |y^{(i)} - \widehat{y}^{(i)}| \tag{6.10}$$

6.2.1.2.2 Mean Square Error: The mean square error (MSE) is the L2 loss used to minimize error as the average sum of the all the squared differences between the actual/ground truth value and the predicted value as in (6.11). In this work, the root mean square is used to evaluate how far away (deviation) the target image's pixels are from the predicted image's pixels.

$$Acc_2 = \frac{1}{N}\sum_{i=1}^{N}(y^{(i)} - \widehat{y}^{(i)})^2 \tag{6.11}$$

6.2.1.2.3 Root Mean Square Error: The root mean square error (RMSE)is the square root of the MSE and measures the standard deviation of residuals in the dataset.

$$Acc_2 = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y^{(i)} - \widehat{y}^{(i)})^2} \tag{6.12}$$

6.2.1.2.4 The Cross-Entropy Loss: The cross-entropy loss as formulated in (6.13) is also known as the logarithmic/log/logistic loss and is one popularly used for classification. This loss is used in this work for different reasons including: 1.) classifications that use sigmoid or softmax activation functions, which are more robust with improved performance using the cross-entropy loss [183], 2.) the problems are multi-class classification. The function outputs 1 when the network predicts the correct image and is 0 otherwise, in a one-hot encoded format.

$$L_{CE} = -\sum_{i=1}^{N}\sum_{j=1}^{K} y_j^{(i)} \cdot \log \widehat{y}_j^{(i)} \tag{6.13}$$

where $y_j^{(i)}$ and $\widehat{y}_j^{(i)}$ are the one-hot encoded actual classification and predicted outputs, j is the number of classes (for multi-class), and i represents the data points. Hence, the cross-entropy measures the error between two probability distributions under the maximum likelihood framework is derived for multi-class classification as:

$$P_{model}(Y|X,\theta) = \prod_{i=1}^{N}\prod_{j=1}^{K}\left(\widehat{y}_j^{(i)}\right)^{y_j^{(i)}} \tag{6.14}$$

$$\log P_{model} = \sum_{i=1}^{N}\sum_{j=1}^{K} y_j^{(i)} \cdot \log \widehat{y}_j^{(i)} \tag{6.15}$$

Let $i^{(l)}$ be the correct class for the l^{th} example e.g., $y^{(l)}$ = $\left(\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right)$ and the first class $i^{(l)}$ is the correct class,

$$\log P_{model} = \sum_{l=1}^{N} \log \widehat{y}_{i^{(l)}}^{(l)} \tag{6.16}$$

Using the softmax model:

$$\log P_{model} = \sum_{l=1}^{N} \log softmax(z)_{i^{(l)}} \tag{6.17}$$

$$\log P_{model} = \sum_{l=1}^{N} \frac{e^{z^l_{i^{(l)}}}}{\sum\limits_{j} e^{z^l_j}} \tag{6.18}$$

$$\log P_{model} = \sum_{l=1}^{N} \left[e^{z^l_{i^{(l)}}} - \log \sum_{j} e^{z^l_j} \right] \tag{6.19}$$

$$\log P_{model} = \sum_{l=1}^{N} \left[z^l_{i^{(l)}} - \max_{j} z^l_j \right] \tag{6.20}$$

which is basically the error distance.

6.2.1.3 Metrics

6.2.1.3.1 Accuracy: The accuracy of the multi-class classification is evaluated as in (6.21) by using the score function defined as the mean of the sum of correct predictions over the sample size N. Similarly, the accuracy of the regression problems is evaluated by using the average L1 distance as in (6.22).

$$Acc_1 = \frac{1}{N} \sum_{i=1}^{N} \sum_{j=1}^{K} y_j^{(i)} \cdot \widehat{y}_j^{(i)} \tag{6.21}$$

$$Acc_2 = \frac{1}{N} \sum_{i=1}^{N} |y^{(i)} - \widehat{y}^{(i)}| \tag{6.22}$$

6.2.2 UAV Resource Integration to SL-PWR

6.2.2.1 Quantitative Input Data from STWIP

In this section, we discuss the spatial definitions of quantitative input data. The STWIP produces wildfire threat maps which provides potential ignition locations ($i.loc$) with their probabilities ([0,1]) of ignition readiness [184]. Hence, a spatial location is a point i with geospatial coordinate $i.loc$ defined by a latitude and longitude *(lat,lon)* at any location in a grid cell. Grid cells here are g×g km polygons which have uniform past spatio-temporal wildfire characteristics and a centroid. Each grid centroid also has geospatial coordinates $g_c.loc$ [*]. The STWIP provides the grid centroids $g_c.loc$ with different levels of wildfire threat according to the potential ignition probabilities (wildfire threat/wildfire risk) of all $i.loc$ located within the grid. For instance, in Fig.6.11, on the potential ignition map, the grid G1 contains high risk locations while G5 contains moderate risk locations, hence G1 is an extreme risk grid, G5 is an elevated risk grid and all other grids are normal with little to no threat. The STWIP then sends this information ($g_c.loc$, risk level) as input to the UAV navigation for visual inspection. The information can further be used in optimizing the UAV monitoring routes as proposed in Section 6.4.3. When the trip information gets to the UAVs, they begin their monitoring travel along the specified paths taking images from $g_c.loc$. We assume that at the UAVs' capture location, $g_c.loc$, the entire grid can be monitored.

6.2.2.2 UAV Image Capture

Conventionally, utilities occasionally perform visual inspection using manual field surveys like foot patrol crew and manned helicopters, for vegetation management and monitoring power equipment [185]. More advanced techniques have also been employed in literature including aerial images from manned helicopters and fixed-wing platforms, land-based platforms, airborne laser scanner, synthetic aperture radars, optical satellite, and UAVs [186]. Land-based platforms include techniques that utilize mobile platforms such as cars, integrating different navigation, locational and imaging data sensors [186]. Additionally, helicopters and fixed-wing aircraft have been typi-

[*] The grid centroids are standard spatial grid points obtained from the National Oceanic and Atmospheric Administration's High Resolution Rapid Refresh model

cally used for power line inspection and vegetation monitoring respectively. Airborne laser scanning technique is also basically active remote sensing from an aircraft using Light Detection and Ranging (LiDAR) [187]. Satellite image data can also be employed e.g., satellites orbiting at lower (500–2000 km) altitudes can detect wildfires in the early phases due to their finer resolution but these satellites can take several hours to days to return to the same view. For example, VIIRS has a 12-hour revisit time while the Landsat-8 has a 16 day revisit time hence it is rare that one of these satellites provides the first wildfire alerts [188, 189]. Using satellites have additional limitations including:

1. The detected heat signatures are averaged over pixels, making it difficult to pinpoint fire location and size.

2. Wildfire intensity is indicated by thermal signals which can be smoldered by smoke and hence radiate relatively less energy, causing data misinterpretation.

3. At lower altitudes (up to 215m) UAVs can capture 5cm resolution imagery, which is much higher than imagery captured from satellites, 25cm resolution [190].

Also, helicopters and airplanes can also be used as conventionally done by power utilities, however, [190], discovers that Low-flying airplanes can capture comparable imagery to UAVs, but are expensive to hire and flying at low altitudes increases the possibility of a crash, thus employing the UAV technology lowers costs and improves operator safety for such missions.

Hence in this work, we choose to use the UAVs since:

1. UAVs provide more continuous monitoring than satellites, which periodically visit specific parts of earth.

2. Unlike satellites, the system would rarely be blinded by local weather conditions or smoke/dust of wildfires.

3. Satellite imagery e.g., from Google Earth can only support so much detail in the image resolution before images begin to appear blurred or pixelated.

4. Most UAVs do not need runways, takeoff can be from car-top launcher and recovery with parachute, if needed.

Additionally, although microwaves from synthetic aperture radars, also obtained from earth observation satellites, are capable of penetrating clouds, the UAVs are cost efficient for visual inspection and have widely been employed by power utilities, hence, will be an economic resource choice for SL-PWR since fewer investments will have to be made in terms of purchase and training the operating crew.

With the UAV-enabled SL-PWR model, the vehicles fly over the service area using the optimization model proposed in Section 6.4. The geographical layout of the service area is as defined in Section 6.2.2.1. The image attributes (image, $g_c.loc\ (lat, lon)$) are then sent as output from the UAVs and input to the SL-PWR via a communication link e.g., cellular communication or leased lines from internet service providers (ISPs) since they provide more redundancy (availability of various ISPs) in a wildfire scenario. As the UAVs fly over, the images (vegetation, endogenous ignition source, fire spread/smoke, burn-damaged equipment) are captured from different scales/angles and taken at different times of day and weather conditions. To capture these conditions, diverse images are collected and augmentations/transformations are applied, which also serves to increase the training data.

6.2.2.3 UAV Control and Routing

UAV control is performed in the mission planning "ground station" software which can easily run on Windows PCs. The software enables the operator plan and upload missions to UAVs wirelessly, launch the UAVs, monitor trip progress and issue landing commands. Specifically, photogrammetry tools in the software can be used for the mission planning and route specification after route optimization. In this tool, the aerial image of the service area to be monitored is highlighted within a rectangle, producing a preview of the proposed flight paths using waypoints which signify the UAV turning points in the trip. Typically, "no waypoints zones" (e.g., close to major airports) are also indicated by the software so as to mitigate the UAV flying into restricted airspace. After confirmation, the trip is uploaded wirelessly to the UAV via it's datalink which creates a communication bridge between the control software PC and UAV. The UAV can then be launched, its trip monitored through each waypoint, and automatically landed upon trip completion via the software. Furthermore, the captured image's geographical coordinates is also recorded since the GPS receiver avails the UAV positional data along with the images which are sent to SL-PWR for analysis, detection and estimation.

6.2.3 Image Acquisition and Processing

A few databases [184, 191–193] exist for wildfire detection but these are limited to smoke dataset [192], NASA's quantitative forecast data [193], image data of wildfire hotspots detected by NASA satellites and the Fire Information for Resource Management System [191]. However, no known database captures SL-PWR input requirements including utility equipment, wildfire fire-smoke, vegetation type and clearance data. Therefore, image acquisition and processing is a significant effort in the training of the SL-PWR and thus one of the envisioned contributions of this work is dataset provision. Search engines were scraped for RGB image data of different pixels using the SL-PWR python scrapper code for image collection while relevant images were retained. The input data consists of over 1800 original images including 863 images, 307 vegetation type images, and 286 images for the burnt equipment detection and estimation module, distributed as illustrated in Fig. 6.4. Additionally, there are 283 vegetation distance dataset images, 125 images for fire spread prediction, and 286 images for the burnt equipment detection and estimation module.

6.2.3.1 Resize Images

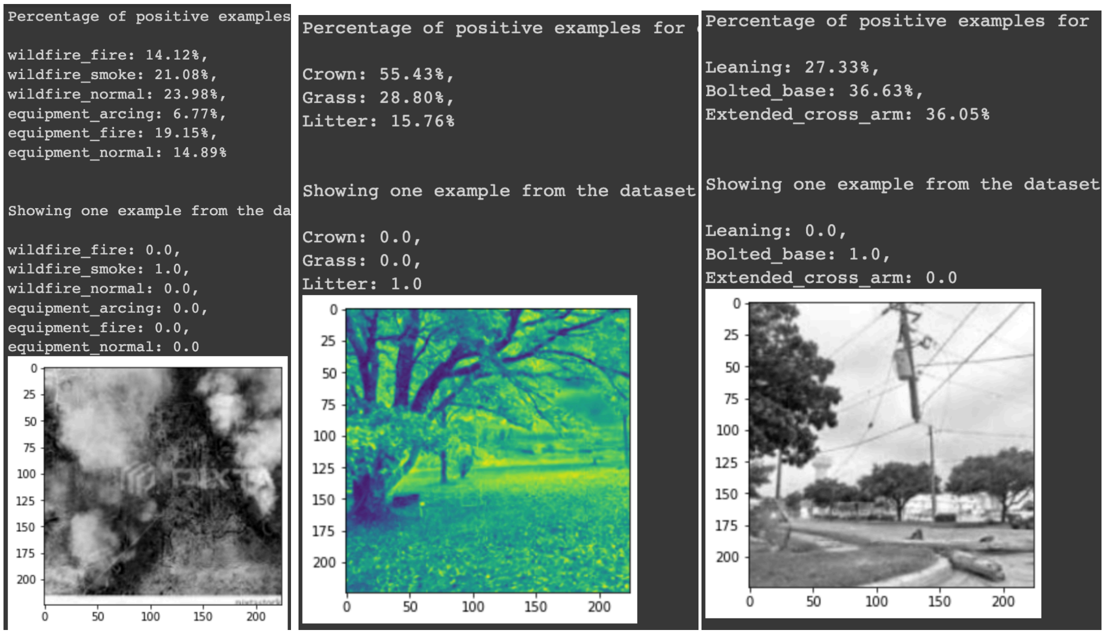
The images are then resized to the input size requirement of the ResNet-18 network at 224 x 224 pixels which have 3 (RGB) color channels. The resizing unifies the images also. A python function is developed in this work in order to convert all images to size 224 x 224 x 3 with a .jpg image extension. Here, other functions are also developed to perform center crop, resize and normalize with ImageNet dataset statistics with average and standard deviation of $mean = [0.485, 0.456, 0.406]$ and $std = [0.229, 0.224, 0.225]$ per channel, respectively.

6.2.3.2 *Encode Data labels*

The data is labeled to the ground truths as the training is supervised. Qualitative/categorical labels are transformed to quantitative data points e.g., crown=1, grass=2, litter=3.

6.2.3.3 *Import Data*

The data is then uploaded to google drive from where it is imported into the google Colaboratory platform which affords the GPU computation required for the model analysis. The data is then sliced into the different categories of the multiple classes. After importing the data, each data class/category is shuffled in order to randomly rearrange the data and avoid bias towards particular classes by utilizing an unbiased data distribution.



```
Percentage of positive examples

wildfire_fire: 14.12%,
wildfire_smoke: 21.08%,
wildfire_normal: 23.98%,
equipment_arcing: 6.77%,
equipment_fire: 19.15%,
equipment_normal: 14.89%


Showing one example from the da

wildfire_fire: 0.0,
wildfire_smoke: 1.0,
wildfire_normal: 0.0,
equipment_arcing: 0.0,
equipment_fire: 0.0,
equipment_normal: 0.0
```

```
Percentage of positive examples for

Crown: 55.43%,
Grass: 28.80%,
Litter: 15.76%


Showing one example from the dataset

Crown: 0.0,
Grass: 0.0,
Litter: 1.0
```

```
Percentage of positive examples for

Leaning: 27.33%,
Bolted_base: 36.63%,
Extended_cross_arm: 36.05%


Showing one example from the dataset

Leaning: 0.0,
Bolted_base: 1.0,
Extended_cross_arm: 0.0
```

(a) Wildfire and endogenous threat detection

(b) Vegetation type detection

(c) Burnt equipment detection

Figure 6.4: Visualizing input data distributions for the wildfire ignition detection, vegetation (fuel) type detection, and equipment damage detection modules.

6.2.3.4 Data Augmentation

In data augmentation, the input data amount for each of the SL-PWR modules are increased by slightly modifying copies of already existing input images using different techniques such as horizontal flipping, random cropping, color normalization and jittering. Random cropping can be applied by first inputting (224+x) x (224+x) pixel images and then cropping at fixed (cropping by moving towards the four edges and then a center crop) or random locations, to get 224 x 224 images. Also, this can be done by inputting 224 x 224 images and then adding horizontal and vertical padding to the images and then applying the crop to fixed or random locations on the image. Specifically, color normalization sets the lowest-highest intensity pixels from values of 0-255 while pixels in all 3 channels are then scaled accordingly. The color jittering changes the image parameters following a normal distribution with zero mean and different standard deviations which change the image brightness, contrast, saturation, and hue, respectively. This gives the image different contrasts which represent images captured by the UAV at different times of the day, and different diurnal weather conditions respectively. Gaussian blur augmentation was added to make the model sturdy against weather conditions such as fog, mist, etc. These techniques also perform as regularizing parameters to reduce model overfitting.

6.2.3.5 Data Split

This function is developed for every module according to the input data in the different categories in order to randomly split the dataset to avoid predictability in the dataset and hence overfitting and ensure that bias is mitigated in cross-validation as well as evaluate the model accuracy with different random dataset distributions. In this operation, 100% of the data is added to a split termed “all”, 60% of the data is added to a split termed “$train$” for the training dataset, 20% of the data is added to a split termed “val” for the validation dataset, and 20% of the data is added to a split termed “$test$” for the testing dataset.

6.3 The Proposed Model

The proposed SL-PWR include four main modules, 1.) the vegetation module, 2.) the wildfire module, 3.) the power equipment module, and 4.) burnt equipment detection and estimation module. These modules also include sub-modules which are used to improve the system resilience at different phases of the resilience trapezoid as illustrated in Fig. 6.1. These models and their sub-models are further described as follows.

6.3.1 The Vegetation Module

This module is active in the wildfire analysis stage of the resilience trapezoid. Vegetation is one of the most abundant biotic elements and refers to the plant life of a region. It is the ground cover provided by plants and is necessary for shaping the ecosystem. However, given the above and even enhancing environmental beauty, different types of vegetation (e.g., needleleaf forests, shrublands, savannas) can also cause issues for the electric power utilities when they grow close to overhead power lines which are not protected by insulation. When these trees and it's limbs (branches, etc) fall, they could also bring down power lines and other electrical equipment leading to power outages or in a worse case cause arcing and fires on the lines, or become a direct pathway for electricity, which can in turn engender wildfires. Electric power utilities hence perform vegetation management on thousands of miles of overhead power lines through careful pruning of trees, or removal of vegetation that could interfere with power lines. Moreover, the Federal Energy Regulatory Commission (FERC) has granted the North American Electric Reliability Corporation (NERC) the authority to audit annual vegetation management plans for lines carrying $\geq$ 200kV and levy fines to ensure the plans meet standards [194]. Additionally, there are professional standards, established by the American National Standards Institute and the International Society of Arboriculture, to vegetation management which the utilities follow. Hence, typically, utilities employ the services of certified arborists to provide some level of supervision to the professional tree-trimming crew who are contracted for vegetation management projects which could be within intervals of 4-5 years, or less for vegetation that is fast growing [195].

6.3.1.1 Vegetation Type Detection Sub-Module

The vegetation type model distinguishes between different vegetation types which can serve as fuels for wildfires. In order to simplify analysis, we have grouped the vegetation types to three types, crown, grass, and litter, aided by a consulted fire expert [172,184]. This logic is also efficient because of the types of wildland fires: 1.) Crown fires, 2.) Surface fires, 3.) Ground fires, which can be associated with these categorical vegetation types. Additionally, this classification can help the fire crew easily recognize vegetation types, recognize the fuel characteristics of the vegetation, and also the rate of spread characteristics. Hence, the vegetation type model not only helps with the vegetation management plan drawn by the arborists but also helps with mapping the spread rate of the different vegetation that is attainable in different areas.

6.3.1.2 Vegetation Clearance Detection Sub-Module

Vegetation clearance is done to (1.) prevent line sags and sways that can cause direct contact or flashovers that happen when electricity arcs from an energized line to nearby vegetation, (2.) allow distance between vegetation and power equipment since natural storms can fell trees or tree limbs onto lines, poles, and other electric equipment, (3.) allow growth of vegetation such that they do not form a direct path for electricity to travel to the ground. For scheduled maintenance trimming, the vegetation is trimmed along, below, and above power lines, thus removing tree limbs that are within 8 feet along the sides, 10 feet below, and 15 feet above the power lines [195]. Clearance distances are mandated by Occupational Safety and Health Administration (OSHA) and vary with the voltage carried by the line [194]. However, the process of vegetation management is usually manual , using land and air machines, and manual tools which is very time-consuming and expensive, up to billions of dollars annually [194]. For the SL-PWR input data, depending on the level of threat posed by the distance between vegetation and equipment, the input data is labelled as 0.1 for normal distance and hence no threat, 0.5 for elevated threat level, i.e., the vegetation of the area should be managed as soon as the utility can, and 0.8 for extreme threat, where vegetation is in contact with power equipment whether vegetation-to-power equipment or vice versa in the case of sagging or downed lines and equipment, or according to the distance to the ground vegetation.

6.3.2 The Power Equipment Module

This module is active in the “Wildfire Analysis” and “Wildfire Progression” phase of the resilience trapezoid as illustrated in Fig.6.1. During wildfire analysis phase, the UAVs inspect the transmission lines in high threat grids, along the travel path, for arcing/flashovers due to electrical faults. Lines can ignite/arc and remain in place after the actions of protective equipment, or can dissociate from the overhead poles and contact vegetation or ground to become an ignition source for a location with a high ignition potential. In the wildfire progression phase, we suppose the equipment fire/flashovers come in contact with vegetation or the line ejects combustible hot-metal particles to ground and starts ignitions in different locations, or the arcing remains continuous and provides a sustained source of ignition for a tangible amount of time. For example, high impedance (HiZ) faults occur in a sizeable number of faults when a single energized line conductor breaks and falls to earth but the resulting fault draws electrical current that is too small to blow a fuse or trip a circuit breaker due to surface contact resistance. Specifically, a line with HiZ fault can remain energized while it is on the ground for long periods of time which could be tens of minutes producing high-energy, high-temperature arcing. Conventionally, utilities rely on customer calls to detect this condition all while the line could still remain energized on the ground [196]. Hence, the module would alert the operator on fault reclosing recommendations and as well inform the operator when the equipment risk has become a wildfire ignition.

For this reason, we integrate and co-train this module with the wildfire module and modify the training network to output 6 classes which include “wildfire-fire", “wildfire-smoke", “wildfire-normal", “equipment-fire", “equipment-arc", “equipment-normal". The module should be able to differentiate between an equipment fire and an actual wildfire ignition as this is very important information for utilities to be able to route appropriate resources accordingly. Additionally, the module is trained to distinguish between equipment fire and arcing in order to adequately enable the operator take corrective actions to mitigate the fault. For instance, power line arcing can be caused by short-circuits which can result from damage/collapse of the poles/insulators/line structures, high winds which may cause conductor slap, an external conductive object (e.g., birds, wet objects) resting across live lines. On another note, equipment/power line fire can be caused by component contamination or failure in the equipment especially during prolonged dry periods. Component contamination can be as a result of a build-up of debris mixing with moisture to create conducting paths within components, which may lead to arcing and eventually equipment fires. Hence, distinguishing between these event types can aid in faster failure and fault forensics for the utility. Given the above, this module can, thus, also be applied in maintenance of power system equipment.

6.3.3 The Wildfire Module

The wildfire module of the SL-PWR consists of 1.) the fire and smoke detection sub-module, 2.) the fire localization and spread estimation sub-module. It aids to i.) detect ignitions/wildfires/under-surface fires, ii.) prepare utility crew routing to affected areas e.g., extra gear requirements due to heavy smoke. Additionally, this module informs the spread of the fire once ignited and burning, and is active in the wildfire progression phase of the resilience trapezoid as illustrated in Fig. 6.1.

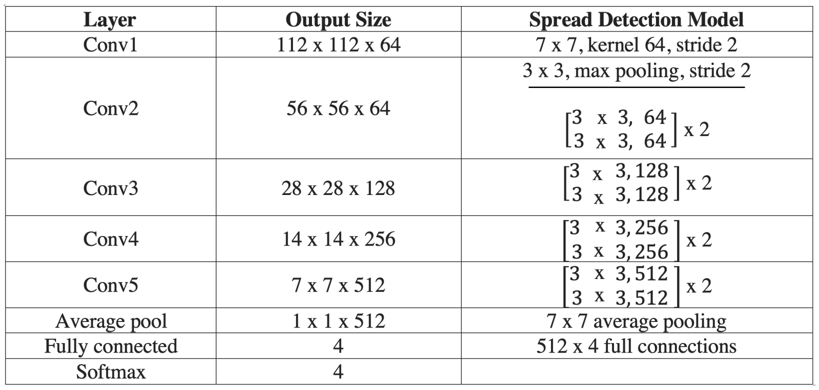
6.3.3.1 Wildfire Fire-Smoke Detection Sub-Module

This sub-module detects the ignition/occurrence of a wildfire. The grid being monitored could be in normal, smoke, or wildfire conditions, hence a multi-class approach is used by adapting the ResNet-18 as in Fig. 6.2. It is co-trained with the power equipment fire-arc detection to improve robustness in distinguishing actual wildfire ignitions from fires/arcs captured on power equipment but have not yet caused an ignition.

6.3.3.2 Wildfire Localization and Spread Estimation Sub-Module

This predicts the wildfire boundaries using bounding boxes and then calculates the radial spread using the box coordinates. Hence, it performs two main functions: 1.) localizes the wildfire in the grid and 2.) calculates wildfire spread area. It also enables a third function, which is 3.) calculating the rate of spread of the wildfire in real-time. The network architecture for this sub-module is illustrated in Table 6.1. where the fully connected layer is modified to an input of 512 neurons

Table 6.1: The CNN training parameters of the localization and spread estimation sub-module.



Layer	Output Size	Spread Detection Model
Conv1	112 x 112 x 64	7 x 7, kernel 64, stride 2
Conv2	56 x 56 x 64	3 x 3, max pooling, stride 2 $\begin{bmatrix}3\text{ x }3, 64\\ 3\text{ x }3, 64\end{bmatrix}$ x 2
Conv3	28 x 28 x 128	$\begin{bmatrix}3\text{ x }3, 128\\ 3\text{ x }3, 128\end{bmatrix}$ x 2
Conv4	14 x 14 x 256	$\begin{bmatrix}3\text{ x }3, 256\\ 3\text{ x }3, 256\end{bmatrix}$ x 2
Conv5	7 x 7 x 512	$\begin{bmatrix}3\text{ x }3, 512\\ 3\text{ x }3, 512\end{bmatrix}$ x 2
Average pool	1 x 1 x 512	7 x 7 average pooling
Fully connected	4	512 x 4 full connections
Softmax	4	

with an output of 4 neurons which represent the wildfire bounding box coordinates to be detected. The 4 neurons indicate fire height h_f, fire width w_f, fire boundary positions on the x and y axis, x_f and y_f respectively, in a 2-dimensional grid, where the UAV captures the wildfire image from above the grid.

Importantly, this calculation takes into account the scale of the UAV image to the actual size of the grid at any height level at which the UAV captures the image, since this height influences the wildfire localization and spread calculation, as illustrated in Fig. 6.5. Hereon, the localization model is developed assuming radial spread and hence an ellipse, as represented in (6.23), inside or outside the predicted bounding boxes, as illustrated in Fig.6.6.

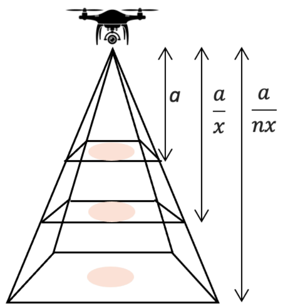


Figure 6.5: Illustrating the UAV-height-informed scaling for radial spread calculation. In the figure, a signifies the area of the fire spread given that a short UAV height/distance from ground-level, x signifies that, as the UAV's distance from the ground increases, the spread area localized by the bounding boxes reduces and this can be applied to any distance-from-ground of the UAV using nx.

$$\left(\frac{y}{b}\right)^2 + \left(\frac{x}{a}\right)^2 = 1 \tag{6.23}$$

$$Area_{box} = 4xy = 4ab \cdot \cos\theta \sin\theta \tag{6.24}$$

$$4ab \cdot \cos\theta \sin\theta = 2ab \sin 2\theta \tag{6.25}$$

where $x = a\cos\theta$ and $y = b\sin\theta$ and the considered ellipse is centered at $(x + \frac{w}{2}, y + \frac{h}{2})$ where w and h are the height and width of the box, respectively. The ellipse external to the locus of the bounding box (i.e., the ellipse circumscribing the localization box) should be used when the bounding boxes are predicted conservatively, i.e., bounding box does not quite enclose fire area, then the area of the spread/ellipse should be assumed largest when $\sin 2\theta = 1$. However in this work, the box coordinates adequately enclose the wildfire location and hence the inscribed ellipse technique is utilized for fire spread as detailed below.

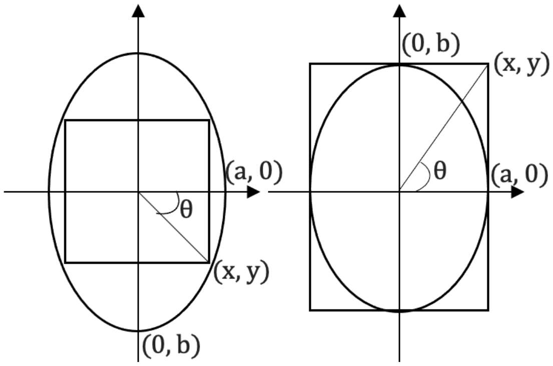


Figure 6.6: Illustrating the wildfire spread calculation assuming radial spread.

Let $a - 0 = A$ and $b - 0 = B$ in Fig. 6.6, then the area of the ellipse is:

$$A_{ellipse} = \pi AB = \pi \times \frac{h_{box}}{2} \times \frac{w_{box}}{2} = \frac{\pi \times h_{box} \times w_{box}}{4} \tag{6.26}$$

Now assume that the box is the wildfire bounding box located in a captured grid which is a scaled version of the original grid, i.e., the UAV distance to ground level decreased during the capture of the image hence the captured image is magnified in comparison to the original image, as in Fig. 6.7. Then, the area of the wildfire spread can be calculated as follows. In order to find the scale of the wildfire bounding boxes, with height and width h_f and w_f respectively, to the original image, the following relationship is defined mathematically as:

$$Area_{b\_box} = \frac{\left(\frac{w_f \times h_f}{h^2}\right)}{\left(\frac{original\_image\_length}{captured\_image\_length}\right)^2} \tag{6.27}$$

where $Area_{b\_box}$ is the scaled area of the wildfire bounding box with height and width w_f and h_f as illustrated in Fig. 6.7.

$$Area_{b\_box} = \frac{\left(\frac{w_f \times h_f}{h^2}\right)}{\left(\frac{h+2a}{h}\right)^2} \tag{6.28}$$

Then assuming radial spread as illustrated in Fig. 6.6, the spread area S_{Area} is calculated as in (6.29).

$$S_{Area} = \frac{\left(\frac{\frac{\pi h_f w_f}{4}}{h^2}\right)}{\left(\frac{h+2a}{h}\right)^2} \tag{6.29}$$

Furthermore, the fire localization and spread detection model can also inform the grid operator on the spread rate of the wildfire. In literature, mathematical models are developed in order

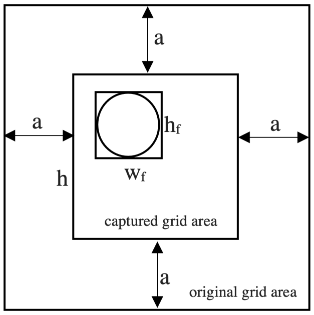


Figure 6.7: Calculating real-time wildfire spread: Scaling to grid area when UAV distance to ground level varies by the parameter "a" as illustrated in Fig. 6.5

to calculate wildfire spread rate, however, to improve situational awareness in utility operations, real-time monitoring is indispensable as spread rates are dynamic parameters which could be exacerbated or otherwise by weather conditions. These parameters such as spread rate can also be unique to certain geographical attributes not represented in the pre-defined mathematical models (e.g., spread rate according to topology/slope/landuse of an area) hence making preexisting models inaccurate for real-time spread rate inference. Hence, the SL-PWR's wildfire localization and spread detection model in the wildfire module can aid to estimate the spread rate of the wildfires in real-time without any dependence on mathematical models, vegetation models, or quantitative data.

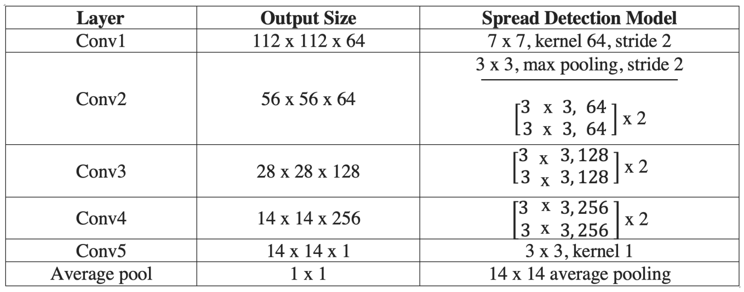
The spread rate can be obtained by getting the spread area of the fire at every time stamp that the UAV captures. The spread rate is then calculated by (6.30).

$$S_{rate} = \frac{{S'_{Area}}^{t} - {S'_{Area}}^{(t-1)}}{t^{t} - t^{(t-1)}} \tag{6.30}$$

where ${S'_{Area}}^{t}$ and ${S'_{Area}}^{(t-1)}$ are the farthest point towards the direction of wildfire spread at time t and $t-1$, respectively.

6.3.4 The Burnt Equipment Detection and Estimation Module

This module is active in the restoration phase of the resilience trapezoid post wildfire occurrence. After the wildfire is suppressed, the power grid equipment in the area will most likely suffer



Layer	Output Size	Spread Detection Model
Conv1	112 x 112 x 64	7 x 7, kernel 64, stride 2
Conv2	56 x 56 x 64	3 x 3, max pooling, stride 2 $\begin{bmatrix} 3 \text{ x } 3, 64 \\ 3 \text{ x } 3, 64 \end{bmatrix}$ x 2
Conv3	28 x 28 x 128	$\begin{bmatrix} 3 \text{ x } 3, 128 \\ 3 \text{ x } 3, 128 \end{bmatrix}$ x 2
Conv4	14 x 14 x 256	$\begin{bmatrix} 3 \text{ x } 3, 256 \\ 3 \text{ x } 3, 256 \end{bmatrix}$ x 2
Conv5	14 x 14 x 1	3 x 3, kernel 1
Average pool	1 x 1	14 x 14 average pooling

Figure 6.8: The CNN architecture and parameters of the Burned Equipment Detection/Estimation training module.

some damages and burns depending on the amount of time the fire-fighting crew spent to curtail the fire. Conventionally, power utilities would route supervisory crews to different areas of the burnt grids to inspect the level of equipment damage towards an estimation of restoration costs [197]. This technique would increase not just the cost of damage estimation but also time to infrastructural restoration of the system. With the Burn Equipment Detection and Estimation Module, the UAVs can monitor the status of equipment providing the type and level of burn damage towards a more economic and transparent approach to cost estimation. A major advantage of this module is that it comes with actual equipment images and provides a high level of transparency in cost estimation. The architecture of this sub-module consists the detection and estimation parts. The detection part is a classification model that aims to differentiate between the main types of damages to the power equipment after wildfires occur which are 1.) The burning/damage of the top/cross arm area of the power pole 2.) The burning of the base of the power pole 3.) The leaning of the power pole structure from the axis of the normal as illustrated in Fig. 6.9. In this case, the detection network is basically as in Table 6.1, however, with the fully-connected and softmax layers having 3 neurons respectively.

The estimation network for each of these types of damage then consists of a series of convolutional layers which take as input, positively classified images and culminate towards predicting a scalar that informs the extent of burn damage. The architecture of this sub-module is as illustrated in Fig. 6.8, where the layer 5 of the convolution is modified from 512 channels to 1 channel, and then the 14 x 14 average pooling is performed which then yields the scalar value representing the burn damage estimation of the input image. The labelling of the input image ground truth takes certain logic for different burn damage scenarios as illustrated in Fig. 6.9.

6.3.4.1 Calculating the parameters of poles affected by burning

Here, we discuss the calculation technique for obtaining accurate electric equipment parameters after a wildfire/burning/arcing incident. After the incident occurs, the UAV arrives and takes images of the power system equipment. However, there is need to map the height parameters of the captured image with the real equipment parameters, as in Fig.6.10. In order to do this, we employ

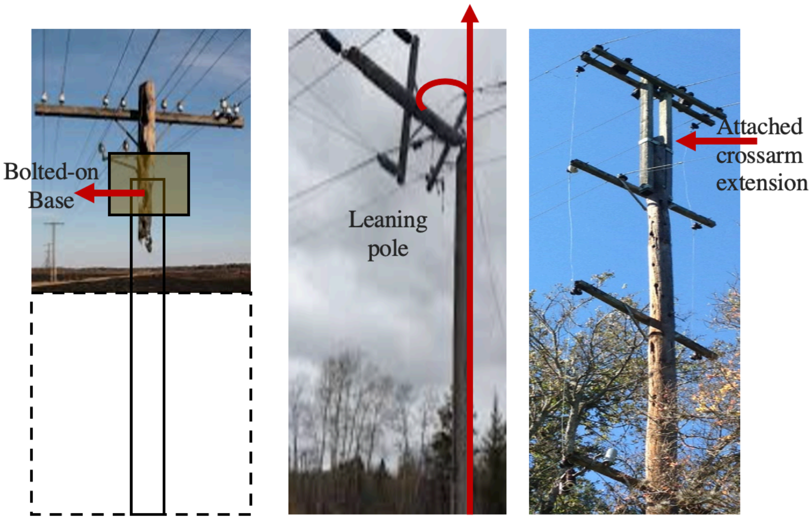


Figure 6.9: Scenario types for system restoration in the Burn Damage Detection and Estimation module.

the use of reference heights in electric poles, where references will be any object/mark of a known height. For instance, the reference could be the pole tags which are already widely employed by power utilities. The pole height can be calculated as:

$$H_T = \left(\frac{H_T^p}{H_R^p}\right) H_R \tag{6.31}$$

where H_T is the actual height of the electric equipment, H_T^p is the measured height of the electric equipment in the captured image/picture, H_R is the actual height of the reference, and H_R^p is the measured height of the reference object in the captured image/picture. The normal image of the equipment for which H_T is calculated can be used as a permanent documentation of the height measurement of the equipment in question and or similar equipment. As illustrated in Fig.6.9, for the three common scenarios being considered, estimation are as follows.

6.3.4.1.1 Scenario 1/Bolted-on base:

$$H_{bolted} = \left[\left(\frac{H_T^p}{H_R^p}\right) H_R - \left(\frac{H_{T_{burnt}}^p}{H_R^p}\right) H_R\right] + L \tag{6.32}$$

where H_{bolted} is the estimated height of the burnt base to be bolted-on, $H^p_{T_{burnt}}$ is the measured height of the remaining top part of the equipment from the captured image, and L is the total of the margin of error + the part of the pole that goes underground for the foundation of the equipment.

6.3.4.1.2 Scenario 2/Leaning pole:

$$H_D = H_T - H_{TL} = \left[\left(\frac{H^p_T}{H^p_R} \right) H_R - \left(\frac{H^p_{T_{leaning}}}{H^p_R} \right) H_R \right] \tag{6.33}$$

where $H_{T^p_{leaning}}$ is the measured height of the leaning power equipment in the captured image.

Furthermore, the angle of lean/angle of tilt φ can either be estimated directly from the image or can be calculated more accurately albeit more rigorous, as follows.

$$\varphi = \sigma \tag{6.34}$$

where σ is the angle made by the line parallel to the leaning part of the pole at the baseline with length b and perpendicular to the slope with distance s, θ is the angle of view of the camera mounted

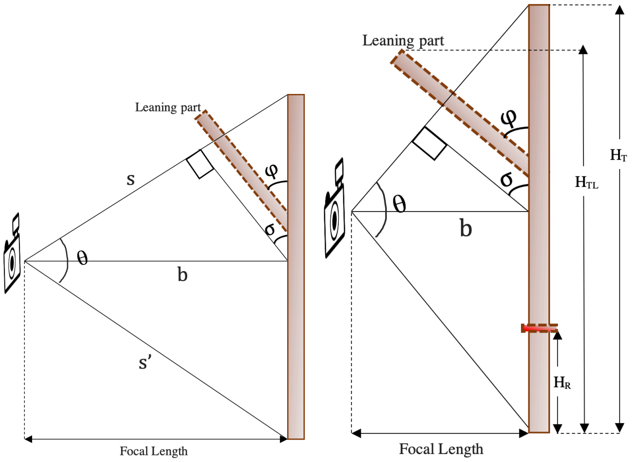


Figure 6.10: Restoration estimation for damaged poles.

on the UAV and is calculated as follows.

$$\theta = 2 \times \arctan\left(\frac{S_W}{2 \times F_L}\right)(180/pi) \tag{6.35}$$

where S_W is the sensor width also known as the width of the camera film (these are standard for different camera types), F_L is the focal length of the camera lenses, and $(180/pi)$ aids the conversion between degrees and radians. In practice, it may become problematic to position the UAV in such a way as to obtain the line which is parallel to the leaning part and perpendicular to the slope in order to calculate the angle σ as $\left[90° - \left(90° - \frac{\theta}{2}\right)\right]$, hence close approximations can be made by "eye-balling" the images.

6.3.4.1.3 Scenario 3/Attached cross-arm extension:

$$H_{cross-arm} = \left[\left(\frac{H_T^p}{H_R^p}\right) H_R - \left(\frac{H_{T_{base}}^p}{H_R^p}\right) H_R\right] + e \tag{6.36}$$

where $H_{T_{base}}^p$ is the measured height of the remaining unburnt part of the power equipment. Here, the parameter L is eliminated since the margin of error can easily be compensated for using e and there is no need for estimating the height of the equipment to be buried towards the equipment foundation.

6.4 Optimization of system UAV resources

It is important to mitigate both endogenous and exogenous wildfires before they occur, or manage these fires in real-time, if they occur. Toward this end, the SL-PWR model utilizes potential ignitions pre-wildfire in order to prepare for critical scenarios and proceed with optimal strategies to better respond to and mitigate risks arising from extreme wildfire events including the propensity of outages caused by exogenous wildfires and power shutoff to customers as a result of wildfire threat (de-energization to prevent endogenous/power equipment-caused wildfire).

Hence, the UAV system of the SL-PWR is tasked with obtaining images of geographical locations of interest in terms of power equipment, vegetation, and potential ignition locations towards preventing both endogenous and exogenous wildfires. In order to obtain the input images, the UAV flies over the geographical area under consideration taking in GPS navigation enabled by the potential ignition probability maps produced by the STWIP model [184]. First the STWIP sends in all the $i.loc$ with normal-elevated-extreme levels of wildfire threat, where normal threat level locations ($i.loc$) has probability ≤ 0.5, elevated threat level $i.loc$ have $0.5 \leq$ probability ≥ 0.8 and extreme threat level $i.loc$ have probability ≥ 0.8. Note that since the forecasted threat locations in the potential ignition probability map have a "cluster-like" attribute, i.e., if an $i.loc$ is of extreme threat level then there is a high probability that surrounding grid points have the same threat level, the UAVs can be stationed in the center ($g_c.loc$) of the grid with the cluster under consideration. Assume the resource information collection is as illustrated in Fig.6.11, and the potential ignition map from STWIP is as furnished where grids G1 and G5 have the extreme and elevated threat levels respectively, and Vg_i is the vegetation type (crown Vg_1, grass Vg_2, litter Vg_3) associated with the grids. Furthermore, PE_i is the amount of power equipment associated with the grids, for instance, PE_1 has a higher criticality (weight) in terms of power equipment since it has more 4 lines, a generator and 3 buses, than PE_2 with 4 lines and 2 buses, and PE_3 with 2 lines and 2 buses,

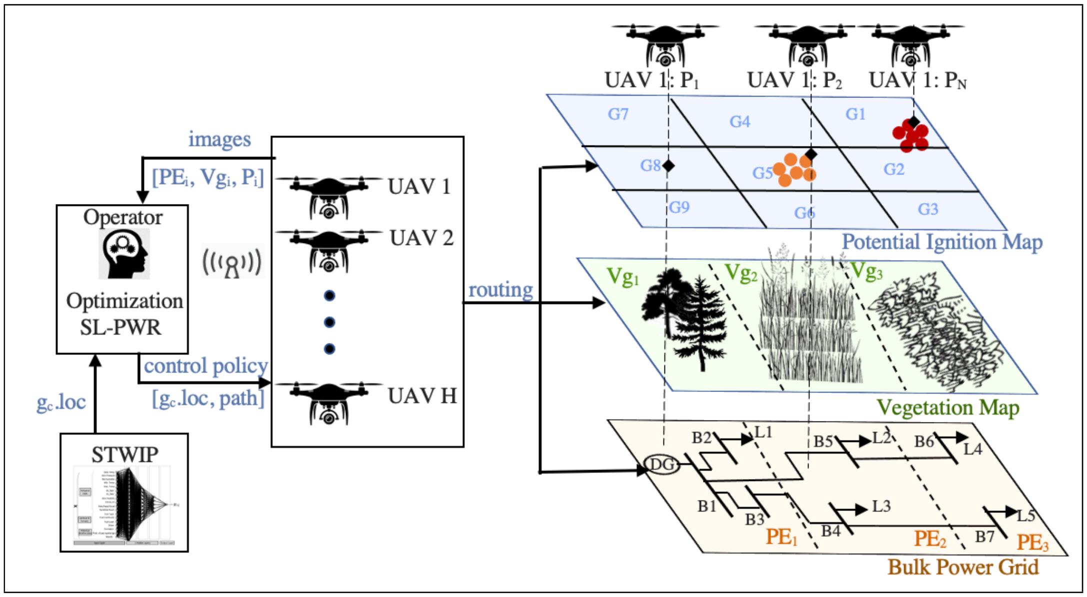


Figure 6.11: Illustrating the UAV resource optimization problem.

assuming the loads served in each area are equal i.e., $L1 = L2 + L3 = L4 + L5$. Additionally, PE_i factors in the **"Power Equipment Age"** and **"Fault Frequency"** of the equipment in the said grids.

The goal is to route $UAV1$ to grid $G1$ to monitor the extreme threat for the length of time the threat is viable. However, in order to get to $G1$, the $UAV1$ gets to travel along a path, and since the UAVs are limited resources, the operator wants to maximize the monitoring of critical grids without compromising with the risk posed by $G1$. Towards this aim, a weighting/criticality factor is also assigned to the grids $(G1 - G9)$ depending on the threat level in the potential ignition maps i.e., criticality of $G1 \geq$ criticality of $G5 \geq$ criticality of ($G2 - G4, G6 - G9$). A sample optimal route would be $\{G8 - G5 - G1\}$ because in $G8$ there exists crown vegetation and higher amount of power equipment, increasing the likelihood of there being tall encroaching vegetation towards power lines. In $G5$ there are also 4 power lines with grass vegetation making the rate of spread of fires rapid if power lines sag or fall to the ground. Thus the SL-PWR will obtain more crucial and targeted information via this path as opposed to $\{G3 - G2 - G1\}$ which has a lower number of power lines and with litter vegetation which does not pose as much threat in a wildfire scenario.

Note that the grid centers are assumed equidistant since the UAVs are airborne and can fly directly to grid centers as opposed to land mobiles that have to go through a road network. Hence, the optimization proposed in this section is to capture the routing of UAV resources since these resources can be limited in availability due to cost of purchase (dollar cost) or cost of operation (computational and dollar cost of training and transport). The UAV routing problem is a bi-level one illustrated in Fig.6.12 and formulated as follows:

6.4.1 Upper Level

This determines the UAV path by maximizing the criticality across the PE, Vg, and G layers of the geographical area as illustrated in Fig.6.11. In (6.37), the objective is to maximize the criticality

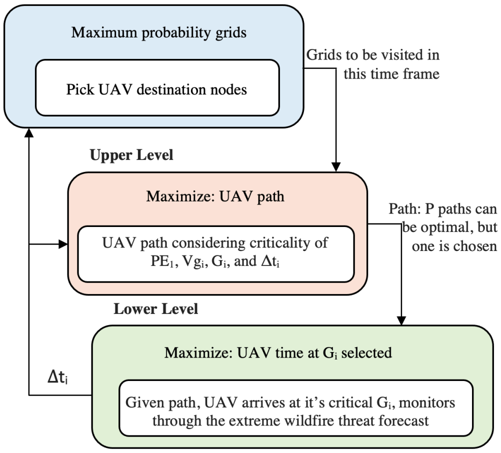

Maximum probability grids
Pick UAV destination nodes
Grids to be visited in this time frame
Upper Level
Maximize: UAV path
UAV path considering criticality of PE$_1$, Vg$_i$, G$_i$, and Δt$_i$
Path: P paths can be optimal, but one is chosen
Lower Level
Maximize: UAV time at G$_i$ selected
Given path, UAV arrives at it's critical G$_i$, monitors through the extreme wildfire threat forecast
Δt$_i$

Figure 6.12: Illustrating the UAV resource optimization problem. The maximum probability grids are picked from the potential ignition probability map from STWIP and these become the monitoring destination of the UAVs. However, the path of the UAV to the destination grid is optimized in order to utilize limited UAV resources more efficiently.

of the grids towards optimizing the travel path of the UAV as it moves along to its destination grid.

$$\max \quad \sum_{i \in path} PE_i \cdot Vgi \cdot Cr_i \cdot \Delta t_i \tag{6.37}$$

The equation is maximized $path = \{p_1, p_2, \cdot\cdot\cdot, p_N\}$, $\forall$ UAV $=\{1, 2, \cdot\cdot\cdot, J\}$ where PE_i is the information of power lines (amount/density, age, fault frequency) in the grid i, Vg_i is the growth rate of vegetation predominant in i, Cr_i is the criticality of potential ignition in i (normal, elevated and extreme probability grids), and Δt_i is the amount of time since the grid was last visited by a UAV. Hence, the objective of (6.37) is to choose the optimal UAV paths given that high vegetation growth areas are quickly able to encroach power lines and need to be visited often. As well, grids with high power equipment density are more likely to cause endogenous wildfires than lower density grids. The criticality of the grids ensures that even elevated wildfire threat grids can also be visited even if not as oven as the extreme grids. This is because, occasionally wildfires can occur outside the predicted extreme area as was the case with the famous Campfire. Lastly, Δt_i ensures that grids of sufficient criticality are not overlooked for too long and are visited occasionally.

6.4.1.1 UAV-Resource Constraints:

$$\sum_{i=1}^{N} p_i^d \leq s_{UAV} \cdot t_{UAV}^{charge} \quad \forall \quad UAV \tag{6.38}$$

where N is the number of grids in the chosen path, s_{UAV} is the travel speed of the UAV, t_{UAV}^{charge} is the time the UAV charge will last, and p_i^d is the distance it takes to get to grid i from the preceding grid $i-1$ in the path assuming equidistant grid centers, since the UAVs fly and there is a straight line of flight between the $g_c.loc$ of adjacent grids $i-1$ and i in the path. This constraint ensures that the UAV path is feasible in terms of the time of travel afforded by the UAV's charge state. Further weeding out of infeasible paths can be done with high-fog/high storm grids. The output of this level is a set of selected paths $P_{UAV} = \{p_1, p_2, \cdot\cdot\cdot, p_N\}$ for every UAV.

6.4.2 Lower Level

The lower level problem is a maximum UAV monitoring coverage one taking in the output of the upper level, $P_{UAV} = \{p_1, p_2, \cdot\cdot\cdot, p_N\}$. In each path p_i, there are grids from $i = \{1, \cdot\cdot\cdot, I\}$ The UAV optimization has to ensure that the UAV does not spend undue and valuable time monitoring/flying through the paths $(I-1)$ leading to the assigned destination grid I. Hence, this level ensures that the UAV-assigned extreme threat grid gets maximum monitoring coverage in and within the appropriate time.

$$\max \quad \sum_{p_i \in P_{UAV}} y_j \cdot \tau_j^I \cdot Cr_{sum}^{p_i} \quad \forall \quad UAV \tag{6.39}$$

$$\sum^{P_{UAV}} y_j \leq 1 \tag{6.40}$$

$$\tau_j^{I-1} \leq T_s^I \tag{6.41}$$

$$\tau_j^I \geq T_e^I - T_s^I \tag{6.42}$$

In (6.39), the goal is to ensure that within the selected paths, the paths with higher criticality is maximized while ensuring that the most time within the UAV travel time is spent monitoring the assigned destination grid I which is the last grid in the selected path, where y_j is a binary variable that indicates if a path is selected $(y_j = 1)$ for UAV j or not, τ_j^I is the amount of time spent at I by UAV j, and $Cr_{sum}^{p_i}$ is the criticality of the path i.e., weight of all grid nodes in the path. In (6.40), the aim is to ensure that for each UAV, no more than a path is selected for travel to its destination node I, however, once the UAV arrives at that destination it can still add another route to its trip if the feasibility constraints allow, (6.41) ensures that the travel time through the path just before the UAV arrives at I is less than the predicted start time of the wildfire threat T_s^I, and (6.42) ensures that the UAV keeps monitoring I for the duration of the wildfire threat, where T_e^I is the end time of the wildfire threat i.e., the time until which the wildfire threat is viable.

6.4.3 UAV Optimization Process

A graph-theoretic algorithm is proposed for the UAV optimization procedure presented. A three-step procedure is proposed to determine the optimal UAV monitoring strategy: 1.) build the UAV monitoring trees forming UAV paths based on grid criticality 2.) path selection and 3.) solve for maximum monitoring coverage at I. In the first step, the paths from the UAVs to the extreme wildfire threat grids are identified. Hence, each UAV could have more than one monitoring path forming a monitoring tree with all paths starting from that UAV as the root node. In the second step the path selection is carried out limiting the set of paths to feasible paths through which the UAV could travel and considering the UAV charge capacity. The third step takes care of the maximum monitoring coverage of the UAV over the assigned high wildfire risk grid. In this step, it is ensured that the UAV flies through the most critical path while not spending crucial time on the path of travel and spends the optimal time monitoring it's assigned grid. This is achieved by ensuring the UAV time spent at it's assigned grid is maximized while making sure the time spent in the travel path does not exceed the start time of the wildfire risk forecast and that the UAV monitors the high risk grid till the end of the high risk forecast.

6.4.3.1 Building the Monitoring Trees

The geographical area is modeled as an undirected graph **G = (V, E)** with different layers including the potential ignition map, the vegetation layer and the power equipment layer. The set of nodes **V** represent the grid centers that carry the grid attributes through these different layers. The set of edges **E** represent the inter-grid UAV flight path which is assumed to be an equidistant and direct line of flight. Additionally, a source node is the node from which a UAV takes off while a destination node is the critical high risk node to which a UAV has been assigned to monitor. Each node has a weight w whose value is set to the combined criticality of the grid across all its layers, and each path has a weight $Cr_{sum}^{p_i}$ which is the sum of criticality of the nodes on the path. The UAV-monitoring path is the path with the highest criticality/weight that gets to the destination node within the critical time. A modified Dijkstra's algorithm is used to obtain the paths from the UAV source node to the assigned destination node to form the monitoring tree and via pruning the tree, infeasible paths are eliminated. The pseudo code for the building the UAV monitoring tree is as illustrated in Algorithm 5. From the algorithm, the UAV monitoring paths are returned as a tree whose root node is sourced from s. Furthermore, for a node v $\in$ **V**, v.dist is the distance from s to v which is the weight/criticality $Cr_{sum}^{p_v}$ of the nodes in the monitoring path from s to v, and v.dist will be updated to equal the weight of the monitoring path when a monitoring path is found. The criticality of each grid is adjusted to M-Cr_i^{tot*} in order to maintain the shortest path attribute of the algorithm since our objective is to maximize the weight of the chosen path and the Dijkstra's algorithm does not work well with negative weights, where M is a fixed number bigger than Cr_i^{tot*} across all UAVs. Additionally, v.path is the set that will contain the predecessors of v forming individual paths which are then appended to v.trip. A priority sequence S is used to store nodes that have not been explored by the algorithm and also to manage the nodes which form key-value pairs with the node's distance. The nodes are explored by extracting from S, the node with the minimum distance and adding such a node to the v.path for that UAV which should run from its source node to the assigned destination if a path exists.

Algorithm 5 Building the UAV Monitoring Tree

```
▷ Initialization of parameters
for node v $\in$ V do
    v.dist $\leftarrow \infty$
    v.path $\leftarrow \{\}$
    v.trip $\leftarrow \{\}$
    v.trips $\leftarrow \{\}$
    D* $\leftarrow \{\}$
    M $\leftarrow$ big number
end for
s.dist $\leftarrow$ 0
S $\leftarrow$ V
D $\leftarrow$ Set of UAV destination nodes
T $\leftarrow$ Set of wildfire threat start time of elements of D
▷ Obtain UAV monitoring paths
while D $\neq \emptyset$ do
    $q \leftarrow$ EXTRACT-MIN-DIST(S)
    for node v $\in$ adjacent to $q$ do
        ▷ Modified Dijkstra relaxation operation
        $Cr_i^{tot*}$ = $PE_i \cdot Vgi \cdot Cr_i \cdot \Delta t_i$
        $Cr_i^{tot}$ = M-$Cr_i^{tot*}$
        if v.dist $\geq$ q.dist + $Cr_i^{tot}$ then
            v.dist $\leftarrow$ q.dist + $Cr_i^{tot}$
            v.path $\leftarrow q$
        end if
    end for
    if $q \in$ D then
        D $\leftarrow$ D - {q}
        v.trip $\leftarrow$ v.path
        v.path $\leftarrow \emptyset$
    end if
    if S $= \emptyset$ then
        D* $\leftarrow$ q
        v.trips $\leftarrow$ v.trip
        v.trip $\leftarrow \emptyset$
        S $\leftarrow$ V
    end if
end while
▷ Build the UAV monitoring tree
$\mathbf{V_{tree}} \leftarrow \{s\}$
$\mathbf{E_{tree}} \leftarrow \emptyset$
for destination node v $\in$ D* do
    Check the monitoring trip feasibility from s to v
    Feasibility based on the UAV flight range, weather conditions, and travel time.
    Travel time is before threat start time forecast in T
    if monitoring path is feasible from s to v then
        ▷ Add nodes to monitoring path, v to $\mathbf{V_{tree}}$, and add edges to $\mathbf{E_{tree}}$.
        ▷ Drop extra paths if any, leaving one feasible path in v.paths
        while v $\notin \mathbf{V_{tree}}$ do
            $\mathbf{V_{tree}} \leftarrow \mathbf{V_{tree}} \cup$ {v}
            $\mathbf{E_{tree}} \leftarrow \mathbf{E_{tree}} \cup$ {v.trips[v], v}
            v $\leftarrow$ v.trips[v]
        end while
    end if
end for
▷ Return
Tree $\leftarrow$ ($\mathbf{V_{tree}}$, $\mathbf{E_{tree}}$) =0
```

Hence, Lines 2-10 initializes the parameters for the nodes towards implementing the modified Dijkstra's relaxation operation where distance value (dist) of all nodes are set to infinity while the source node's is set to 0 (Line 10). For each v, the v.path is a null set where the predecessors q of v are appended. In Line 8, a fixed number, M, bigger than Cr_i^{tot*} across all UAVs is defined in order to maintain the minimum distance attribute of the Dijkstra's shortest path. In Line 11, all nodes (grid centers) are inserted into the sequence $\mathbf{S}$, the set of destination nodes $\mathbf{D}$ is defined in Line 10, while the set of predicted potential wildfire risk start time in each of the grids $\mathbf{T}$ is defined in Line 13. Since the distance from adjacent grid centers are equidistant, the time taken to travel a path can be easily obtained given the speed of the UAV. In the **while** loop of Lines 15-37, a modified Dijkstra's algorithm is utilized to find the UAV monitoring paths to the destination node. Here, for each destination node, the node q, with the minimum distance (in the first iteration, this is the source node with s.dist=0), is extracted from $\mathbf{S}$ and explored. After extracting q, the relaxation operation is applied to the nodes adjacent to q as seen in Lines 17-25, and it is removed from $\mathbf{S}$. This is modified in this paper, since we seek the path with the maximum criticality for the UAV, hence the fixed number M is introduced for which Cr_i^{tot} must be positive across all UAVs. If q is a destination node, then a monitoring path is found for that destination node and q is removed from the set of destination nodes (Lines 26-27), v.path is appended to v.trip (Lines 28) while the UAV moves along to another destination node in the same trip if feasible. This ensures that in a UAV trip it could be able to get to more than one destination node if possible. This is enabled by Lines 31-36, the node set in G is appended back to $\mathbf{S}$ if the sequence becomes empty before $\mathbf{D}$ becomes empty (signifying the end of a trip). This ensures that each destination node is explored and reached once if a path exists, and while all destination nodes have not been explored but $\mathbf{S}$ is empty, the UAV monitoring path is renewed from s to form several other paths (and possibly trips) to explore the destination nodes that have not been explored. In Line 32, the elements of set $\mathbf{D}*$ are the leaf nodes of each UAV tree. This is further demonstrated in Fig.6.13.

The search for the monitoring path ends when either of the all destination nodes have been explored if path found ($\mathbf{D} = \emptyset$) or otherwise e.g., when there is an obstacle such as storm that

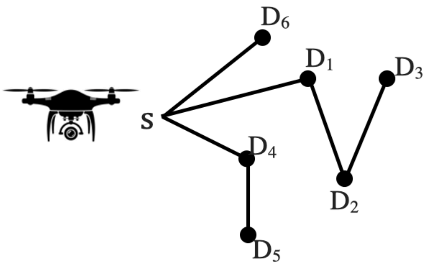


Figure 6.13: Illustrating the UAV trip with destination nodes $\{D_1, D_2, D_3, D_4, D_5, D_6\}$, the first total travel path (a trip) for the UAV may contain the paths to $\{D_1, D_2, D_3\}$ before the set $\mathbf{S}$ goes empty, then the set $\mathbf{S}$ is replenished with $\mathbf{V}$ to make another trip which may contain $\{D_4, D_5\}$ before the set $\mathbf{S}$ goes empty, then again $\mathbf{S}$ is replenished with $\mathbf{V}$ to make a trip to $\{D_6\}$. This is more efficient as the UAV trip covers more destination nodes in one trip, as opposed to returning to the source after reaching one destination.

prevents the UAV from traveling through a grid. Lines 38-53 build the UAV monitoring tree, where a feasible trip is chosen for each UAV from source node s to destination node $\in \mathbf{D}*$. The graph Tree which is made up of ($\mathbf{V_{tree}}$, $\mathbf{E_{tree}}$) represents the UAV monitoring tree where $\mathbf{V_{tree}}$ is the set of nodes of the tree, and $\mathbf{E_{tree}}$ is the tree's edge set, not including infeasible paths or dropped trips.

6.5 Simulation and Results

We evaluate all modules of the SL-PWR model using well performing hyper-parameters, for instance, learning rates are tested in powers of 10 as optimizing the hyper-parameters are better in log space. Moreover, since there are no existing image databases towards the different modules of the proposed model, the work in this chapter significantly focuses tangible effort on data collection and processing, using search engines to gather relevant images which serve as substitute to the UAV captured images. Input data post screening consisted of $>$ 1800 images including 863 images of which 307 vegetation type images consisting of 55.43% of crown vegetation, 28.80% of grass vegetation, and 15.75% of litter vegetation types. Additionally, there are 283 vegetation distance dataset images and 125 images for fire spread prediction, and 286 images for the burnt detection and estimation module with Leaning: 27.33%, Bolted_base: 36.63%, Extended_cross-

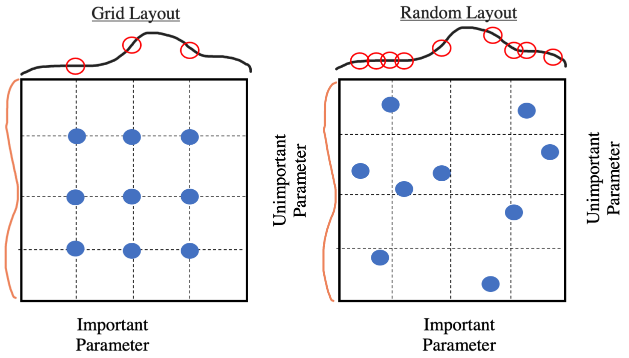


Figure 6.14: Using random search hyper-parameter optimization ensures that more of the hyper-parameter space is visited while training the CNNs.

arm: 36.05%. The images are resized to 224 x 224 with RGB color channels to rhyme with the input requirements of the base ResNet model, and are color normalized. This color normalization aids the emulation of different times of day in which the UAV will supposedly capture images for the SL-PWR model, using contrast from 0-255 for minimum to maximum intensity pixels. For all modules, we split it's database to a training, validation and test dataset which have three major data augmentations including five-crop, random flipping and color jittering. Prior to the five-crop, the images are padded and resized to 235 x 235 and the images are cropped at the four image edges and at the image center to a final 224 x 224 size. The hyper-parameters such as the learning rate are set after cross-validation where, using the random layout technique [198], such that distinct values of the function are visited during the hyper-parameter optimization as illustrated in Fig. 6.14. Different learning rates are trained over epochs and validated, where the hyper-parameter with the

Table 6.2: Parameters of the SL-PWR model.

Module	Sub-modules	Learnable params.	Train. And Eval. Samples	Epochs	Train&Eval. time (sec.)	Image prediction time (sec./image)
Vegetation	Type Detector	11178051	245	25	222.18	0.139188909
	Clearance Estimator	2783041	227	100	188.05	0.181152294
Power Equipment	Type Detector	11179590	690	25	608.75	0.067470726
Wildfire	Fire-Smoke Detector					
	Spread Estimator	2783041	100	100	170.07	0.027984476
	Localization Estimator	11178564	100	200	391.07	0.035381708
Burnt-Equipment	Damage Type Detector	11178051	230	150	778.13	0.16672171
	Damage Estimator	2783041	230	100	492.25	0.028728008

best validation result is chosen. The training hyper-parameters are then fixed while a batch size of 64 images are mostly used, with Adam optimizer and 25 training epochs using the TensorFlow framework and Google Colaboratory using designated GPU runtime. The modules are trained and validated individually except for the wildfire module and the power equipment module which is intentionally trained together so that the SL-PWR model could be sensitive to an equipment fire vs. an ignited and flaming wildfire. The model, summarized in Table 6.2, which shows "Very Early Detection" of less than 40 milliseconds once the UAV images are captured. This "Very Early Detection" is crucial in fire fighting as every second matters. For all the modules, the dataset is split into $\frac{6}{10}$ for training data, $\frac{2}{10}$ for validation data, and $\frac{2}{10}$ for test data.

6.5.1 The Vegetation Module

This module consists of the base CNNs which are trained towards detecting the vegetation types and the vegetation clearance distance towards the utility vegetation management. The input dataset of the first CNN consists of all images from the 3 different classes for vegetation types namely: grass, crown and litter, while the output consisted of the classification of the input image into one of these 3 umbrellas. In training this network, the Adam optimizer is used with a learning rate of 5×10^{-5}, while a batch of 64 images is trained over 25 epochs. The sub-module performance can be seen in Fig.6.15, where the validation accuracy is up to 93.4% and the test accuracy against

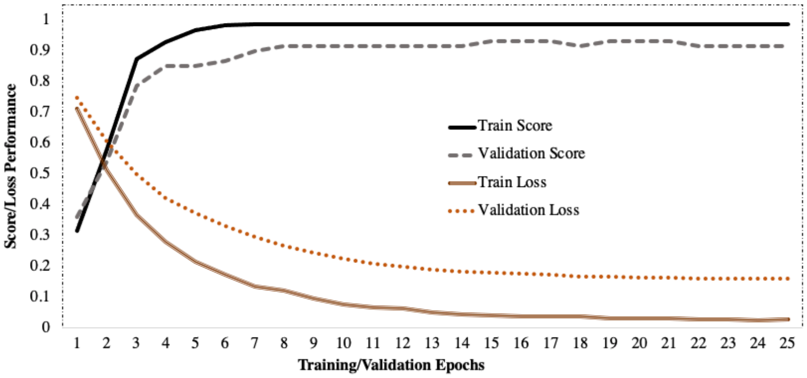


Figure 6.15: Training and validation performance of the Vegetation Type module. The validation accuracy improves over training epochs while the loss is minimized.

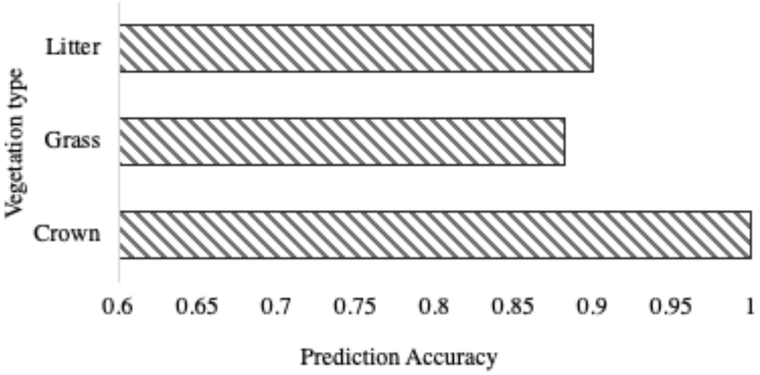


Figure 6.16: Independent prediction accuracy results for the Vegetation Type module.

the unseen part of the dataset is 91.8%. The Fig.6.15 also shows the variation of the cross entropy loss function over different epochs in the training and validation of the network, showing great improvement as the training epochs progressed.

The second network in this module estimates the vegetation clearance distance, hence taking an input of images and outputting a scalar value of the level of clearance of vegetation from the power equipment. The level of clearance is on a scale of (extreme = 0.1, elevated = 0.5, normal = 0.8) depending on the closeness of the vegetation to the power lines. The parameters such as the optimizer used is similar to the previous network, however, the learning rate is 2×10^{-5}, with

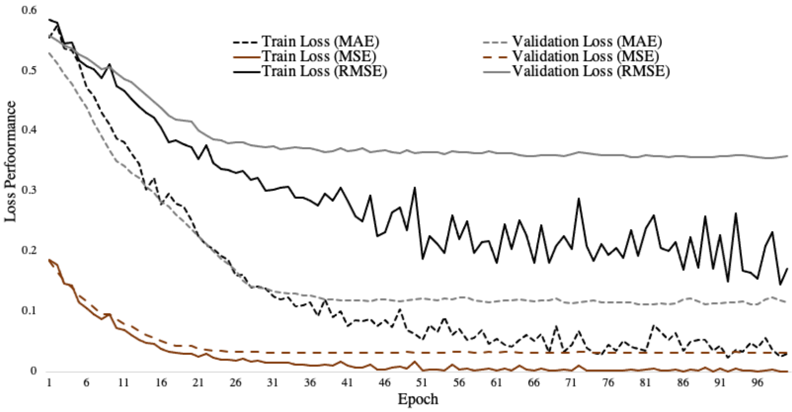


Figure 6.17: Vegetation clearance estimator results.

the batch size reduced to 32 while the number of epochs is increased to 100 in order to further facilitate learning.

6.5.2 The Power Equipment Module

As discussed earlier, the power equipment module is co-trained with the wildfire fire-smoke detection in order to further learn the different fire types ("equipment fire", "wildfire fire") and also the similar incidents such as equipment arcing. The Adam optimizer is also used with a learning rate of 5×10^{-5} and a batch size of 64 images trained over 25 epochs. The performance of the module is as visualized in Fig. 6.18, with the performance of the module on unseen images i.e., the test data prediction accuracy as 89.60%.

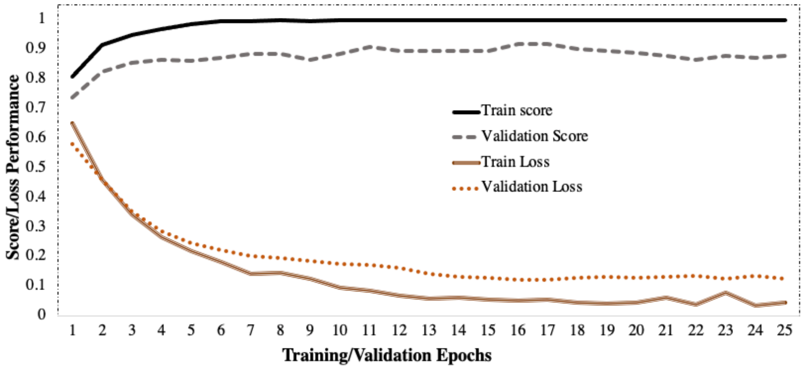
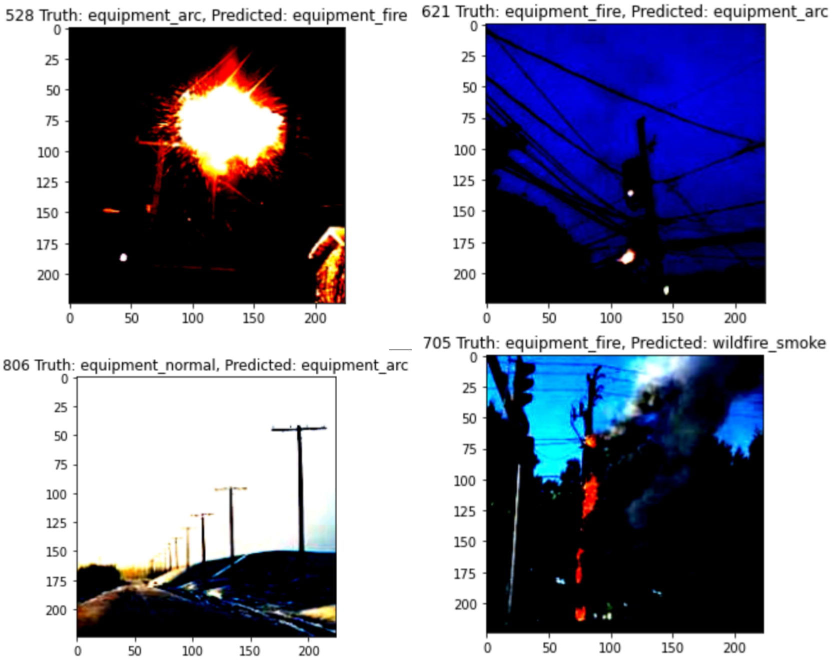


Figure 6.18: The accuracy and loss results of the Power Equipment module combined with the Wildfire and Smoke Detection module.

Next, we illustrate the mispredictions of the module in order to understand how to better improve the network. It can be seen that the network generally performs relatively worse when the data augmentation is darker i.e., simulating night time. For instance, according to Fig. 6.19, at night time, the module is quite stumped on the difference between an equipment arcing and an equipment fire since both are bright reddish at night time. On a similar note, with the data augmentation emulating sunrise in the third image, the brightness of the sun angle is seemingly confused for an arcing incident down the line of sight of the poles. In the fourth image, there is both fire and smoke in the image and since the night time shadows the smoke, the equipment fire is more visible. This highlights the need for using night vision cameras with the UAVs. It also highlights the need for the system operator to take a look at the reason the SL-PWR is raising an incident alarm by looking at the captured image in particular. These mispredictions can be improved or even mitigated with more training data samples of these incident types.

6.5.3 The Wildfire Module

The wildfire module consists of the 1.) wildfire fire-smoke detector, 2.) the spread estimation 3.) the fire localization model. The wildfire fire-smoke detector is co-trained with the power equipment module as discussed earlier. The spread estimation evaluates the spread of the fire in the "gxg" km grid cell that the UAV is monitoring according to (6.29), while the localization model tells the location of the fire in the monitored grid cell. These sub-modules are further discussed as follows.


528 Truth: equipment_arc, Predicted: equipment_fire

621 Truth: equipment_fire, Predicted: equipment_arc

806 Truth: equipment_normal, Predicted: equipment_arc

705 Truth: equipment_fire, Predicted: wildfire_smoke

Figure 6.19: The mispredictions of the equipment type module .

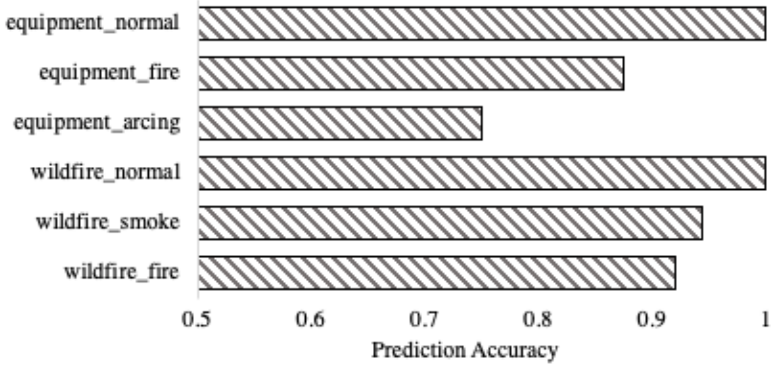


Figure 6.20: Independent accuracy of the Wildfire-Equipment classification.

6.5.3.1 Wildfire Fire-Smoke Detection Model

Since this module is co-trained with the equipment module, the same parameters apply with the training of the network. The mispredictions of the network relative to the wildfire fire-smoke detection can be seen to be challenging during the night time also, where the darkness masks the smoke and hence the network is only able to detect the fire.

Moreover, we can see the prediction accuracy for individual classes predicted by the wildfire-equipment type network as in Fig. 6.20. The network is 100% able to detect the normal conditions hence leaving little to no chance of a false positive. With the wildfire fire and smoke, the network's performance is $>$ 90%, while the equipment fire is a little short of 90% prediction accuracy. The least prediction accuracy is the equipment arcing with performance at about 75%. This performance can be improved by increasing the number of input samples fed into the network which as can be seen in Fig. 6.4, the equipment arcing examples is barely 7% of the input data.

6.5.3.2 Wildfire Localization and Spread Estimation Model

First, we discuss the spread estimation sub-module. The wildfire spread is calculated and labeled as discussed in (6.29). The network is trained with the Adam optimizer, with a learning rate of 2×10^{-5} and a batch size of 32, over 100 epochs. The performance of the spread estimator is as shown in Fig. 6.21 which shows the MAE and MSE reduction with the training epochs, while the average MSE for the test data is 0.01166.

Secondly we discuss the localization estimator which locates the fire on the grid cell being monitored. In order to do this, we need the fire position in the x and y axis and the height and width of the fire around its boundaries. The localization estimator then needs to predict these 4 parameters in order to locate the fire on the monitored grid. The network is trained with Adam optimizer, minimizing over the MSE loss (regression model), with a learning rate of 1×10^{-3} and a batch size of 64, over 200 epochs. The performance of the model with respect to the loss minimization (MAE and MSE) is recorded in Fig. 6.22, while the average pixel deviation recorded by the MSE on the test data is 42.09. Furthermore, we visualize the predictions of the localization estimator to see sample deviations between the GT (orange square) and the predicted location (green square) in Fig. 6.23.

6.5.4 The Burnt Equipment Detection and Estimation Module

With knowledge of the equations (6.31, 6.32, 6.33, 6.35, 6.36), the inputs to this model can easily be calculated. However, because there is no available database of actual utility pole images (with reference heights H_R, H_R^p etc.) and the SL-PWR images are mostly sought from search engines, we make some realistic assumptions based on current utility practices in the United States in image labelling as follows.

In order to label the image data input, we assume that all pole heights are 12 m long as in the United States [†], the standard electric power utility pole is on average 12 m long and buried often

[†] The National Electrical Safety Code, published by the Institute of Electrical and Electronics Engineers (IEEE),

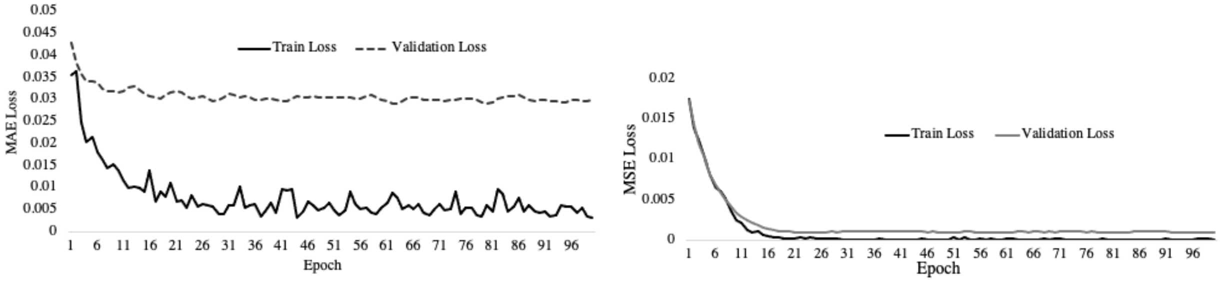


Figure 6.21: Performance of the wildfire spread estimator sub-module.

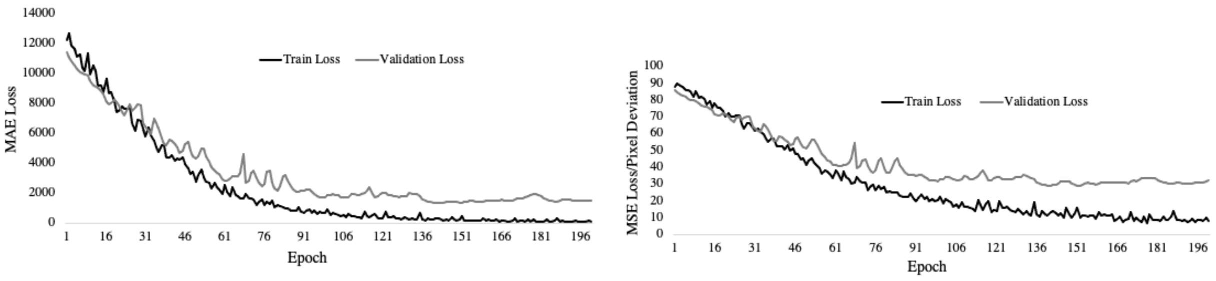


Figure 6.22: Performance of the wildfire localization estimator sub-module.

2 m in the ground. Hence, we use this information in this work in order to label the image data. We assume that the length of all poles is 12 m, however, for scenario 1 (bolted-on base), the 2 m pole-burying height is also considered.

$$L_{estimate} = \frac{n \times (12m/14m)}{h} \tag{6.43}$$

where $L_{estimate}$ is the length of the burnt off part of the pole, n is the length of the burnt off part of the pole in the image with respect to the ground, h is the height of the entire pole in the image with respect to the ground, and 14 m is used for estimating in scenario 1 (bolted-on base) as the the 2 m pole-burying height is also considered, as opposed to the scenario 3 (attached cross-arm

sets the standards for construction and maintenance of utility poles.

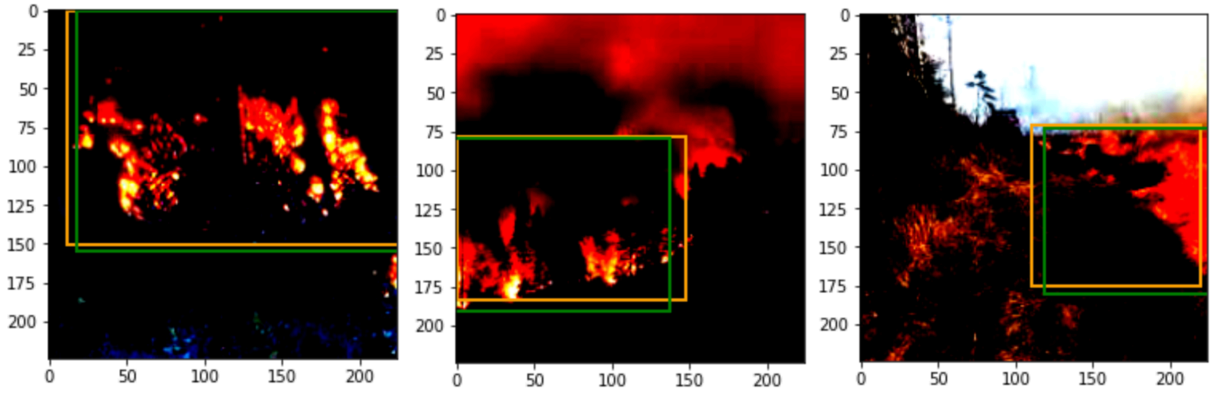


Figure 6.23: Visualizing the wildfire localization estimator output. The orange square is the ground truth while the green square is the localization estimator's prediction

extension). The angle of tilt/lean of the electric poles are also measured in the input image labeling as the images obtained from search engines do not have any standard position/height/angle of capture. While training the model, the risk of overfitting was quite high due to the dearth of training image data (burnt and leaning power poles with missing base and cross-arms). In order to reduce the overfitting, we integrate additional data augmentation including Image flipping, gray scaling on all 3 channels, and color jittering with brightness=0.2, contrast=0.2, saturation=0.2, hue=0.2. The Random Affine transformation is also used in order to preserve points, straight lines, and planes where parallel lines remain parallel after an affine transformation, hence aiding to correct for geometric distortions or deformations that occur with non-ideal camera angles. However, obtaining more image input for training the module will improve it's performance substantially.

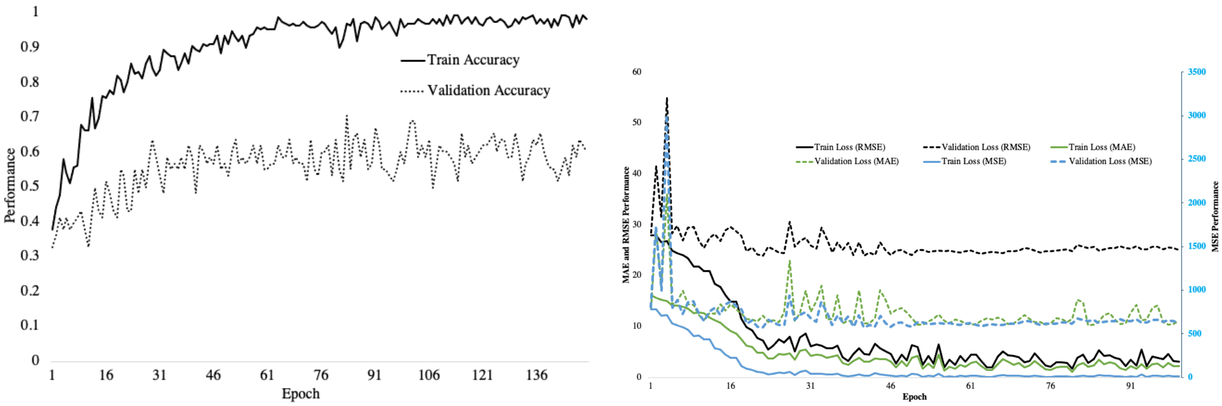


Figure 6.24: Accuracy and loss performance results of the burnt equipment module.

6.5.5 UAV optimization

A gridded area which consists of 16-grid cells superimposed on the standard IEEE 33-bus test system is used to test the UAV optimization process and monitoring trees in order to validate the effectiveness of the proposed method. The one-line diagram of the test system is shown in Fig. 6.25. The layer 1, layer 2, and layer 3 weights are chosen off a random distribution [0,1] for the different grids, Δt_i is assumed to be 1 $((t_i^1 - t_i^0) = (1 - 0))$ since the first optimization timestep is illustrated, while M is chosen to be 1. The same graph structure is used for the modified Dijkstra's

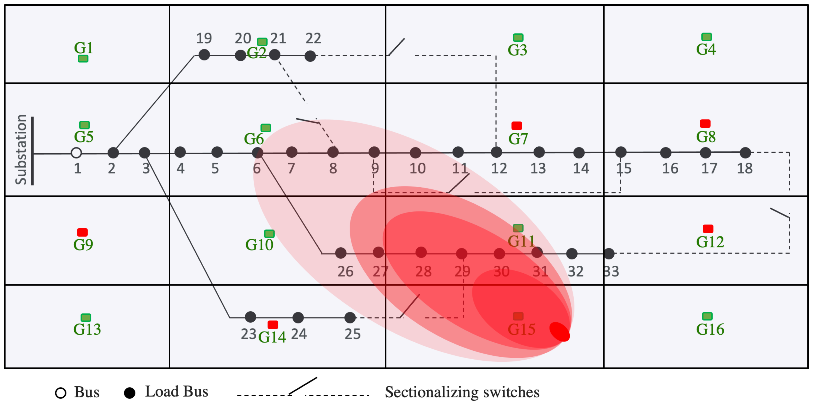
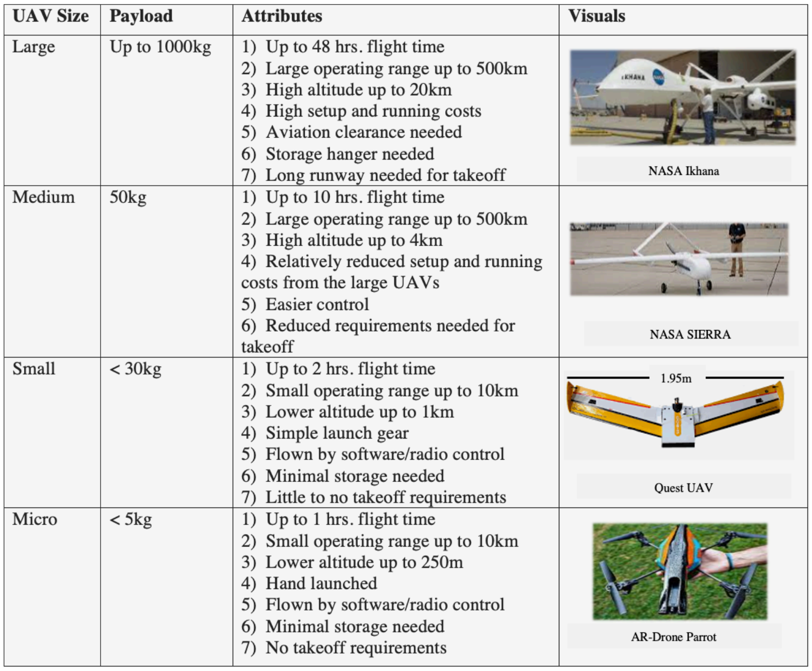


Figure 6.25: The UAV monitoring system of the SL-PWR spatially and temporally optimizes routing to high wildfire threat grids.

relaxation to get the UAV tree, and then the graph attributes are modified to inter-grid travel time, to select feasible UAV trips. For adjacent grids, the travel time is 1, while for diagonal grids, the travel time is 1.41. The trip feasibility based on the travel time of the paths which make up the trip, is informed by: 1.) Forecasted threat start time: that STWIP or any utility prediction technique indicates a wildfire threat. From this time, if that grid is exposed to an ignition source, a wildfire can be sustained. Hence, the UAV must arrive at the grid on/before this time. 2.) Monitoring time: that the wildfire threat in a grid is viable and hence the UAV must monitor this grid for this threat duration before routing to another destination if feasible in the same trip.

We consider two scenarios which inform the mission planning software as in Tables 6.4 and 6.5, a) The Lax case: where monitoring time is an estimate, e.g., extreme threat expected from noon to within 5-7pm when temperature, a wildfire contributing variable, goes down. b) The Strict case: where utility's confidence in the wildfire threat forecast model is high, and UAVs are routed strictly to that forecast. The difference being that in the strict case, the UAV must monitor till the end of the threat period while in the lax case, the UAV can leave the grid before estimated threat end time since, if a wildfire did not occur within about 90% of the threat duration, chances are that it would not occur in that grid. Hence, the UAV saves some time and routes to the next destination.

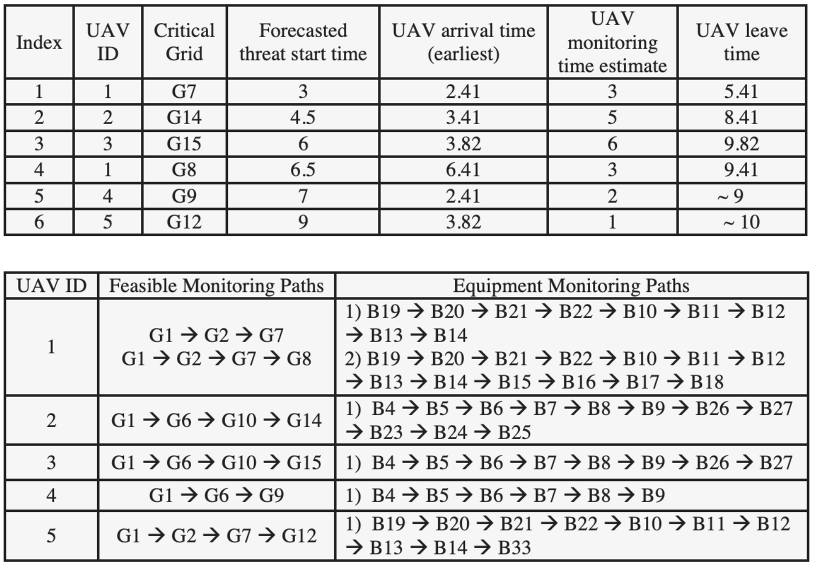
Table 6.3: Different UAV classes. These classes can be enhanced such that their attributes are improved e.g., medium class UAVs can be enhanced to a flight time of > 20 hours.



UAV Size	Payload	Attributes	Visuals
Large	Up to 1000kg	1) Up to 48 hrs. flight time 2) Large operating range up to 500km 3) High altitude up to 20km 4) High setup and running costs 5) Aviation clearance needed 6) Storage hanger needed 7) Long runway needed for takeoff	NASA Ikhana
Medium	50kg	1) Up to 10 hrs. flight time 2) Large operating range up to 500km 3) High altitude up to 4km 4) Relatively reduced setup and running costs from the large UAVs 5) Easier control 6) Reduced requirements needed for takeoff	NASA SIERRA
Small	< 30kg	1) Up to 2 hrs. flight time 2) Small operating range up to 10km 3) Lower altitude up to 1km 4) Simple launch gear 5) Flown by software/radio control 6) Minimal storage needed 7) Little to no takeoff requirements	1.95m Quest UAV
Micro	< 5kg	1) Up to 1 hrs. flight time 2) Small operating range up to 10km 3) Lower altitude up to 250m 4) Hand launched 5) Flown by software/radio control 6) Minimal storage needed 7) No takeoff requirements	AR-Drone Parrot

In these scenarios, we have chosen the high risk cells to be $[G7, G14, G15, G8, G9, G12]$ arranged in the order of the forecasted start times (T_s^I) of the wildfire risk, while the UAVs all route from the source grid $[G1]$. In Table 6.4, the first destination grid is G7 with T_s^{G7} = 3, the earliest time of UAV arrival is at T = 2.41 $< T_s^{G7}$ = 3, so that the UAV can positioned to monitor before the wildfire risk begins. After the UAV arrival, the time the UAV should remain in the grid for monitoring τ_1^{G7} = 3, which means this is the estimated duration of the wildfire threat. The UAV leaves G7 at T = 2.41 + 3 = 5.41 and checks the grid cells that are reachable from the current G7 given the T_s^I. G8 is the next feasible destination from G7 as by the time the UAV gets to G8, the time would be 5.41 + 1 (adjacent grids) = 6.41, and T_s^{G8} is 6.5, hence the UAV can make it in time to its second destination, the UAV then spends τ_1^{G8} = 3 and leaves G8 at 9.41. At that time, the

Table 6.4: The UAV Monitoring Tree. The Lax case is proposed such that the service area can be fully monitored where the SL-PWR UAVs are limited.



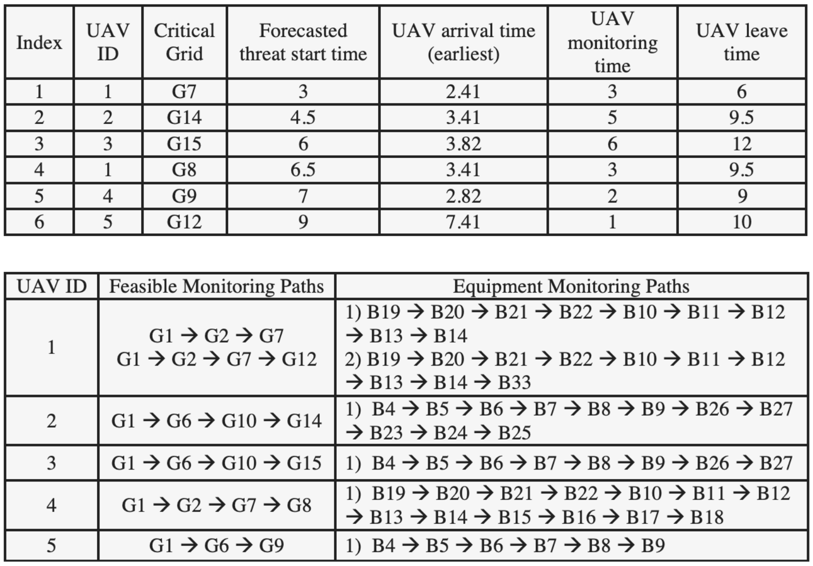
Index	UAV ID	Critical Grid	Forecasted threat start time	UAV arrival time (earliest)	UAV monitoring time estimate	UAV leave time
1	1	G7	3	2.41	3	5.41
2	2	G14	4.5	3.41	5	8.41
3	3	G15	6	3.82	6	9.82
4	1	G8	6.5	6.41	3	9.41
5	4	G9	7	2.41	2	~ 9
6	5	G12	9	3.82	1	~ 10

UAV ID	Feasible Monitoring Paths	Equipment Monitoring Paths
1	G1 → G2 → G7 G1 → G2 → G7 → G8	1) B19 → B20 → B21 → B22 → B10 → B11 → B12 → B13 → B14 2) B19 → B20 → B21 → B22 → B10 → B11 → B12 → B13 → B14 → B15 → B16 → B17 → B18
2	G1 → G6 → G10 → G14	1) B4 → B5 → B6 → B7 → B8 → B9 → B26 → B27 → B23 → B24 → B25
3	G1 → G6 → G10 → G15	1) B4 → B5 → B6 → B7 → B8 → B9 → B26 → B27
4	G1 → G6 → G9	1) B4 → B5 → B6 → B7 → B8 → B9
5	G1 → G2 → G7 → G12	1) B19 → B20 → B21 → B22 → B10 → B11 → B12 → B13 → B14 → B33

UAV cannot reach any other destination grids in its current trip, making UAV 1 have 2 paths in its trip.

Next, UAV 2 picks up from “G1 - G14" with earliest arrival time at 3.41 (1.41 + 1 + 1) it then

Table 6.5: The UAV Monitoring Tree. The Strict case is proposed where SL-PWR UAV supply is not limited and the UAV can monitor a grid for the predicted full threat period.



Index	UAV ID	Critical Grid	Forecasted threat start time	UAV arrival time (earliest)	UAV monitoring time	UAV leave time
1	1	G7	3	2.41	3	6
2	2	G14	4.5	3.41	5	9.5
3	3	G15	6	3.82	6	12
4	1	G8	6.5	3.41	3	9.5
5	4	G9	7	2.82	2	9
6	5	G12	9	7.41	1	10

UAV ID	Feasible Monitoring Paths	Equipment Monitoring Paths
1	G1 → G2 → G7 G1 → G2 → G7 → G12	1) B19 → B20 → B21 → B22 → B10 → B11 → B12 → B13 → B14 2) B19 → B20 → B21 → B22 → B10 → B11 → B12 → B13 → B14 → B33
2	G1 → G6 → G10 → G14	1) B4 → B5 → B6 → B7 → B8 → B9 → B26 → B27 → B23 → B24 → B25
3	G1 → G6 → G10 → G15	1) B4 → B5 → B6 → B7 → B8 → B9 → B26 → B27
4	G1 → G2 → G7 → G8	1) B19 → B20 → B21 → B22 → B10 → B11 → B12 → B13 → B14 → B15 → B16 → B17 → B18
5	G1 → G6 → G9	1) B4 → B5 → B6 → B7 → B8 → B9

spends τ_2^{G14} = 5 and leaves “G14" at 8.41 by which time it cannot make it to any other grids before their T_s^I. Another interesting trip to look at will be the trip to G9, the earliest arrival time would be 2.41, however, the start time of the wildfire risk is T_s^{G9} = 7, hence, the UAV operator has to start out the UAV on the route on/before T = 4.59 and the leave time should be approximately T = 9. Same applies to “G12". In Table 6.5, the illustration is that the model confidence can change the route to the UAVs. For instance, if the forecasting model for T_s^I and τ_j^I is closer to 100%, then the UAV strictly follows these times and will only leave a grid cell at T = T_s^I + τ_j^I. In this case, the UAV 1 routes from G7 to G12, instead of G7 to G8 as in the previous case, and this would be the best case if there are more UAV supplies that trip time conservation can be overlooked. Runtime for the UAV optimization code is 0.0182 secs.

Furthermore, the UAV optimization also considers the weather in the grids that UAV takes on its trip. One way to include the weather would be to not go through the routes with high wind gusts but in this method, there may be only one efficient route considering the forecast start time, hence the optimal way would be to schedule medium or large UAVs for the trips with high wind gust grids during the times the UAV is flying through. On the same hand, the total trip time would also influence the UAV type (large, medium or small as shown in Table6.3) which will be scheduled on a trip. This parameter can be easily be manually selected by the operator during trip planning given the available UAV types. If the trip is long, e.g., 10 hour-trip, a medium UAV can be scheduled for monitoring since these UAVs can get up to 20 hours of round-trip time. Table 6.3 shows the minimum attributes, as these UAVs can still be improved, for instance, medium UAVs like the Penguin B has an optional 7.5 L capacity fuel tank, and in addition, an 80W on-board generator system to improve on its flight time from 6 hours to above 20 hours, and does not need a runway as it can take off from a car-top launcher and could be recovered by a large parachute if the need arises.

Therefore, these UAV types can also be used as the initial firefighting efforts. Once a fire is detected, the UAV operator gets an alarm, and depending on the UAV type (and hence payload capacity for carrying firefighting fluids) nearest to the burning grid cell, the operator can use the ground station software to circumvent the early-detected-fire with firefighting fluids, hence bounding the wildfire while routing more firefighting resources to the burning grid cell. The advantage of this method is that the utility does not have to route a ground fire fighting crew as the first response since road networks are longer and traffic could be a delaying factor e.g., the PG&E 10 hour response delay to Dixie Fire. On the same hand, the fluid-carrying UAVs can easily be re-routed to aid contain the fire pending the arrival of the ground crew in order to give the firefighting crew headstart.

6.6 Conclusion

This chapter proposes a self-sufficient low-cost wildfire mitigation (SL-PWR) model that is resilience-oriented in its approach to spatio-temporally predict wildfire threat, detect and localize wildfire occurrence, spread, and other wildfire-related incidents e.g., power equipment as ignition sources. The SL-PWR model is self-sufficient as it's comprehensive nature informs power system resilience at each stage of the resilience trapezoid. The SL-PWR's vegetation module improves vegetation management in the pre-wildfire phase, the power equipment module aids in mitigating endogenous wildfires, the wildfire module aids containment of already progressing wildfires, and the burnt equipment module sees to the restoration of the power grid after wildfire damages. In order to enable these functionalities, the SL-PWR uses already-owned utility UAV resources to obtain input data used in training the SL-PWR modules to comprehensively inform power system resilience against wildfires using spatio-temporally optimized UAV monitoring trees, hence, achieving transparency. Results show effective performance of the SL-PWR in improving power system-wildfire resilience, hence reducing risk. The optimization model developed in SL-PWR for the UAV resources using predicted wildfire threat parameters from STWIP wildfire potential map outputs improves situational awareness with limited availability of UAV resources. This improves resilience by reducing response time, extremely important in wildfire mitigation. Additionally, with this optimization, more monitoring trips can be completed within threat time, encouraging wildfire risk integration with power system operation. Most importantly, the proposed SL-PWR model will aid to save lives of utility crew, avoiding disastrous events such as the 2020 fire siege regrettably cost the lives of pilot, Michael Fornier, fire captain, Diana Jones, and firefighter Charles Morton.

7. ECONOMIC ANALYSIS AND RETURN ON INVESTMENT: A SELF-SUFFICIENT LOW-COST MITIGATION MODEL TO IMPROVE RESILIENCE IN POWER UTILITY WILDFIRE RESPONSE

7.1 Introduction

This chapter presents the economic incentive for adopting the SL-PWR model as opposed to the current utility wildfire mitigation practices. The chapter provides a detailed budget analysis, of the SL-PWR vs. conventional utility methods, which integrates the dollar cost of technologies. Herein, we further expand on discussions and recommendations on the use of the proposed SL-PWR model towards visualizing the return on investment (ROI).

The rest of this chapter is dedicated to the investment potential aspect of SL-PWR for power utilities. The chapter provides a detailed Cost Benefit Analysis showing the return on investment of the SL-PWR model relative to the conventional utility wildfire mitigation techniques. Discussions and recommendation comes in Section 7.3 including state-of-the-art wildfire designs that can as well complement the SL-PWR model, if desired by the utilities. Furthermore, the chapter discusses the benefits of employing the SL-PWR model as compared to similar models currently offered by existing wildfire mitigation companies to power utilities.

7.2 Cost Benefit Analysis for the SL-PWR

Conventionally, power utilities detect wildfires by obtaining reports from:

1. The general public: Many wildfires are detected and reported by the general public who provide information including fire location, lives and property at risk, fire size, vegetation type e.g., is the fire burning trees, spreading rate and the color of the smoke.

2. Air patrols: Air patrols consist of a pilot and trained aerial observers who fly predetermined routes over remote areas during periods of high wildfire risk.

3. Infrared technology: This is used by ground personnel and aircraft with thermal imaging

technology to assist in fire operations.

4. Computer technology: This is used to obtain current weather, predict the probability and location of wildfires, predict rate of spread and moisture content of fuels.

5. Lookout observers: These are observers situated in strategic lookout stations with extensive visibility whose primary purpose is to spot and report wildfires early as well as continued observation of the fire behavior pending the arrival of fire fighting crew.

These methods are insightful, however, are not cost efficient leading to unrecoverable expenses as illustrated in Fig.1.7. Additionally, these methods are not efficient when it comes to saving time, which is critical during wildfire occurrence and spread. In fact, with these reporting methods, it could take longer hours before wildfires are reported and hence even a longer time to respond to the wildfires, this makes the wildfires even more intransigent and difficult to subdue. For instance, it took PG&E more than 10 hours to get to the location of the Dixie fire after ignition. Conventional utility methods, such as monitoring crew on helicopters need to go through safety checks and take off only once clearance is granted, and hence are less advantageous. Moreover, these conventional methods of manned-monitoring for wildfires [199] puts the monitoring crew at risk (e.g., crashing manned-aircraft due to high temperatures or smoke fog, or even trapped lookout observers), exposing the utility to even more liability. For instance, the 2020 fire siege regrettably cost the lives of pilot, Michael Fornier, fire captain, Diana Jones, and firefighter Charles Morton, in memoriam [139], among many others. With the UAV-enabled SL-PWR, these liabilities are avoided to a highly tangible extent. In fact, most kinds of UAVs can be taken to the site, easily assembled, launched, and within minutes the UAV can be airborne taking aerial photographs, reaching humanly inaccessible areas or areas that pose a high risk to humans if accessed. The SL-PWR affords the utility more benefits including optimized routing paths which can be socially and economically quantified e.g., faster wildfire is detected, the less likely it is to cause loss of lives and properties and hence improves the customers faith in their service area utility efforts. If these are comprehensively integrated in the cost benefit analysis, will also improve the ROI of the SL-PWR considerably. However, our goal in this chapter is to highlight the trajectory of improvement that can be harnessed by investing in the SL-PWR technology and how rapidly the utility will begin to recoup on their investment.

Hence, in this section, we do a cost-benefit analysis on the SL-PWR model vs. the conventional utility methods in order to estimate the ROI that these models afford the power utility. Here, we try to limit the dollar price on the benefits associated with the SL-PWR model to mitigate bias e.g., addressing power system resilience on all 4 phases of the trapezoid is allocated a meagre cost of \$1000/phase in the entire year, while allocating up to \$6 million/month for the costs of unforeseen contingencies in the first year of setting up the SL-PWR model. The following details were used in this analysis.

7.2.1 Conventional Utility Methods

For this case, the benefits include: system resilience, which with this conventional method, is active in 2 phases of the resilience trapezoid, namely, the pre-wildfire phase during wildfire monitoring and in the disruptive phase during firefighting using firefighting helicopters. The benefits also include: the improvement of situational awareness using manned-aircraft, the time saved by detection using lookout stations, monitoring aircrafts, and random observers, social welfare and community relations, life and property saved by detection, and bankruptcy avoidance. Similarly, the costs included one-time costs of purchasing utility helicopters, aircraft and pilot commissioning, and recurring costs of flight cost per hour, contractor-manned aircraft, flight planning, helicopter pilot salary, insurance, cost of false reports, firefighting crew costs, helicopter storage and maintenance. Helicopter insurance cost consists of 2 separate coverages, the Liability coverage (up to \$4000) which covers Bodily Injury, Property Damage and provides Legal Defense, and Hull Coverage (up to 10% of helicopter cost) which covers covers damage to the helicopter itself. The helicopter is assumed to be powered by a turbine engine with fuel consumption of 180 gallons/h at \$6/gallon. Here, we take the detection time of wildfires for the conventional power utility to be 5 hours which is the time it takes for the satellite imagery to become available during active fires e.g., NASA's Fire Information for Resource Management System (FIRMS), which uses MODIS and VIIRS data to provide updates on active fires throughout the world, including a rough location of a detected hotspot [200]. The detection time could be up to or more than 10-to-24 hours or more depending on the technique employed e.g., random observer reports from phone calls may occur > 10 hours after fire ignition.

7.2.2 SL-PWR model

The benefits of the SL-PWR model include: improving system resilience at every phase of the trapezoid as illustrated in Fig.6.1, sequential monitoring of vegetation, vegetation clearance, and equipment, early detection, improving community relations, detection of equipment failure type, database acquisition from captured images, mitigating traffic delays in routing monitoring crews, situational awareness enhanced by spatio-temporal imaging and resource optimization. On the other hand, the costs include one-time costs of UAV purchases, cost of photographic equipment and ground station software. Ongoing costs then consisted of UAV image processing, insurance, firefighting crew, computation & storage cost of images, UAV flight cost/hour, alternative fuel, UAV storage, UAV labor/operation, UAV maintenance and miscellaneous costs.

For UAVs, the Hull coverage generally costs 8-12% of the hull value. The approximate image processing costs for SL-PWR will include license costs = (license cost for RAM per GB per hour) + (license cost for vCPU per hour) + (license cost for GPU per hour). For instance, for a 64 GB RAM, 16 vCPUs, 4 GPUs: License cost/Virtual Machine (Monthly) = [(0.000127 * 64) + (0.018063) + (0.120)] * 24hrs * 31 days, while local storage costs a monthly rate of 8 cents/GB. The fuel consumption of the UAV depends on different factors such as wind speed and direction, the UAV speed, the UAV weight and payload, air density, temperature, etc. For the cost analysis, this is assumed to be at an average value of 672.2kg/h [201], and at $5/kg [202] for the large UAVs, with an average operator rate of $23/h [202]. Additionally, the Li-Po battery pack is considered as alternative fuel for the UAVs for either stand-alone use or hybrid, at $2600 per unit of 200 h lifetime [202]. We assume an average of 1200 wildfire threat monitoring hours per year. The UAV maintenance costs are the costs associated with the repair of any failed units or parts of the UAvs and calculated at 5-10% of the UAV initial cost [203].

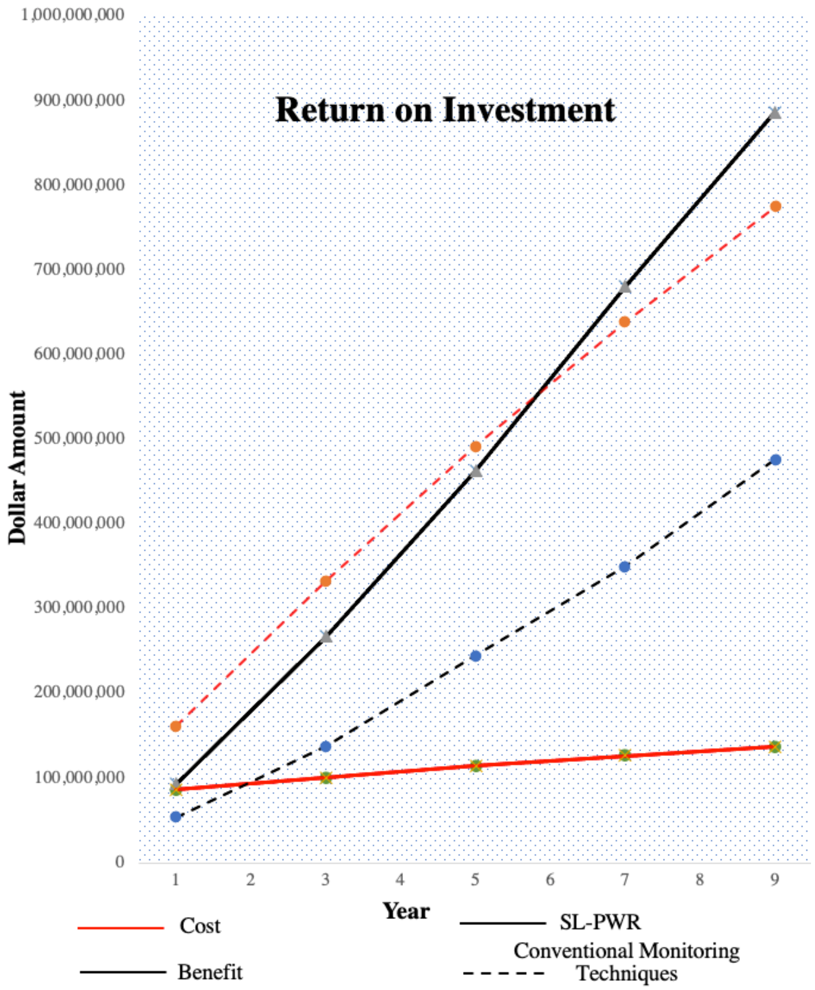


Figure 7.1: Return on Investment (ROI) over a period of 5 years for SL-PWR model and the conventional utility techniques.

In this analysis, we assume that the average wildfire response in a year is 16, inspired by the number of endogenous wildfires linked to PG&E electric power utility in 2021 [204]. Additionally, we calculate the benefits of lives and property saved based on a maximum of 6 lives and 400 properties based on 2019 Kincade fire, as well as, Sonoma County's district attorney charge of PG&E with five felonies and 28 misdemeanors [205]. In the calculation, we extrapolate the firefighting crew count per fire from the type of firefighters in each crew that respond to wildfires [206]. These are the 1.) 20-person Handcrews team who mop up or control the wildfires by constructing surrounding firelines, 2.) 10-person Hotshots team of highly skilled personnel fighting the toughest parts of the wildfires, 3.) 10-person Engine crew that carry fire fighting fluids 4.) 5-person Smokejumper team that parachute from airplanes to quickly contain the wildfires, 5.) 2-5 person Helitack crew that are transported on helicopters to fight nearby fires. Typically, utilities employ the services of certified arborists to provide some level of supervision to the professional tree-trimming crew who are contracted for vegetation management projects which could be within intervals of 4-5 years, or less for vegetation that is fast growing [195]. Hence, we assume that one person is a paid arborists. With early detection afforded by the SL-PWR model, less Firefighters are required and hence the analysis considers 10-person-less team of firefighters in the SL-PWR model. We also assume that it takes an average of 6 hours to put out detected wildfires [207].

The results as illustrated in Fig.7.1, considering an inflation rate of 7.9% (as in the year 2022), indicate that the conventional models have the costs of fire-fighting heavily superseding the benefits and hence causing a negative return on investment for the power utilities leading to bankruptcy and liabilities which cannot be recouped in any foreseeable future. However, even with undervaluing the benefits of the SL-PWR and addition of unforeseen contingency set-up costs of $6 million/month for the first year and $1 million/month for subsequent years, the SL-PWR is able to recoup its costs within it's first year.

7.3 Discussions and Recommendations

Here, we discuss different technologies, some in the pioneer stages that electric power utilities have starte adopting for wildfire detection. We recommend ways in which these technologies can be integrated with the SL-PWR model to further drive accuracy in wildfire detection and hence improve the resilience-enhancing-capacity of the SL-PWR model.

7.3.1 Integrating state-of-the-art designs with SL-PWR

Utilities have begun adopting pioneer technologies towards wildfire response and mitigation [208]. Among these technologies, the Unmanned Aerial Systems which have been begun to be integrated to wildfire inspections programs from 2019 in PG&E. This makes the SL-PWR even lower cost in terms of cost of UAV purchase and training the UAV operator since the base technology is already integrated to some level in power utilities operations either for wildfire monitoring or transmission infrastructure inspection. Other designs that could be integrated into the SL-PWR design for wildfire mitigation are discussed as follows.

1. While travelling on their optimized monitoring routes, the SL-PWR UAVs can be fitted with fire extinguishing agent like dry powder. A medium drone with a maximum load of 15 kg payload capacity and maximum flight time of 45 minutes, can carry fire extinguishers and other rescue equipment including ip65 protection. This way when a fire is detected, the SL-PWR powered UAVs can serve as first responders and be utilized to extinguish or contain the fire ignition to avoid spread until the firefighting crew arrive. This can as well supply protective equipment, e.g., masks to protect the crew or people affected by wildfires against pollutants, rather than wait for the utility/fire crew to route resources to the affected areas.

2. Furthermore, PG&E has also adopted the Distribution Fault Anticipation tool (DFA). The DFA consists of a system of hardware and software that detect circuit anomalies and notify the utility operators before these anomalies spark fires. Accordingly, these anomalous conditions can build up over weeks and can impact minute details in the electric currents before actual failure, hence the DFA applies algorithms to detect and report these anomalies [208]. In the SL-PWR model, the DFA tool can be integrated into the calculation of PE_i in the UAV optimization objective function as in (6.37) which factors in the power equipment layer in the routing of the UAVs for power equipment monitoring. Hence, as illustrated in Fig. 6.1, the DFA technology can aid the SL-PWR model to narrow down the equipment monitoring in the wildfire progression phase of the wildfire resilience trapezoid.

3. Additionally, increased emphasis has been placed on wildfire detection leading to several competitions including the United States Environmental Protection Agency's "Wildland Fire Sensors Challenge" whose winner developed air quality monitoring system prototype to improve smoke monitoring towards protecting public health from smoke generated during wildfires. On the same hand, SCITI labs' wildfire sensor research focuses on real-time and

continuous detection of heat and smoke in order to locate and track fire perimeters including the fire characteristics. These sensors are placed in several locations in the service area e.g., within several feet radius of one another. If already adopted by power utilities, these sensors can also improve geographically targeted warnings. The sensors can be integrated into the SL-PWR model to further enhance monitoring and improve the wildfire spread rate calculation as detailed in Section 6.3.3.2, where the distance from on sensor to another and the time between the sensor alarms can also be used to improve spread rate estimation.

7.3.2 SL-PWR-Improved Power Grid Resilience

As illustrated in Fig. 6.1, the SL-PWR model aids to improve the wildfire resilience of the power system comprehensively, which means that the system resilience is improved on all phases of the wildfire resilience trapezoid.

1. In the pre-wildfire/"wildfire analysis" phase of the resilience trapezoid, the vegetation management afforded by the vegetation module of the SL-PWR aids to sustain system performance until such a time that the wildfire threat occurs. Wildfire threat leads to precautionary/preventive measures such as adjusting protective equipment settings. Currently, utilities employ public safety power shutoff (PSPS) as a response to wildfire threats. With the SL-PWR, the utilities can be more confident in supplying power until there is wildfire ignition.

2. The SL-PWR's equipment failure module then kicks in during the "wildfire progression" phase, which begins with when there is threat of wildfire to actual ignition and spread. This module monitors for ignition sources from power equipment using the optimization parameters discussed prior. Conventionally, utilities will de-energize huge zones of their service areas in or surrounding high fire risk zones given the threat of a wildfire occurring [184]. With the STWIP-produced wildfire maps and other maps as illustrated in Fig. 6.11, the spatio-temporal granularity of the SL-PWR is improved and then routing the UAVs optimally to monitor the grids with high wildfire potential. By so doing, it tangibly reduces the risk i.e., the dip (section 1 of the trapezoid in Fig. 6.1) after the wildfire threat, because instead of

the utility de-energizing large portions of the grid in anticipation of a wildfire i.e., PSPS, the utility can keep supplying power cautiously until actual ignition is detected.

3. If a wildfire occurs, still in the "wildfire progression phase", the system performance is further diminished and can get to the minimal functionality as the wildfire gets contained. The SL-PWR monitoring, optimized using the potential wildfire ignition maps of the service area, detects and localizes the fires while stationed at the high threat grids. The UAV-powered SL-PWR can hence aid rapid wildfire containment as it can carry initial firefighting efforts (e.g., firefighting fluids) when the fire has just been detected (i.e., early detection = minimal spread). Given that the SL-PWR can also localize the wildfire, the UAVs can be used to apply the firefighting fluids at the bounding boxes (fire boundary) detected by the SL-PWR. Hence, aiding contain the fire pending the arrival of bigger firefighting UAVs or the firefighting crew.

4. After containment, "the restoration phase" of the system resilience sets in. The burnt equipment detection and estimation module aids to minimize the time taken to restore the system hence providing a desirable steeper positive restoration slope i.e., rapidity in restoration. This is aided by the ability of the SL-PWR to automate the conventionally manual repair crew inspection and estimate the required repair type and amount of material needed for the repair e.g., length of cross-arm extension to be replaced as shown in Fig. 6.9

7.4 Solutions to Power System Problems Provided by the SL-PWR

Wildfires have become a huge threat to not only power utilities and communities but to the country's economy at large. Hence, a comprehensive model like the SL-PWR is essential to aid in wildfire mitigation. The SL-PWR, a self-sufficient and low-cost model, further provides unmet needs such as:

1. Rapid, granular, and spatio-temporal wildfire detection, within the timeline of milliseconds (Very Early Detection) that can be integrated into power systems operations.

2. The SL-PWR mitigates both endogenous (caused by power equipment) and exogenous (caused by natural and human sources other than power equipment) wildfires. Other existing tools

tackle either endogenous (e.g., FIREBird) or exogenous (e.g., the smoke detectors) but not both simultaneously, and not comprehensively like the SL-PWR.

3. In addition to wildfire detection, the SL-PWR performs wildfire localization. This means that the SL-PWR is able to "box in" and report where exactly a wildfire is (latitude, longitude, height and width of wildfire location), and can also report in real-time the wildfire spread, and rate of spread.

4. The SL-PWR's early detection and localization ability means that it can also act as the first point of firefighting, where medium/larger UAVs can carry firefighting fluids on their optimized routes. This SL-PWR ability to serve as first responders prevents issues like the situation during the Dixie fire which took the PG&E the firefighting crew more than 10 hours to get to the fire location, hence leading to a wildfire that had spread more than can be relatively easily controlled.

5. Enabling the concept of the Digital Twin: The SL-PWR tool enables the concept of digital twins in asset management where the tool provides itself as a resource that enables the critical infrastructure to mirror itself in normal operation using real and accurate data towards aiding recovery back to functional system state after a high impact event.

6. The SL-PWR operates in a spatio-temporal technique which works in a gridded and granular manner that is effective for the topology of the bulk power grid. Hence, the spatio-temporally granular modeling that the SL-PWR provides is efficient for power utilities in wildfire mitigation, unlike other existing solutions.

7. To the best of our knowledge, ALL existing wildfire mitigation solutions are used for wildfire detection ONLY and no comprehensive solution has been proposed that caters to utility needs such as automatic vegetation management. The SL-PWR aids in other wildfire mitigation-related processes like vegetation management, power equipment monitoring/maintenance, and equipment restoration post-wildfire,in an “All-In-One” technique that prevents both en-

dogenous and exogenous wildfires using already-owned utility UAV resources.

8. In this multi-tasking and efficient way, the SL-PWR further provides the "Low-Cost" since it can be employed in improving multiple fundamental power utility processes with utility-owned resources which will not require further cost of installation or training of operating personnel. Hence, the SL-PWR provides a comprehensive culminating solution for utility wildfire needs, making investment in the technology extremely economically rewarding as well.

9. The SL-PWR provides automation in the detection and localization of small, undersurface, and large wildfires, vegetation management, and equipment monitoring/restorations. It, hence, eliminates the need for full-time monitoring personnel as well as minimizes manned operations.

10. The Self- Sufficient SL-PWR model which can be employed wholly on its own as it does not need supporting application that would require any integration pipeline.

11. The SL-PWR comprehensively integrates and enhances resilience in power utility wildfire response. The SL-PWR achieves this by improving the power utility wildfire response at the different resilience phases which the power system lies during wildfire threats and events.

12. Provides transparency (via dynamically captured images) in power utility analysis which otherwise would not be a provision of conventional utility techniques e.g., foot inspection crew, monitoring and repair crew.

13. The SL-PWR can detect wildfires dynamically at any location in the service area, unlike other tools like the FIREBird, air sensors, FireALERT MK I by Vigilys, etc. discussed in Section7.4.2, that are statically installed and relatively have extremely limited coverage in service areas which span large expanses of wildland. This means that, with other tools, utilities are burdened with solving the problem of environmental pollution from installing a lot of these tools in a service area, and as well the problem of optimal installation locations

which then limits situational awareness in the service area and negatively affects system resilience. E.g., the FIREBird tool can only be installed in locations where there are electric poles, and only functions to detect wildfires that start at road boundaries (i.e., along right-of-way easements) in their immediate installation location with limited line of sight range.

14. The SL-PWR enables transparency in it's functionalities by providing visual situational awareness via the UAV captured input images sent to the system operator at the power utility base station.

7.4.1 Unique Features of the SL-PWR that enable these Solutions

1. The SL-PWR which functions for comprehensive resilient detection, classification, estimation, and localization of wildfires, wildfire related events, and utility processes, consists of 4 major modules including 1.) the vegetation module, 2.) the power equipment module, 3.) the wildfire module, and 4.) the burnt equipment module, which are active in all the wildfire resilience phases of the power system.

2. The input of the SL-PWR integrates efficient spatio-temporal wildfire potential maps to generate the optimal monitoring routes for the SL-PWR UAVs. This map, an output of the STWIP model, was validated with up to 93% accuracy and it's predictions were tested over the 2018 wildfire year. The predicted results of the STWIP model were compared with the actual wildfire occurrence in that year and results, as in Fig.5.7, show that predicted hotspots are similar to the actual historical test year and the wildfire hotspots were clustered between the same latitudes and longitudes, verifying the accuracy of the predicted maps. No other wildfire detection tools employ this crucial step in optimizing the wildfire detection.

3. The SL-PWR model performs analysis in real time with computation time that can be easily integrated into power system operations under wildfire threats. Existing wildfire detection solutions such as the FIREBird tool detects wildfires in 2 mins, while the FireALERT MK I tool by Vigilys functions with 4 mins detection time. The SL-PWR detects a wildfire in less than 40 msecs after the UAV captures the wildfire image. This is the most time the

SL-PWR takes to detect a wildfire since it's UAV resources are optimally routed to situate in the extreme wildfire threat grids as enabled by the STWIP wildfire input map.

4. The SL-PWR, as opposed to the other solutions, has the ability to differentiate between fire ignition source (power equipment fire/arcing) and actual wildfire ignition. This information is highly crucial for the utility to route the appropriate crew e.g., power equipment repair crew vs. firefighting crew. The results of this module were validated and tested with real-data and the performance was outstanding with: The wildfire fire and smoke detector achieving more than 90% accuracy with real test data, the spread estimator attaining minimization of estimation losses over epochs with 0.01166 average test data MSE, while the localization performs well with average pixel deviation recorded by the MSE on the test data as 42.09.

5. The proposed SL-PWR model also aids in transparent inventorying during post-wildfire restoration with its "Burnt Equipment Detection and Estimation Module". For instance, instead of contracting manual road crews to take inventory of damaged equipment which the system operator will be blind to, the SL-PWR can aid transparency, helping stakeholders to visualize and estimate damage cost, while improving rapidity and automating the restoration process.

7.4.2 Comparing the Functionalities of the SL-PWR to Similar Existing Models

7.4.2.1 Monitoring and Detection Tools such as The FIREBird and The FireALERT MK I.

The FireALERT MK I by Vigilys is a self-contained, early warning, wildfire detection sensor system that detects, analyses and wirelessly communicates the occurrence and position of a fire in real time [209]. It is a wildfire detection device that should be installed in every square mile in order to detect a fire signature. Its horizontal sensing rotates 360 degrees in about 4 minutes. However, these imply that:

- It takes even more time to begin to differentiate the fire signatures and since it cannot detect wildfires unless the fire is within a mile,

- The device itself risks being engulfed by the wildfire before detection can be made as wildfires can spread over miles in those 4 minutes of detection.
- This solution is additionally limited in the same ways as the other installed solutions such as the FIREBird wildfire detection tool detailed as follows.

The FIREBird wildfire detection tool is deployed along high fire risk rights-of-way, such as utility power lines, or wildland urban interface boundaries, and can support continuous wildfire detection along these high fire risk boundaries when installed at regular intervals [210]. The FIREBird is capable of detecting wildfires as small as 5×5 feet as far away as 900 feet [210]. However, compared to the SL-PWR, the FIREBird is limited in the following ways:

- The FIREBird performs a sub-function (wildfire detection) of one of the four modules of the SL-PWR. The wildfire module of the SL-PWR has 2 sub-modules which perform “wildfire and smoke” detection and “localizes and estimates” the spread of the wildfire.
- The FIREBird is stationary, installed on utility electric poles, hence can have a limited view of the area, only as vertically allowed by the height of the utility pole. However, the SL-PWR is dynamic, flying above ground with a great span of sight for the service area being monitored. The SL-PWR functionalities, during calculations, also take into account the zooming of the captured images in the case of small wildfires.
- The line of sight of the FIREBird cannot be blocked. Otherwise, it assumes that the tool will be mounted on a pole taller than the vegetation of the area or that the land is flat.
- This limited view means that the wildfire has to get closer to the device in order to be detected. With the high rate of spread of wildfires, the device can risk getting burnt during detection, which typically 2 minutes for this device. The SL-PWR can fly at any feasible height above ground and capture the wildfire event without risk of burning with a detection time of approximately 40 milliseconds, compared to the other solutions, SL-PWR provides much important time efficiency “Very Early Detection”.

- The cost of a basic FIREBird monitoring is [($60k/device + cost of installation) × number of devices needed to continuously monitor the service area]. With the device risk of getting burnt during detection, the cost to the utility after every wildfire event will include frequent replacement + re-installation costs. This can run into billions in recurring costs/year. This recurring annual cost is averted in the dynamic SL-PWR.

- This proximity of the wildfire to the device also implies that the wildfire will most likely burn the device(s) before the first responders arrive. This is averted in SL-PWR since the optimized SL-PWR can serve as the first response in a wildfire ignition where UAVs that carry firefighting fluids can be used to contain a fire.

- The FIRBird considers only one phase of system resilience "Wildfire Progression" during wildfire i.e., The FIREBird dooes not function "Pre-Wildfire" or "Post-Wildfire" like the SL-PWR, not sustainable (one has to be mounted on every line in the service area $60k/unit, and with the variability in weather and climate, wildfire threat areas are highly likely to change more frequently.

- The FIREBird will not detect wildfires unless they come closer to the road boundary where the evices are installed on the power lines. Hence for exogenous fires that are not started by power lines, the FIREBird is not effective. Also, by the time an exogenous fire gets to a road, it is highly spread in the wildland leading to increased firefighting time. The SL-PWR is designed both for endogenous and exogenous wildfires.

- The FIREBird requires personnel to move out and replace batteries every about twice or thrice a week [210], hence with one installed for every mile, this becomes burdensome and costly to undertake. Also, this means that personnel have to be out in the field replacing batteries during high wildfire threat days, and this defeats the unmanned process. With the cost-efficient and truly unmanned SL-PWR, the optimized routing of its UAVs considers fueling automatically in such a way that monitoring during high wildfire risk is not disrupted and personnel do not have to go into the field to retrieve the SL-PWR as it is optimized to route back to refuel.

7.4.2.2 Sensory Tools such as Air Quality Sensors, Fire and Smoke Detection Tools.

There are many wildfire solutions centered on fire/smoke detectors that monitor air quality. These solutions are commendable however, with perceived limitations since:

1. The cost of installation which also includes the cost of optimizing the locations of installation is high.

2. These solutions have limited sensory range and hence have to be installed all over the service area. In other words, the tools are statically installed and hence can only detect in their immediate surroundings.

3. In order to efficiently cover the service area, installing these devices could not only be uneconomical and tasking, but create an environmental pollution crises in the area.

4. Most detection solutions follow the wildfire thermal detection signature with functionalities same as sample cases discussed below.

7.4.2.3 Conventional Solutions used by Power Utilities

Conventional solutions used by utilities also include: Satellite Images, Utility Inspection Helicopters, and Lookout Observers.

7.4.2.3.1 Satellite Data: Satellite image data can also be employed e.g., satellites orbiting at lower (500–2000 km) altitudes can detect wildfires in the early phases due to their finer resolution, however:

1. Some satellites can take several hours to return to the same view. For example, VIIRS has a 12-hour revisit time while the Landsat-8 has a 16 day revisit time hence it is rare that one of these satellites provides the first wildfire alerts.

2. Additional limitations could arise including that the detected heat signatures are averaged over pixels, making it difficult to pinpoint fire location and size.

3. Wildfire intensity is indicated by thermal signals which can be smoldered by smoke and hence radiate relatively less energy, causing data misinterpretation.

The SL-PWR improves upon this satellite method since:

1. The SL-PWR UAVs provide more continuous monitoring than satellites which periodically visit specific parts of earth.

2. Unlike satellites, the SL-PWR system would rarely be blinded by local weather conditions or smoke/dust of wildfires because of its height of flight and choice of camera (e.g.,enhanced-vision cameras).

3. Unlike the SL-PWR, the Satellite imagery e.g., from Google Earth can only support so much detail in the image resolution before images begin to appear blurred or pixelated.

Although with improvements in the continuity of modern satellites, satellite imagery can be processed by the SL-PWR as well, providing the same real-time information to appropriate response teams.

7.4.2.3.2 Manned Helicopters and Airplanes: Manned helicopters can also be used as conventionally done by power utilities, low-flying airplanes can capture comparable imagery to UAVs, but are expensive to hire continuously especially for the range of services that the SL-PWR provides. Additionally, with this method, flying at low altitudes increases the possibility of a crash, thus employing the SL-PWR technology lowers costs and improves operator safety for such missions. Hence the SL-PWR avoid these additional limitations posed by conventional utility methods:

1. At lower altitudes (up to 215m) SL-PWR can capture 5cm resolution imagery, which is much higher than imagery captured from satellites, 25cm resolution.

2. It captures images hence, heat signatures cannot be smothered and cause misinterpretation of data.

3. Most of the SL-PWR UAVs do not need runways, takeoff can be from car-top launcher and recovery with parachute, if needed.

4. The SL-PWR UAVs are unmanned hence reducing the liability of the power utility for loss of lives of the crew.

7.4.2.3.3 Lookout Observers: These are observers situated in strategic lookout stations with extensive visibility whose primary purpose is to spot and report wildfires early as well as continued observation of the fire behavior pending the arrival of fire fighting crew. The SL-PWR totally avoids the need for a monitoring person as all monitoring is automated by the UAV system and can be manually controlled by the operator from a safe office space, hence further reducing the liability of the power utility for loss of lives of the crew.

The SL-PWR improves upon lookout observers and firefighting crew since:

1. It employs already-owned utility UAV resources and hence the cost of sustainability is relatively low.

2. It is not delayed by road networks and can serve as adequate first responders.

3. It has a "birds eye" view that can spot endogenous as well as exogenous wildfires.

4. It can avoid direct burns/heat damages by flying increased distances above and away from direct impact from the wildfire.

7.4.3 Comparison In Wildfire Detection

All existing wildfire solutions so far focus on detection alone. Hence the SL-PWR has so much more utility for resilient power systems response against wildfire threats for which wildfire detection is just a sub-module.

1. Existing solutions like the FIREBird, FireALERT MK I, and other smoke/fire detectors, function only in the “Wildfire Progression” phase of the system’s resilience during wildfire threats. Comparatively, the SL-PWR functions comprehensively in all resilience phases of

the system during a wildfire threat. These automated functionalities range from the "pre-wildfire –> wildfire progression –> post-wildfire" phases. In the pre-wildfire phase, the modules of the SL-PWR that are active include the vegetation module and the power equipment module. The next resilience phase that the power system lies during wildfire threat is the “Wildfire Progression” phase. This phase becomes active IF all efforts of the SL-PWR fail in the previous phase discussed, and a wildfire is ignited. In this phase, the SL-PWR has five functionalities enumerated below, which not only detect and pin-point the exact wildfire location/boundary but aid firefighting efforts as a first-responder, given SL-PWR’s information on the wildfire progress.

(a) To detect wildfires including undersurface fires or fires that come with smoke

(b) Locate and localize the wildfire (by detecting the wildfire boundaries)

(c) Estimate the spread of the wildfire (size of the wildfire)

(d) Detect the rate of spread of the wildfire

(e) Monitor the wildfire in real-time.

The next phase is the Post-Wildfire/Restoration phase, where the SL-PWR’s "Burnt Equipment Detection and Estimation Module" is active. This module detects, classifies, and estimates the equipment damage after the wildfire. This enhances the utility process which conventionally is the manual inspection crew taking inventory of damaged equipment and damage extent. The SL-PWR’s "Burnt Equipment Detection and Estimation Module" functions to make this process more efficient by enabling automation, rapidity, and transparency in restoration efforts.

7.5 Deployability of the SL-PWR

The SL-PWR is designed so it can be deployed in different ways including Energy Management System (EMS)/ Outage Management System (OMS)/ SCADA room, or deployed as a packaged hardware.

7.5.1 Energy/Outage Management System-Controlled SL-PWR

Depending on utility preferences, the SL-PWR can be designed and deployed as in Fig.6.1, where the processing software GUI is managed from the EMS/ OMS/ SCADA operation room. Already existing utility monitoring methods such as service area cameras and satellite imagery can be processed by the SL-PWR to provide real-time qualitative information to appropriate wildfire response teams. This deployment method may add additional time to the processing of the input images depending on the time it takes the internet service provider (ISP) communication service to transfer the captured images to the SL-PWR software at the operator's base. Some utilities have also begun integrating private communication networks to mitigate dependence on third party service providers. With the UAV-enabled SL-PWR model, the UAVs fly over the service area using the SL-PWR's spatio-temporal optimization model. The image attributes [image,UAV geographical location (lat, lon)] are then sent as output from the UAVs and input to the SL-PWR operations via a communication link e.g., cellular communication or leased lines from ISPs since they provide more redundancy (availability of various ISPs) in a wildfire scenario. As the UAVs fly over, the images (vegetation, endogenous ignition source, fire spread/smoke, burn-damaged equipment) are captured from different scales/angles and taken at different times of day and weather conditions. UAV control is performed in the mission planning "ground station" software which can easily run on Windows PCs. The software enables the operator plan and upload missions to UAVs wirelessly, launch the UAVs, monitor trip progress and issue landing commands. Specifically, photogrammetry tools in the software can be used for the mission planning and route specification after route optimization. In this tool, the aerial image of the service area to be monitored is highlighted within a rectangle, producing a preview of the proposed flight paths using waypoints which signify the UAV turning points in the trip. Typically, "no waypoints zones" (e.g., close to major airports) are also indicated by the software so as to mitigate the UAV flying into restricted airspace. After confirmation, the trip is uploaded wirelessly to the UAV via it's datalink which creates a communication bridge between the control software PC and UAV. The UAV can then be launched, its trip monitored through each waypoint, and automatically landed upon trip completion via the software. Furthermore, the captured image's geographical coordinates is also recorded since the GPS receiver avails the UAV positional data along with the images which are sent to SL-PWR for analysis, detection and estimation.

7.5.2 Deployed in Compact Hardware

The SL-PWR could also be designed to be compressed to function all in a device that would be mounted on the UAVs as in Fig. 7.2, depending on the commercialization requirements of the utilities. This mode of deployment will retain the < 40msecs time of detection, while the system operator deals with verification of alerts sent in by the SL-PWR by looking at the images associated with the alerts and following protocol thereafter. In this mode, the operator can still control and

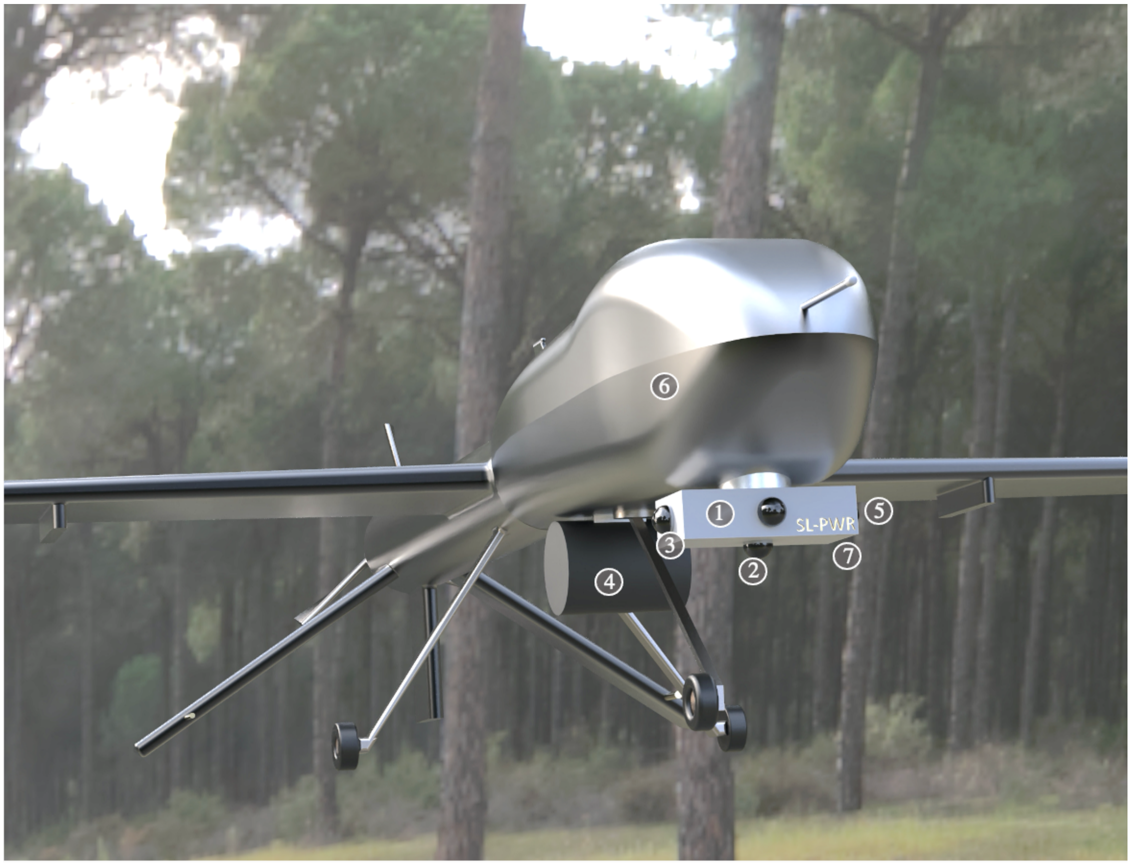


Figure 7.2: The SL-PWR Prototype Deployment. 1.) Controller and Software BrainBox, 2.) Main View Camera, 3.) Lateral View Cameras 4.) SL-PWR Fluid Holder, 5.) Thermal sensor, 6.) UAV, 7.) Communication module

manage the ground station software of the UAVs if the utility requires. The following illustration visualizes the compact mode of deployment.

7.6 Conclusion

This chapter discusses in great detail the advantages of utilities employing, as compared to existing solutions, the self-sufficient low-cost wildfire mitigation (SL-PWR) model that spatio-temporally predicts wildfire threat and also detects and localizes wildfire occurrence, spread, and other wildfire-related incidents e.g., power equipment as ignition sources. Results show effective performance in improving and optimizing power system resilience in the wildfire response of utilities, and as well, shows that the return on investment supersedes the conventional utility techniques of wildfire response. Most importantly, the proposed model will aid to save lives of utility crew, avoiding disastrous events such as the 2020 fire siege regrettably cost the lives of pilot, Michael Fornier, fire captain, Diana Jones, and firefighter Charles Morton.

8. CONCLUSION AND FUTURE DIRECTIONS

8.1 Conclusion

This work, inspired by the catastrophic effects of high impact low probability events on the cyberphysical power grid, addresses risk reduction of critical power system infrastructure to top cyber and physical threats, with the aim of improving critical infrastructure resilience, building into enabling the next generation energy management.

On the cyber side, the work begins by proposing the component ranking and risk sensitivity analysis model (CRSA), that improves system robustness to adversary intrusion by reducing the adversary exploitable paths from the point of intrusion to the target control devices. Given that adversary intrusion has occurred, the work proposes techniques to proactively detect the actions of stealth adversaries seeking to disrupt system operations via the threat of false data injection. The proposed graph neural network (GNN) based detector captures the spatial correlations of field measurements, and functions against the adversary objectives which are to maximize system impact (deviation from normal system state) while remaining stealth enough to evade the conventional power system detectors. Given a major aspect of resilience-oriented risk reduction, which lies in timeliness i.e., the rapidity of defense actions, this work proposes the OpenConduit tool which automates the creation of a digital twin of the power system network which enables discussed use cases that aim to improve defense-side actions.

On the physical side, the work proposes resilience-oriented risk minimization approaches against the threat of wildfires. First is the development modeling approaches better suited for wildfire risk reduction in the bulk power grid, as opposed to conventional approaches that use methods better suited for wildlands. The proposed Spatio-temporal wildfire ignition predictor (STWIP) model integrates data-driven, mathematical, and physics-based approaches to better model the spatio-temporal potential for wildfires, and then uses the results of this model to optimize risk-based operations of the power system to endogenous and exogenous wildfires based on potential scenarios from real wildfire events. Beyond the STWIP, the work discusses the design and implementation of the self-sufficient low-cost model (SL-PWR) which addresses wildfire risk mitigation comprehensively in the resilience pipeline and improves the response of power systems to wildfires. Results presented in this work illustrate the effectiveness of the proposed methods towards improving resilience and reducing risk in critical infrastructure operations. The techniques proposed in this work can generalized to other critical infrastructure but for the purposes of specificity have been demonstrated for the power grid.

8.2 Future Directions: Vision Board for Next Generation Energy Management

Beyond the use cases discussed in the body of the work, the vision is for the approaches developed and implemented in this work be used to improve risk analysis and situational awareness in the cyber physical power system via visualization in the next generation energy management.

REFERENCES

[1] "Critical infrastructure sectors," https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors, [Online; accessed 24-March-2023].

[2] B. Cotterell, "Electric grid vulnerable to cyber attack, experts warn," https://www.tallahassee.com/story/news/2015/04/13/electric-grid-vulnerable-cyber-attack-experts-warn/25736629/, 2015, [Online; accessed 17-March-2023].

[3] C. S. Holling, "Resilience and stability of ecological systems," *Annual review of ecology and systematics*, pp. 1–23, 1973.

[4] B. Obama, "Presidential policy directive 21: Critical infrastructure security and resilience," *Washington, DC*, 2013.

[5] R. Francis and B. Bekera, "A metric and frameworks for resilience analysis of engineered and infrastructure systems," *Reliability engineering & system safety*, vol. 121, pp. 90–103, 2014.

[6] M. N. Albasrawi, N. Jarus, K. A. Joshi, and S. S. Sarvestani, "Analysis of reliability and resilience for smart grids," in *2014 IEEE 38th Annual Computer Software and Applications Conference*. IEEE, 2014, pp. 529–534.

[7] A. Umunnakwe, H. Huang, K. Oikonomou, and K. Davis, "Quantitative analysis of power systems resilience: Standardization, categorizations, and challenges," *Renewable and Sustainable Energy Reviews*, vol. 149, p. 111252, 2021.

[8] M. Bruneau, S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace, and D. Von Winterfeldt, "A framework to quantitatively assess and enhance the seismic resilience of communities," *Earthquake spectra*, vol. 19, no. 4, pp. 733–752, 2003.

[9] O. Kulak, S. Cebi, and C. Kahraman, "Applications of axiomatic design principles: A literature review," *Expert Systems with Applications*, vol. 37, no. 9, pp. 6705–6717, 2010.

[10] H. Suh, *Axiomatic Design: advances and applications MIT-Pappalardo series in Mechanical Engineering*. Oxford University Press, USA, 2001.

[11] S. Shin, S. Lee, D. R. Judi, M. Parvania, E. Goharian, T. McPherson, and S. J. Burian, "A systematic review of quantitative resilience measures for water infrastructure systems," *Water*, vol. 10, no. 2, p. 164, 2018.

[12] R. Arghandeh, A. Von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renewable and Sustainable Energy Reviews*, vol. 58, pp. 1060–1069, 2016.

[13] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," in *Situational awareness*. Routledge, 2017, pp. 9–42.

[14] T. Pahi, M. Leitner, and F. Skopik, "Analysis and assessment of situational awareness models for national cyber security centers." in *ICISSP*, 2017, pp. 334–345.

[15] D. Eisenberg, "Resilience corner: Resilience is not about what you have, it is about what you do," 2020.

[16] A. Abur and A. Expósito, *Power System State Estimation: Theory and Implementation*, ser. Power Engineering (Willis). CRC Press, 2004.

[17] G. Andersen, M. Cleveland, and D. Shea, "Modernizing the electric grid: State role and policy options," 2021, [Online; accessed 17-March-2023].

[18] B. Fung and G. Sands, "Ransomware attackers used compromised password to access colonial pipeline network," 2021. [Online]. Available: https://www.cnn.com/2021/06/04/politics/colonial-pipeline-ransomware-attack-password

[19] T. Maynard and N. Beecroft, "Business blackout: The insurance implications of a cyber attack on the us power grid," *Emerging Risk Report*.

[20] W. T. Shaw, “Scada system vulnerabilities to cyber attack,” https://electricenergyonline.com/energy/magazine/181/article/SCADA-System-Vulnerabilities-to-Cyber-Attack.htm, [Online; accessed 17-March-2023].

[21] Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response, “Electric disturbance events (OE-417) annual summaries,” https://www.oe.netl.doe.gov/OE417_annual_summary.aspx, [Online; accessed 17-March-2023].

[22] C. Brooks, “3 Alarming Threats To The U.S. Energy Grid – Cyber, Physical, And Existential Events,” https://www.forbes.com/sites/chuckbrooks/2023/02/15/3-alarming-threats-to-the-us-energy-grid--cyber-physical-and-existential-events/, 2023, [Online; accessed 17-March-2023].

[23] “Threats to the energy grid,” https://www.americansecurityproject.org/climate-energy-and-security/energy/threats-to-the-energy-grid/, [Online; accessed 10-February-2023].

[24] “Suppression costs: Federal firefighting costs (suppression only),” https://www.nifc.gov/fire-information/statistics/suppression-costs, [Online; accessed 24-March-2023].

[25] Fortinet, “Independent study pinpoints significant scada/ics security risks,” https://www.fortinet.com/content/dam/fortinet/assets/white-papers/WP-Independent-Study-Pinpoints-Significant-Scada-ICS-Cybersecurity-Risks.pdf, [Online; accessed 17-March-2023].

[26] The MITRE Corporation, “Mitre att&ck,” https://attack.mitre.org/, [Online; accessed 24-March-2023].

[27] National Institute of Standards and Technology, “National vulnerability database,” https://nvd.nist.gov/, [Online; accessed 9-February-2023].

[28] “Common vulnerability scoring system v3.0: Specification document,” https://www.first.org/cvss/v3.0/cvss-v30-specification_v1.9.pdf, 2021, [Online; accessed 17-April-2023].

[29] C. Kousky, K. Greig, B. Lingle, and K. Kunreuther, “Wildfire cost in california: The role of electric utilities,” *Changes*, vol. 114, no. 18, pp. 4582–4590, 2018.

[30] D. Thomas, D. Butry, S. Gilbert, D. Webb, and J. Fung, *The costs and losses of wildfires: A literature survey.* US Department of Commerce, National Institute of Standards and Technology, 2017.

[31] M. Zhao and M. Barati, "A real-time fault localization in power distribution grid for wildfire detection through deep convolutional neural networks," *IEEE Transactions on Industry Applications*, vol. 57, no. 4, pp. 4316–4326, 2021.

[32] S. Dian, P. Cheng, Q. Ye, J. Wu, R. Luo, C. Wang, D. Hui, N. Zhou, D. Zou, Q. Yu *et al.*, "Integrating wildfires propagation prediction into early warning of electrical transmission line outages," *IEEE Access*, vol. 7, pp. 27 586–27 603, 2019.

[33] N. Rhodes, L. Ntaimo, and L. Roald, "Balancing wildfire risk and power outages through optimized power shut-offs," *arXiv preprint arXiv:2004.07156*, 2020.

[34] J. Wischkaemper, C. Benner, B. Russell, and K. Manivannan, "Reducing wildfire risk through use of advanced electrical waveform monitoring and analytics," in *Presented at the 2013 CIGRE Grid of the Future Symposium, Boston, MA*, 2013.

[35] H. Nazaripouya, "Power grid resilience under wildfire: A review on challenges and solutions," in *2020 IEEE Power & Energy Society General Meeting (PESGM).* IEEE, 2020, pp. 1–5.

[36] M. Abdelmalak and M. Benidris, "Enhancing power system operational resilience against wildfires," *IEEE Transactions on Industry Applications*, vol. 58, no. 2, pp. 1611–1621, 2022.

[37] D. N. Trakas and N. D. Hatziargyriou, "Optimal distribution system operation for enhancing resilience against wildfires," *IEEE Transactions on Power Systems*, vol. 33, no. 2, pp. 2260–2271, 2017.

[38] A. Umunnakwe, A. Sahu, M. R. Narimani, K. Davis, and S. Zonouz, "Cyber-physical component ranking for risk sensitivity analysis using betweenness centrality," *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 139–150, 2021.

[39] National Academies of Sciences, Engineering, and Medicine, *Communications, Cyber Resilience, and the Future of the U.S. Electric Power System: Proceedings of a Workshop*, A. F. Johnson, Ed. Washington, DC: The National Academies Press, 2020. [Online]. Available: https://nap.nationalacademies.org/catalog/25782/communications-cyber-resilience-and-the-future-of-the-us-electric-power-system

[40] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38–45, 2012.

[41] J. J. Grainger, W. D. Stevenson, W. D. Stevenson *et al.*, *Power system analysis*, 2003.

[42] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "Socca: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 3–13, 2013.

[43] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2464–2475, 2015.

[44] K. Davis, R. Berthier, S. Zonouz, G. Weaver, R. Bobba, E. Rogers, P. Sauer, and D. Nicol, "Cyber-physical security assessment (cypsa) for electric power systems," *IEEE-HKN: THE BRIDGE*, 2016.

[45] S. Jin, Z. Huang, Y. Chen, D. Chavarría-Miranda, J. Feo, and P. C. Wong, "A novel application of parallel betweenness centrality to power grid contingency analysis," in *2010 IEEE International Symposium on Parallel & Distributed Processing (IPDPS).* IEEE, 2010, pp. 1–7.

[46] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," *International Journal of Security and Networks*, vol. 6, no. 1, pp. 2–13, 2011.

[47] P.-Y. Chen, S. Choudhury, and A. O. Hero, "Multi-centrality graph spectral decompositions and their application to cyber intrusion detection," in *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2016, pp. 4553–4557.

[48] J. A. Kersulis, I. A. Hiskens, C. Coffrin, and D. K. Molzahn, "Topological graph metrics for detecting grid anomalies and improving algorithms," in *2018 Power Systems Computation Conference (PSCC)*. IEEE, 2018, pp. 1–7.

[49] B. Liu, Z. Li, X. Chen, Y. Huang, and X. Liu, "Recognition and vulnerability analysis of key nodes in power grid based on complex network centrality," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 3, pp. 346–350, 2017.

[50] X. Wang, Y. Koç, R. E. Kooij, and P. Van Mieghem, "A network approach for power grid robustness against cascading failures," in *2015 7th international workshop on reliable networks design and modeling (RNDM)*. IEEE, 2015, pp. 208–214.

[51] Z. Wang, A. Scaglione, and R. J. Thomas, "Electrical centrality measures for electric power grid vulnerability analysis," in *49th IEEE conference on decision and control (CDC)*. IEEE, 2010, pp. 5792–5797.

[52] N. Gaudet, A. Sahu, A. E. Goulart, E. Rogers, and K. Davis, "Firewall configuration and path analysis for smartgrid networks," in *2020 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*. IEEE, 2020, pp. 1–6.

[53] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the ukrainian power grid," 2016. [Online]. Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[54] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[55] T. Morris, R. Vaughn, and Y. Dandass, "A retrofit network intrusion detection system for modbus rtu and ascii industrial control systems," in *2012 45th Hawaii International Conference on System Sciences*. IEEE, 2012, pp. 2338–2345.

[56] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 235–244, 2013.

[57] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "Cpindex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566–575, 2014.

[58] T. A. Ernster and A. K. Srivastava, "Power system vulnerability analysis-towards validation of centrality measures," in *PES T&D 2012*. IEEE, 2012, pp. 1–6.

[59] A. Sahu, H. Huang, K. Davis, and S. Zonouz, "A framework for cyber-physical model creation and evaluation," in *2019 20th International Conference on Intelligent System Application to Power Systems (ISAP)*, 2019, pp. 1–8.

[60] G. A. Weaver, K. Davis, C. M. Davis, E. J. Rogers, R. B. Bobba, S. Zonouz, R. Berthier, P. W. Sauer, and D. M. Nicol, "Cyber-physical models for power grid security analysis: 8-substation case," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2016, pp. 140–146.

[61] "Network perception," https://www.network-perception.com/np-view/, [Online; accessed 17-March-2023].

[62] R. Cohen and S. Havlin, *Complex networks: structure, robustness and function*. Cambridge university press, 2010.

[63] L. C. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, pp. 35–41, 1977.

[64] A. K. Srivastava, T. A. Ernster, R. Liu, and V. G. Krishnan, "Graph-theoretic algorithms for cyber-physical vulnerability analysis of power grid with incomplete information," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 887–899, 2018.

[65] "Deep Cyber Physical Situational Awareness for Energy Systems: A Secure Foundation for Next-Generation Energy Management Cybersecurity," 2022. [Online]. Available: https://cypres.engr.tamu.edu/

[66] TEES, "Cyber physical resilient energy systems: Test cases," https://cypres.engr.tamu.edu/test-cases/, [Online; accessed 17-April-2023].

[67] P. Z. Zahariev, G. V. Hristov, and T. B. Iliev, "Study on the impact of node density and sink location in wsn," in *Technological Developments in Networking, Education and Automation*. Springer, 2010, pp. 539–542.

[68] E. H. Callaway Jr, *Wireless sensor networks: architectures and protocols*. CRC press, 2003.

[69] O. Boyaci, A. Umunnakwe, A. Sahu, M. R. Narimani, M. Ismail, K. R. Davis, and E. Serpedin, "Graph neural networks based detection of stealth false data injection attacks in smart grids," *IEEE Systems Journal*, 2021.

[70] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2012, pp. 342–347.

[71] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2011.

[72] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[73] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2016.

[74] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[75] P.-Y. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang, "Detection of false data injection attacks in smart-grid systems," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 206–213, 2015.

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

[77] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive cusum method and analysis," *IEEE Systems Journal*, vol. 10, no. 2, pp. 532–543, 2014.

[78] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in smart grids based on graph signal processing," *IEEE Systems Journal*, 2019.

[79] J. Duan, W. Zeng, and M.-Y. Chow, "Resilient distributed dc optimal power flow against data integrity attack," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3543–3552, 2016.

[80] M. N. Kurt, Y. Yılmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 498–513, 2018.

[81] M. G. Kallitsis, S. Bhattacharya, S. Stoev, and G. Michailidis, "Adaptive statistical detection of false data injection attacks in smart grids," in *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. IEEE, 2016, pp. 826–830.

[82] M. N. Kurt, Y. Yılmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2015–2030, 2018.

[83] J. Hao, E. Kang, J. Sun, Z. Wang, Z. Meng, X. Li, and Z. Ming, "An adaptive markov strategy for defending smart grid false data injection from malicious attackers," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2398–2408, 2016.

[84] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, “Detecting stealthy false data injection using machine learning in smart grid,” *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2014.

[85] E. M. Ferragut, J. Laska, M. M. Olama, and O. Ozmen, “Real-time cyber-physical false data attack detection in smart grids using neural networks,” in *2017 International Conference on Computational Science and Computational Intelligence (CSCI).* IEEE, 2017, pp. 1–6.

[86] D. Wang, X. Wang, Y. Zhang, and L. Jin, “Detection of power grid disturbances and cyber-attacks based on machine learning,” *Journal of Information Security and Applications*, vol. 46, pp. 42–52, 2019.

[87] S. Binna, S. R. Kuppannagari, D. Engel, and V. K. Prasanna, “Subset level detection of false data injection attacks in smart grids,” in *2018 IEEE Conference on Technologies for Sustainability (SusTech).* IEEE, 2018, pp. 1–7.

[88] K. Vimalkumar and N. Radhika, “A big data framework for intrusion detection in smart grids using apache spark,” in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI).* IEEE, 2017, pp. 198–204.

[89] E. Drayer and T. Routtenberg, “Detection of false data injection attacks in power systems with graph fourier transform,” in *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP).* IEEE, 2018, pp. 890–894.

[90] R. Ramakrishna and A. Scaglione, “Detection of false data injection attack using graph signal processing for the power grid,” in *2019 IEEE Global Conference on Signal and Information Processing (GlobalSIP).* IEEE, 2019, pp. 1–5.

[91] R. Deng, G. Xiao, and R. Lu, “Defending against false data injection attacks on power system state estimation,” *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, 2015.

[92] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.

[93] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2019.

[94] J. Wang, C. Jiang, H. Zhang, Y. Ren, K.-C. Chen, and L. Hanzo, "Thirty years of machine learning: The road to pareto-optimal wireless networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1472–1514, 2020.

[95] J. Zhou, G. Cui, S. Hu, Z. Zhang, C. Yang, Z. Liu, L. Wang, C. Li, and M. Sun, "Graph neural networks: A review of methods and applications," *AI Open*, vol. 1, pp. 57–81, 2020.

[96] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, 2013.

[97] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2011, pp. 244–248.

[98] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *2012 IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 3153–3158.

[99] Z.-H. Yu and W.-L. Chin, "Blind false data injection attack using pca approximation method in smart grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1219–1226, 2015.

[100] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on smart grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[101] P. Bojanowski, A. Joulin, D. Lopez-Pas, and A. Szlam, "Optimizing the latent space of generative networks," in *Proceedings of the 35th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, vol. 80, 2018, pp. 600–609.

[102] L. Thurner, A. Scheidler, F. Schafer, J. H. Menke, J. Dollichon, F. Meier, S. Meinecke, and M. Braun, "pandapower - an open source python tool for convenient modeling, analysis and optimization of electric power systems," *IEEE Transactions on Power Systems*, 2018.

[103] The Electric Reliability Council of Texas (ERCOT). Backcasted (Actual) Load Profiles - Historical. http://www.ercot.com/mktinfo/loadprofile/alp/. [Online; accessed 24-March-2023].

[104] M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, M. Isard *et al.*, "Tensorflow: A system for large-scale machine learning," in *12th {USENIX} symposium on operating systems design and implementation ({OSDI} 16)*, 2016, pp. 265–283.

[105] C. M. Bishop, *Pattern recognition and machine learning*. springer, 2006.

[106] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[107] A. Umunnakwe, P. Wlazlo, A. Sahu, J. Velasquez, K. Davis, A. Goulart, and S. Zonouz, "Openconduit: A tool for recreating power system communication networks automatically," in *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2022, pp. 141–147.

[108] A. Sahu, K. Davis, H. Huang, A. Umunnakwe, S. Zonouz, and A. Goulart, "Design of next-generation cyber-physical energy management systems: Monitoring to mitigation," *IEEE Open Access Journal of Power and Energy*, 2023.

[109] P. J. Wlazlo, "Recreating wide area industrial control systems network within an emulated environment," Master's thesis, 2021.

[110] Amazon Web Services, "What is digital twin technology?" https://aws.amazon.com/what-is/digital-twin, [Online; accessed 28-March-2023].

[111] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case by SANS ICS ," https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[112] L. Dignan, "Colonial pipeline cyberattack shuts down pipeline that supplies 45% of east coast's fuel," 2021. [Online]. Available: https://www.zdnet.com/article/colonial-pipeline-cyberattack-shuts-down-pipeline-that-supplies-45-of-east-coasts-fuel/

[113] E. Kovacs, "Russia-Linked Pipedream/Incontroller ICS Malware Designed to Target Energy Facilities," https://www.securityweek.com/russia-linked-pipedreamincontroller-ics-malware-designed-target-energy-facilities, 2022, [Online; accessed 27-March-2023].

[114] J. Ahrenholz, C. Danilov, T. R. Henderson, and J. H. Kim, "Core: A real-time network emulator," in *MILCOM 2008-2008 IEEE Military Communications Conference*. IEEE, 2008, pp. 1–7.

[115] A. Sahu, P. Wlazlo, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, "Design and evaluation of a cyber-physical testbed for improving attack resilience of power systems," *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 4, pp. 208–227, 2021.

[116] T. Tarman, T. Rollins, L. Swiler, J. Cruz, E. Vugrin, H. Huang, A. Sahu, P. Wlazlo, A. Goulart, and K. Davis, "Comparing reproduced cyber experimentation studies across different emulation testbeds," in *Cyber Security Experimentation and Test Workshop*, 2021, pp. 63–71.

[117] V. Babu and D. M. Nicol, "On repeatable emulation in virtual testbeds," in *2018 Winter Simulation Conference (WSC)*. IEEE, 2018, pp. 3813–3824.

[118] S. Tan, W.-Z. Song, Q. Dong, and L. Tong, “Score: Smart-grid common open research emulator,” in *2012 IEEE third international conference on smart grid communications (SmartGridComm)*. IEEE, 2012, pp. 282–287.

[119] vmware, “Unified Management for Containers and VMs,” https://www.vmware.com/products/vsphere.html, [Online; accessed 5-June-2022].

[120] Sandia, “Github: sandia-minimega,” https://github.com/sandia-minimega/minimega, [Online; accessed 12-June-2022].

[121] “Emulab,” https://www.emulab.net/portal/frontpage.php, [Online; accessed 14-June-2022].

[122] C. Siaterlis, A. P. Garcia, and B. Genge, “On the use of emulab testbeds for scientifically rigorous experiments,” *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 929–942, 2012.

[123] T. Benzel, R. Braden, D. Kim, C. Neuman, A. Joseph, K. Sklower, R. Ostrenga, and S. Schwab, “Experience with deter: a testbed for security research,” in *2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006.* IEEE, 2006, pp. 10–pp.

[124] J. Mirkovic, T. V. Benzel, T. Faber, R. Braden, J. T. Wroclawski, and S. Schwab, “The deter project: Advancing the science of cyber security experimentation and test,” in *2010 IEEE International Conference on Technologies for Homeland Security (HST)*. IEEE, 2010, pp. 1–7.

[125] B. Ferguson, A. Tall, and D. Olsen, “National cyber range overview,” in *2014 IEEE Military Communications Conference*. IEEE, 2014, pp. 123–128.

[126] U. Lamping and E. Warnicke, “Wireshark user’s guide,” *Interface*, vol. 4, no. 6, p. 1, 2004.

[127] P. Biondi, “Scapy documentation, release 2.4.5-dev,” *https://media.readthedocs.org/pdf/scapy/latest/scapy.pdf*, 2022.

[128] A. Hagberg, D. Schult, and P. Swart, "Github: Networkx," https://github.com/networkx/networkx, [Online; accessed 11-June-2022].

[129] J. Ahrenholz, C. Danilov, T. R. Henderson, and J. H. Kim, "Core: A real-time network emulator," in *MILCOM 2008 - 2008 IEEE Military Communications Conference*, 2008, pp. 1–7.

[130] coreemu, "CORE Architecture," https://coreemu.github.io/core/architecture.html, [Online; accessed 29-March-2022].

[131] "psutil documentation," https://psutil.readthedocs.io/en/latest/, [Online; accessed 11-June-2022].

[132] G. Hancock, "Cyber deception: How to build a program," *Attivo Networks*, pp. 1–9, 2019.

[133] A. Umunnakwe, M. Parvania, H. Nguyen, J. D. Horel, and K. R. Davis, "Data-driven spatio-temporal analysis of wildfire risk to power systems operation," *IET Generation, Transmission & Distribution*, vol. 16, no. 13, pp. 2531–2546, 2022.

[134] Executive Office of the President. Council of Economic Advisers, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*. The Council, 2013.

[135] D. Wang, D. Guan, S. Zhu, M. M. Kinnon, G. Geng, Q. Zhang, H. Zheng, T. Lei, S. Shao, P. Gong *et al.*, "Economic footprint of california wildfires in 2018," *Nature Sustainability*, vol. 4, no. 3, 2021.

[136] Insurance Information Institute, "Top 10 costliest wildland fires in the united states," https://www.iii.org/table-archive/21424, [Online; accessed 26-August-2022].

[137] Attorney, Butte County District, "The Camp Fire public report: A summary of the Camp Fire investigation," *Oroville, CA*, 2020.

[138] H. Trabish, "De-energize and DERs: The tough options wildfires pose for California utilities," 2019.

[139] M. I. George and C. Dennis, “2020 fire siege,” pp. 1–122, 2020, [Online; accessed 2-April-2022].

[140] H. Smith, “PG&E under federal probe in Dixie fire, expects more than $1 billion in losses tied to blaze,” https://www.latimes.com/california/story/2021-11-01/amid-federal-probe-in-dixie-fire-pacific-gas-electric-faces-1-billion-in-losses, [Online; accessed 6-May-2022].

[141] Incident Information System, “Dixie Fire (CA),” https://inciweb.nwcg.gov/incident/7690/, [Online; accessed 6-May-2022].

[142] J. D. Horel and X. Dong, “An evaluation of the distribution of remote automated weather stations (raws),” *Journal of Applied Meteorology and Climatology*, vol. 49, no. 7, pp. 1563–1578, 2010.

[143] D. P. Tyndall and J. D. Horel, “Impacts of mesonet observations on meteorological surface analyses,” *Weather and Forecasting*, vol. 28, no. 1, pp. 254–269, 2013.

[144] CNBC, “PG&E to cut off power to nearly 800,000 customers to reduce wildfire risk,” https://www.cnbc.com/2019/10/08/pge-to-cut-off-power-to-nearly-800000-customers-to-reduce-wildfire-risk.html, [Online; accessed 26-August-2022].

[145] California Legislative Information, “AB-1054 Public utilities: wildfires and employee protection,” https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1054, [Online; accessed 17-April-2023].

[146] K. Xu, X. Zhang, Z. Chen, W. Wu, and T. Li, “Risk assessment for wildfire occurrence in high-voltage power line corridors by using remote-sensing techniques: A case study in hubei province, china,” *International journal of remote sensing*, vol. 37, no. 20, pp. 4818–4837, 2016.

[147] D. Chaparro, M. Vall-Llossera, M. Piles, A. Camps, C. Rüdiger, and R. Riera-Tatché, “Predicting the extent of wildfires using remotely sensed soil moisture and temperature trends,”

IEEE journal of selected topics in applied earth observations and remote sensing, vol. 9, no. 6, pp. 2818–2829, 2016.

[148] D. N. Trakas and N. D. Hatziargyriou, "Optimal distribution system operation for enhancing resilience against wildfires," *IEEE Transactions on Power Systems*, vol. 33, no. 2, pp. 2260–2271, 2018.

[149] A. A. Alencar, L. A. Solórzano, and D. C. Nepstad, "Modeling forest understory fires in an eastern amazonian landscape," *Ecological Applications*, vol. 14, no. sp4, pp. 139–149, 2004.

[150] J. P. Prestemon, M. L. Chas-Amil, J. M. Touza, and S. L. Goodrick, "Forecasting intentional wildfires using temporal and spatiotemporal autocorrelations," *International Journal of Wildland Fire*, vol. 21, no. 6, pp. 743–754, 2012.

[151] R. A. Bradstock, J. Cohn, A. M. Gill, M. Bedward, and C. Lucas, "Prediction of the probability of large fires in the sydney region of south-eastern australia using fire weather," *International Journal of Wildland Fire*, vol. 18, no. 8, pp. 932–943, 2010.

[152] H. Zhang, X. Han, and S. Dai, "Fire occurrence probability mapping of northeast china with binary logistic regression model," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 6, no. 1, pp. 121–127, 2013.

[153] J. Arganaraz, A. Lighezzolo, K. Clemoveki, D. Bridera, J. Scavuzzo, and L. Bellis, "Operational meteo fire risk system based on space information for chaco serrano," *IEEE Latin America Transactions*, vol. 16, no. 3, pp. 975–980, 2018.

[154] S. Lall and B. Mathibela, "The application of artificial neural networks for wildfire risk prediction," in *2016 International Conference on Robotics and Automation for Humanitarian Applications (RAHA)*. IEEE, 2016, pp. 1–6.

[155] L. Vilar, D. G. Woolford, D. L. Martell, and M. P. Martín, "A model for predicting human-caused wildfire occurrence in the region of madrid, spain," *International Journal of Wildland Fire*, vol. 19, no. 3, pp. 325–337, 2010.

[156] A. Malik, M. R. Rao, N. Puppala, P. Koouri, V. A. K. Thota, Q. Liu, S. Chiao, and J. Gao, "Data-driven wildfire risk prediction in northern California," *Atmosphere*, vol. 12, no. 1, p. 109, 2021.

[157] J. Storer and R. Green, "PSO trained neural networks for predicting forest fire size: a comparison of implementation and performance," in *2016 international joint conference on neural networks (IJCNN)*. IEEE, 2016, pp. 676–683.

[158] A. Jaafari, E. K. Zenner, M. Panahi, and H. Shahabi, "Hybrid artificial intelligence models based on a neuro-fuzzy system and metaheuristic optimization algorithms for spatial prediction of wildfire probability," *Agricultural and forest meteorology*, vol. 266, pp. 198–207, 2019.

[159] H. Liang, M. Zhang, and H. Wang, "A neural network model for wildfire scale prediction using meteorological factors," *IEEE Access*, vol. 7, pp. 176 746–176 755, 2019.

[160] Y. Li, H. Mulyono, Y. Chen, Z. Lu, and D. Chan, "RtFPS: An Interactive Map that Visualizes and Predicts Wildfires in the US," *arXiv preprint arXiv:2105.10880*, 2021.

[161] B. Ansari and S. Mohagheghi, "Optimal energy dispatch of the power distribution network during the course of a progressing wildfire," *International Transactions on Electrical Energy Systems*, vol. 25, no. 12, pp. 3422–3438, 2015.

[162] M. Choobineh, B. Ansari, and S. Mohagheghi, "Vulnerability assessment of the power grid against progressing wildfires," *Fire Safety Journal*, vol. 73, pp. 20–28, 2015.

[163] "Fire Potential Index," https://fpi.sdgeweather.com, [Online; accessed 17-April-2023].

[164] M. E. Chambers, P. J. Fornwalt, S. L. Malone, and M. A. Battaglia, "Patterns of conifer regeneration following high severity wildfire in ponderosa pine–dominated forests of the colorado front range," *Forest Ecology and Management*, vol. 378, pp. 57–67, 2016.

[165] B. K. Blaylock, J. D. Horel, and C. Galli, "High-resolution rapid refresh model data analytics derived on the open science grid to assist wildland fire weather assessment," *Journal of Atmospheric and Oceanic Technology*, vol. 35, no. 11, pp. 2213–2227, 2018.

[166] N. Hamadeh, B. Daya, A. Hilal, and P. Chauvet, "An analytical review on the most widely used meteorological models in forest fire prediction," in *2015 Third International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE)*. IEEE, 2015, pp. 239–244.

[167] M.-A. Parisien, S. Snetsinger, J. A. Greenberg, C. R. Nelson, T. Schoennagel, S. Z. Dobrowski, and M. A. Moritz, "Spatial variability in wildfire probability across the western united states," *International Journal of Wildland Fire*, vol. 21, no. 4, pp. 313–327, 2012.

[168] M. A. Finney, C. W. McHugh, I. C. Grenfell, K. L. Riley, and K. C. Short, "A simulation of probabilistic wildfire risk components for the continental united states," *Stochastic Environmental Research and Risk Assessment*, vol. 25, no. 7, pp. 973–1000, 2011.

[169] J. Bishop, "Technical background of the fireline assessment method (flame)," in *In: Butler, Bret W.; Cook, Wayne, comps. The fire environment–innovations, management, and policy; conference proceedings. 26-30 March 2007; Destin, FL. Proceedings RMRS-P-46CD. Fort Collins, CO: US Department of Agriculture, Forest Service, Rocky Mountain Research Station. CD-ROM. p. 27-74*, vol. 46, 2007.

[170] E. I. Koufakis, P. T. Tsarabaris, J. S. Katsanis, C. G. Karagiannopoulos, and P. D. Bourkas, "A wildfire model for the estimation of the temperature rise of an overhead line conductor," *IEEE transactions on power delivery*, vol. 25, no. 2, pp. 1077–1082, 2010.

[171] M. Choobineh and S. Mohagheghi, "Power grid vulnerability assessment against wildfires using probabilistic progression estimation model," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 2016, pp. 1–5.

[172] R. Ziel and W. M. Jolly, "Performance of fire behavior fuel models developed for the rothermel surface fire spread model," in *In: Hutchinson, Todd F., ed. Proceedings of the 3rd fire in eastern oak forests conference; 2008 May 20-22; Carbondale, IL. Gen. Tech. Rep. NRS-P-46. Newtown Square, PA: US Department of Agriculture, Forest Service, Northern Research Station: 78-87.*, 2009.

[173] J.-L. Rossi, A. Simeoni, B. Moretti, and V. Leroy-Cancellieri, “An analytical model based on radiative heating for the determination of safety distances for wildland fires,” *Fire Safety Journal*, vol. 46, no. 8, pp. 520–527, 2011.

[174] M. E. Baran and F. F. Wu, “Network reconfiguration in distribution systems for loss reduction and load balancing,” *IEEE Trans. on Power delivery*, vol. 4, no. 2, pp. 1401–1407, 1989.

[175] E. Vugrin, A. Castillo, and C. Silva-Monroy, “Resilience metrics for the electric power system: A performance-based approach,” *Report: SAND2017-1493*, 2017.

[176] R. M. Houtman, C. A. Montgomery, A. R. Gagnon, D. E. Calkin, T. G. Dietterich, S. McGregor, and M. Crowley, “Allowing a wildfire to burn: estimating the effect on future fire suppression costs,” *International Journal of Wildland Fire*, vol. 22, no. 7, pp. 871–882, 2013.

[177] A. Jaafari, E. K. Zenner, and B. T. Pham, “Wildfire spatial pattern analysis in the zagros mountains, iran: A comparative study of decision tree based classifiers,” *Ecological informatics*, vol. 43, pp. 200–211, 2018.

[178] M. Rodrigues, A. Jiménez-Ruano, D. Peña-Angulo, and J. De la Riva, “A comprehensive spatial-temporal analysis of driving factors of human-caused wildfires in spain using geographically weighted logistic regression,” *Journal of environmental management*, vol. 225, pp. 177–192, 2018.

[179] CAL-FIRE, “2018 incident archive,” https://www.fire.ca.gov/incidents/2018/, [Online; accessed 26-August-2022].

[180] M. Calviño-Cancela, M. L. Chas-Amil, E. D. García-Martínez, and J. Touza, “Interacting effects of topography, vegetation, human activities and wildland-urban interfaces on wildfire ignition risk,” *Forest Ecology and Management*, vol. 397, pp. 10–17, 2017.

[181] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 770–778.

[182] S. Wan, Y. Liang, and Y. Zhang, "Deep convolutional neural networks for diabetic retinopathy detection by image classification," *Computers & Electrical Engineering*, vol. 72, pp. 274–282, 2018.

[183] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. MIT press, 2016.

[184] A. Umunnakwe, M. Parvania, H. Nguyen, J. D. Horel, and K. R. Davis, "Data-driven spatio-temporal analysis of wildfire risk to power systems operation," 2020.

[185] M. M. Hosseini, A. Umunnakwe, M. Parvania, and T. Tasdizen, "Intelligent damage classification and estimation in power distribution poles using unmanned aerial vehicles and convolutional neural networks," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3325–3333, 2020.

[186] L. Matikainen, M. Lehtomäki, E. Ahokas, J. Hyyppä, M. Karjalainen, A. Jaakkola, A. Kukko, and T. Heinonen, "Remote sensing methods for power line corridor surveys," *ISPRS Journal of Photogrammetry and Remote sensing*, vol. 119, pp. 10–31, 2016.

[187] J. Beraldin, F. Blais, and U. Lohr, "Laser scanning technology," *Airborne and terrestrial laser scanning*, pp. 1–42, 2010.

[188] Landsat, "Landsat science," https://landsat.gsfc.nasa.gov/data/data-details/, [Online; accessed 29-March-2022].

[189] MODIS, "Modis," https://modis.gsfc.nasa.gov/data/, [Online; accessed 29-March-2022].

[190] A. Rango, A. Laliberte, J. E. Herrick, C. Winters, K. Havstad, C. Steele, and D. Browning, "Unmanned aerial vehicle-based remote sensing for rangeland assessment, monitoring, and management," *Journal of Applied Remote Sensing*, vol. 3, no. 1, p. 033542, 2009.

[191] I. Lee, B. Welsh, and C. Miller, “nasa-wildfires,” https://github.com/datadesk/nasa-wildfires, 2022.

[192] AI for Mankind and W. S. Chung, “wildfire-dataset,” https://github.com/aiformankind/wildfire-dataset, 2019.

[193] O.-S. Younes, “Wildfires,” https://github.com/ouladsayadyounes/WildFires, 2018.

[194] L. Purcell, “Trees and electric lines,” https://extension.purdue.edu/extmedia/FNR/FNR-512-W.pdf.

[195] Eversource, “Understanding vegetation management: Balancing natural beauty with reliable electric service,” https://www.eversource.com/content/docs/default-source/my-account/veg-mgmt-guide.pdf, [Online; accessed 17-April-2023].

[196] Texas Wildfire Mitigation Project, “Reducing the risk of wildfires caused by power lines,” https://wildfiremitigation.tees.tamus.edu/faqs/how-power-lines-cause-wildfires.

[197] A. Alvarado, “Pole inspection guidelines,” *CPS Energy Work Instructions*, pp. 1–36, 2017.

[198] J. Bergstra and Y. Bengio, “Random search for hyper-parameter optimization.” *Journal of machine learning research*, vol. 13, no. 2, 2012.

[199] ENR, “Detecting wildfires,” https://www.enr.gov.nt.ca/en/services/wildfire-operations/detecting-wildfire, [Online; accessed 31-March-2022].

[200] J. Marder, “Nasa tracks wildfires from above to aid firefighters below,” https://www.nasa.gov/feature/goddard/2019/nasa-tracks-wildfires-from-above-to-aid-firefighters-below, 2019, [Online; accessed 29-March-2022].

[201] S. Zhao, B. Li, W. Zhang, H. Wu, and T. Feng, “Research on performance requirements of turbofan engine used on carrier-based uav,” in *AIP Conference Proceedings*, vol. 1839, no. 1. AIP Publishing LLC, 2017, p. 020010.

[202] R. Ahluwalia, J.-K. Peng, X. Wang, D. Papadias, and J. Kopasz, “Performance and cost of fuel cells for urban air mobility,” *International Journal of Hydrogen Energy*, vol. 46, no. 74, pp. 36 917–36 929, 2021.

[203] J. Jackson, K. Ladino, and G. Abdulai, “Decision aid for estimating the cost of using a drone in production agriculture,” *University of Kentucky College of Agriculture,Food and Environment Cooperative Extension Service*, pp. 1–9, 2021.

[204] R. Matthey, “PG&E potentially started the same amount of fires in 2021 than they did in 2020 altogether,” https://krcrtv.com/news/local/pge-potentially-started-the-same-amount-of-fires-in-2021-than-they-did-in-2020-altogether, 2021, [Online; accessed 29-March-2022].

[205] I. Penn, “PG&E Faces Criminal Charges Over Fatal 2020 Wildfire in California,” https://www.nytimes.com/2021/09/24/business/pge-wildfire-criminal-charges.html, 2021, [Online; accessed 29-March-2022].

[206] USDA, “People working in fire,” https://www.fs.usda.gov/science-technology/fire/people, [Online; accessed 29-March-2022].

[207] B. Daley, “What it takes to put out forest fires,” https://theconversation.com/what-it-takes-to-put-out-forest-fires-122644, 2019, [Online; accessed 29-March-2022].

[208] Texas A&M University System Communications staff, “California utility expands use of texas a&m wildfire prevention system,” https://today.tamu.edu/2021/09/20/california-utility-expands-use-of-texas-am-wildfire-prevention-system/, [Online; accessed 1-April-2022].

[209] Vigilys, “Wildfire detection,” https://vigilys.com/technology/firealert/, [Online; accessed 8-March-2023].

[210] Lindsey Firesense, “The firebird device,” https://lindsey-firesense.com/tour/, [Online; accessed 2-March-2023].

[211] P. Roy, “Data for the ieee 24 bus reliability test system,” https://www.academia.edu/13981064/Data_for_the_IEEE_24_bus_Reliability_Test_System, [Online; accessed 17-April-2023].

[212] K. Carbon and B. DAgostino, “Catastrophic risk mitigation through analytics: Wildfire threat index,” Sempra Energy and San Diego Gas & Electric, Tech. Rep., 2015.

[213] SDG&E, “San diego gas & electric company fire prevention plan,” *https://www.sdge.com/sites/default/files/regulatory/SDGE_Fire_Prevention_Plan_2018.pdf*, [Online; accessed 17-April-2023].

APPENDIX A

FIRST APPENDIX [*]

A.1 Spatial Features Details

We assume that land-use data contains information on fuel type, fuel load, fuel continuity as illustrated in Table 5.1 while terrain informs the topography of the ecoregion. The land-use and terrain are examples of spatial features and usually do not change significantly over the short-term, hence the name static. Land-use refers to the natural vegetation and the various ways in which humans make use of and manage the land and its resources. The terrain represents the topography of the geographical area. Hence, input features employed are not exhaustive but motivated from wildfire studies.

A.2 Same Climate Assumption

In this work, we assume same climate distribution over the period which we collect historical data for analysis. This assumption is enabled by similar distribution in spatial and temporal data. In the said period, the later is approximately Gaussian, while the former is as furnished in Fig. A.1.

A.3 Spatio-Temporal Wildfire Estimation Model: Setup

Landuse was obtained from the NOAA's HRRR model and ranges from evergreen needleleaf forest to barren tundra, assigned values [1, 20], while Terrain input gives insight into the topography and elevation of the area with values in the range [6, 2603] meters as shown in Fig. A.2. Temporal variables were obtained from the Open Weather Map database by building an application programming interface scrapper in python, to make data requests to the open weather map online weather database using the *http* protocol. Requested meteorological data includes tem-

[*] ©[2021] IEEE. Reprinted, with permission from, Umunnakwe A, Parvania M, Nguyen H, Horel JD, Davis KR., "Data-driven spatio-temporal analysis of wildfire risk to power systems operation," in IET Generation, Transmission & Distribution, vol. 16, no. 13, pp. 2531-46, Jul 2022, doi: https://doi.org/10.1049/gtd2.12463 [133].

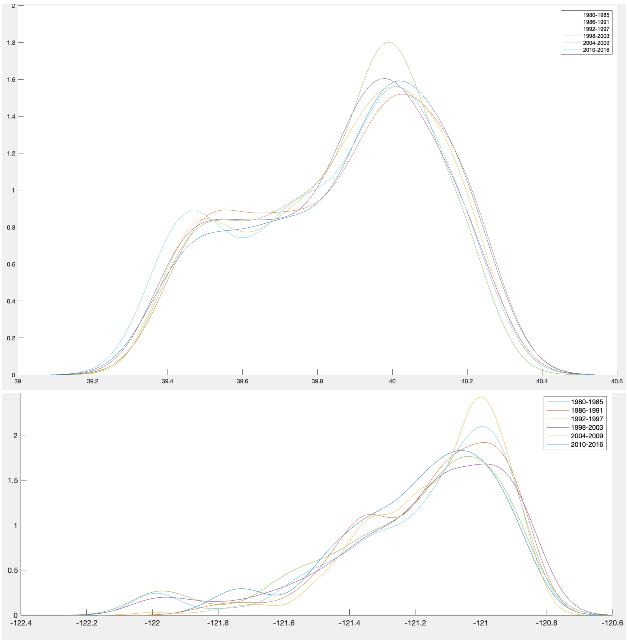


Figure A.1: Same Climate Assumption: Similar distribution of Historical data-points Latitude and Longitude.

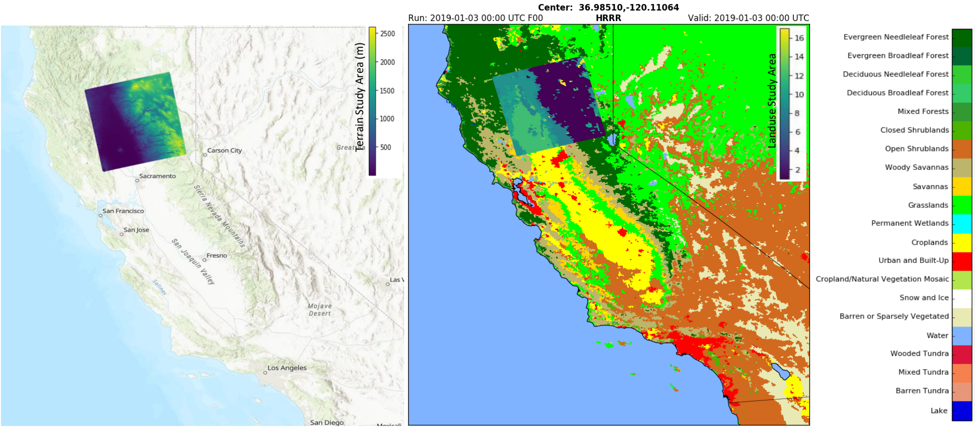


Figure A.2: The spatial features of studied geographical area: terrain (left) and land-use (right)

perature levels, rain, humidity, cloud, atmospheric pressure, visibility, month and sunshine hours, where numerical values are assigned to qualitative features, for instance, the daily weather types (clear, cloudy, hazy, drizzly, rainy) are assigned real values in the ratio [0.1, 0.3, 0.5, 0.7, 0.8] respectively. Historical wildfire ignition records were obtained for the multi-year period of analysis

(1996-2016,2018) from the U.S. Geographical Survey database and provides the samples of the training and test data, respectively.

A.4 Temporal Probability Details

The temporal probabilities of wildfire ignition is also calculated from historical data with the assumption of a same climate period as shown in Fig.A.3.

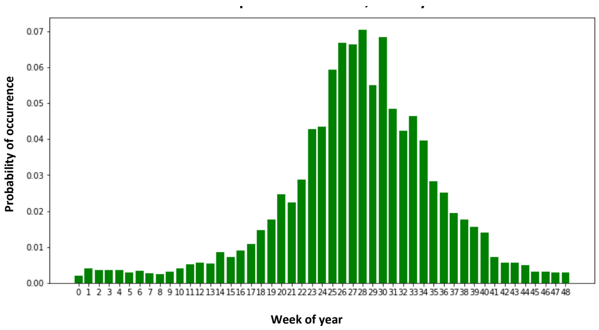


Figure A.3: Weekly Temporal Distribution of Historical Wildfire Occurrence

A.5 The STWIP Algorithm

The trained STWIP, as presented in Algorithm 6, is then validated and utilized in the prediction for unlabelled test samples for a future period j. When the algorithm ends, the probability map of potential ignitions, $\pi_{i,j}$, is returned.

A.6 Mapping Bulk Power Grid to the Wildfire Potential Map

The IEEE 24-bus reliability test system [211] that includes 24 buses, 38 lines and 33 generating units is aligned to the ignition probability map as shown in Fig. A.4. Also, to illustrate conventional power utility wildfire practices, the grid is divided into fire threat areas with extreme, elevated, and normal threat levels, while spatio-temporal analysis employs the most probable generated scenarios.

Algorithm 6 Batch Learning Based STWIP

```
Given a training set $(\mathbf{x}_1, y_1), ..., (\mathbf{x}_n, y_n)$ with features in instances $\mathbf{x}_i \in R^n$, with label $y_i \in \{0, 1\}$
Input(X,Y): A set of labeled input features [temp, ..., month], of training samples $\theta$, batch size $b$
Output: The spatio-temporal ignition probability maps.
Hyper-parameter selection
function $Predictor\_Training$(X, Y)
    Shuffle $\leftarrow$enabled
    count_max $\leftarrow \frac{\theta}{b}$
    count $\leftarrow 0$
    while count $<$ count_max do
        for batch $b$ in $\theta$ do
            STWIP $\leftarrow$ DNN learns ($b\times$[temp, ..., month])
            count $++$
        end for
    end while
    Compute accuracies
    Compute the ROC AUC metrics
    Apply STWIP to test samples
return Wildfire potential ignition maps of $\pi_{i,j}$
end function
```

A.6.1 Utility-Employed Predefined Fire Threat Areas and Levels

Electric power utilities have carried out ground breaking work in modeling wildfire occurrence, including developing analytical tools such as the Fire Potential Index (FPI) and more [212]. These indices, for instance the FPI, calculated at district level corresponding to three levels of wildfire threat alert, are efficient for planning decisions, however, they start to fall short in the day to day operational decisions for utilities as spatio-temporal granularity is lost in these methods i.e., the use of pre-defined wide threat areas and few (extreme, elevated, normal) threat levels.

In particular, the challenges posed by current utility techniques include the use of Fire Threat Areas (FTAs), Fire Threat Levels (FTLs), the independent analysis of the Wildfire Predictor Variables (WPVs), and the exclusion of adequate past wildfire characteristics in analysis. As stated by Brian D'Agostino, SDGE's director of fire science and climate adaptation: "We need to understand what the weather is doing in every canyon, every ridgetop all across the backcountry to really bring that level of customer safety and customer service". Thus, the use of FTAs and FTLs can introduce ambiguity in utility analysis, such as the over allocation of resources, excess load shedding

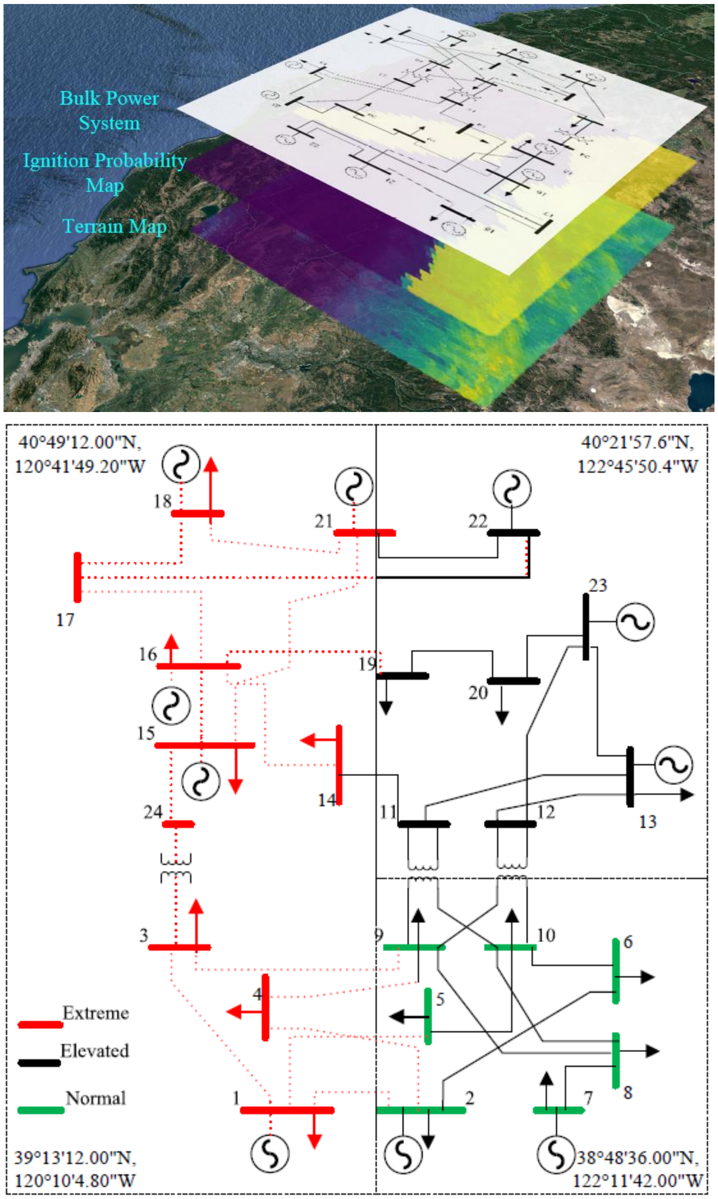
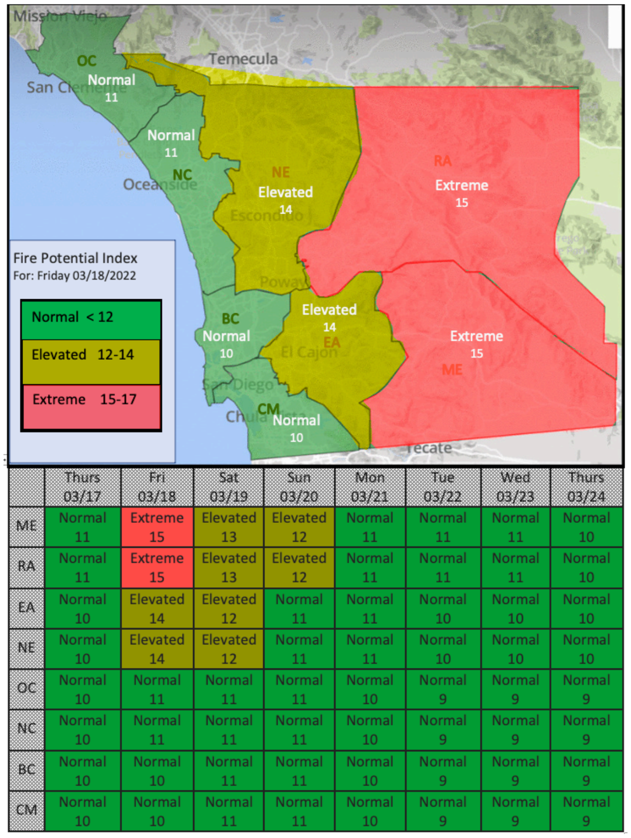

Bulk Power System
Ignition Probability Map
Terrain Map
40°49'12.00"N, 120°41'49.20"W
40°21'57.6"N, 122°45'50.4"W
39°13'12.00"N, 120°10'4.80"W
38°48'36.00"N, 122°11'42.00"W
18
21
22
17
23
16
19
20
15
14
11
12
13
24
3
9
10
6
4
5
8
7
1
2
Extreme
Elevated
Normal

Figure A.4: IEEE 24-bus mapping into three wildfire threat areas

in risk assessment, and lengthened forced outages to customers, since the pre-defined area may not be granular enough for operational wildfire analysis. Furthermore, the independent analysis of wildfire predictor variables introduces errors in estimation due to the exclusion of the effects of the interactions between these variables. For instance, for utility operations, when certain conditions (e.g., relative humidity $\leq 15\%$, sustained winds and gusts $\geq$ 25mph and 35 mph respectively, for



	Thurs 03/17	Fri 03/18	Sat 03/19	Sun 03/20	Mon 03/21	Tue 03/22	Wed 03/23	Thurs 03/24
ME	Normal 11	Extreme 15	Elevated 13	Elevated 12	Normal 11	Normal 11	Normal 11	Normal 10
RA	Normal 11	Extreme 15	Elevated 13	Elevated 12	Normal 11	Normal 11	Normal 11	Normal 10
EA	Normal 10	Elevated 14	Elevated 12	Normal 11	Normal 11	Normal 10	Normal 10	Normal 10
NE	Normal 10	Elevated 14	Elevated 12	Normal 11	Normal 11	Normal 10	Normal 10	Normal 10
OC	Normal 10	Normal 11	Normal 11	Normal 11	Normal 10	Normal 9	Normal 9	Normal 9
NC	Normal 10	Normal 11	Normal 11	Normal 11	Normal 10	Normal 9	Normal 9	Normal 9
BC	Normal 10	Normal 10	Normal 11	Normal 11	Normal 10	Normal 9	Normal 9	Normal 9
CM	Normal 10	Normal 10	Normal 11	Normal 11	Normal 10	Normal 9	Normal 9	Normal 9

Figure A.5: A sample SDG&E wildfire awareness issue

a duration $\geq$ 6 hours) are met, operational decisions e.g., all reclosers being turned off, sensitive relay settings being enabled [213], are taken. However, these assessments of environmental conditions are made independently, leaving little room for evaluating how the interactions between variables drive wildfire potential. Moreover, data obtained from historic events provide increased information on spatial wildfire characteristics as demonstrated in this work.