2024-03

MACHINE LEARNING METHOD TO OPTIMIZE TARGETING OF PHYSICAL NETWORK WITH STOCHASTIC OUTCOME

Chan, Xian Kai

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/72690

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MACHINE LEARNING METHOD TO OPTIMIZE TARGETING OF PHYSICAL NETWORK WITH STOCHASTIC OUTCOME

by

Xian Kai Chan

March 2024

Thesis Advisor:	Ruriko Yoshida
Co-Advisor:	Jefferson Huang
Second Reader:	Javier Salmeron-Medrano

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2024	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE MACHINE LEARNING METHOD TO OPTIMIZE TARGETING OF PHYSICAL NETWORK WITH STOCHASTIC OUTCOME	**5. FUNDING NUMBERS**
6. AUTHOR(S) Xian Kai Chan	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Physical network infrastructure transporting resources, such as fuel, electricity and water, are critical to the survivability of a nation. These infrastructures could be attractive targets for the adversary. One such attempt could be launching of artilleries to interdict these networks. Such an attack is stochastic with certain probability of kill on the arcs subjected to different errors. A defender would want to ensure that the critical networks are robust against such interdictions. While arcs of the physical network may not appear physically connected, they can often be situated close to each other geographically; a single attack may simultaneously disrupt multiple arcs. Therefore, analyzing only the network's physical connectivity, without considering the geographical dependencies of the arcs, could lead to an overly optimistic assessment of the network's robustness. One way to analyze the robustness of the network would be to assume the role of an attacker with full knowledge of the network infrastructure. The attacker would identify aim points to target the network with the objective of minimizing the expected maximum flow of resources from the source to sink. The objective of the thesis is to investigate the potential of utilizing machine learning methods to discern sets of viable aim points that can effectively fulfill the attacker's goal. The trained model achieved an accuracy of 85%, indicating a promising foundation for further enhancements in future iterations.

14. SUBJECT TERMS stochastic, network interdiction, machine learning	**15. NUMBER OF PAGES** 63
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

MACHINE LEARNING METHOD TO OPTIMIZE TARGETING OF PHYSICAL NETWORK WITH STOCHASTIC OUTCOME

Xian Kai Chan
Civilian, DSO National Laboratories
BS, Nanyang Technological University, 2015

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL
March 2024

Approved by: Ruriko Yoshida
Advisor

Jefferson Huang
Co-Advisor

Javier Salmeron-Medrano
Second Reader

W. Matthew Carlyle
Chair, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Physical network infrastructure transporting resources, such as fuel, electricity and water, are critical to the survivability of a nation. These infrastructures could be attractive targets for the adversary. One such attempt could be launching of artilleries to interdict these networks. Such an attack is stochastic with certain probability of kill on the arcs subjected to different errors. A defender would want to ensure that the critical networks are robust against such interdictions. While arcs of the physical network may not appear physically connected, they can often be situated close to each other geographically; a single attack may simultaneously disrupt multiple arcs. Therefore, analyzing only the network's physical connectivity, without considering the geographical dependencies of the arcs, could lead to an overly optimistic assessment of the network's robustness. One way to analyze the robustness of the network would be to assume the role of an attacker with full knowledge of the network infrastructure. The attacker would identify aim points to target the network with the objective of minimizing the expected maximum flow of resources from the source to sink. The objective of the thesis is to investigate the potential of utilizing machine learning methods to discern sets of viable aim points that can effectively fulfill the attacker's goal. The trained model achieved an accuracy of 85%, indicating a promising foundation for further enhancements in future iterations.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

CEP	circular error probable
ILP	integer linear program
MLBA	machine learning based approach
MPI	mean point of impact
MOE	measure of effectiveness
OSM	OpenStreetMap
POI	point of impact
SNIP	stochastic network interdiction problem

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

Physical network infrastructures that facilitate the transportation of vital resources, including fuel, electricity, and water, play a crucial role in a nation's resilience. These infrastructures are susceptible to potential threats from adversaries, making them attractive targets. One method of attack involves the use of artillery to disrupt these networks. An artillery attack can involve the launch of multiple rockets aimed at single or multiple targets. The attack can be modelled as a stochastic event, with a certain probability of success, influenced by factors such as the accuracy of the weapons used. A defender must ensure that critical networks are resilient against such interdictions to safeguard against potential disruptions.

Traditional approaches to analyzing network interdiction often entail the removal of individual arcs to evaluate their impact on the overall flow from the source to the sink. However, this methodology may not be directly applicable to physical networks. While schematic representations may not reveal apparent connectivity among arcs, reality often portrays a different scenario, where arcs are closely situated geographically due to spatial constraints. This geographic proximity introduces a unique challenge, as an artillery attack has the potential to simultaneously disrupt multiple arcs. Thus, conducting an analysis solely based on the network's physical connectivity, without accounting for the geographic interdependencies of the arcs, may result in an overly optimistic assessment of the network's robustness.

Drawing inspiration from the machine learning based approach (MLBA) proposed by Orkun Baycik (2022), we created a decision tree model to assess the resilience of physical networks. The objective of the model was to identify location to attack that would result in the lowest maximum flow from the source to sink in a network. The novel approach involved generating networks with 10 to 50 nodes, intricately connected in a random fashion. The networks were divided into 9×9 grids. For each grid, Monte Carlo simulations were conducted to simulate artillery attacks at the grid center, and the resulting maximum flows were recorded. Features, encompassing neighboring grid characteristics and key network metrics, were extracted for model training. The response variable was the ratio of maximum flow post-attack to pre-attack. Total of 1500 networks were generated; 1000 networks were used to generate training data, yielding total of 8100 data points, remaining 500 networks were used as test data.

A decision tree model was trained using a machine learning library in Python, Scikit-learn (Pedregosa et al. 2011). It exhibited total depth of 34 and underwent 22936 splits during the training process. The model correctly predicted the optimal grid to target for 427 out of 500 test networks, achieving accuracy of 85%.

In evaluating the model's performance, it was imperative to highlight a key aspect influencing its predictions—the importance score assigned to each feature. This score played a pivotal role in guiding the model's decision-making process. Notably, our model exhibited a heightened emphasis on the number of arcs within the target grid, as indicated by the importance scores extracted. This specific emphasis on arc counts could introduce potential inaccuracies. For example, the model predicted a low maximum flow to a grid with a significant number of arcs, even when the impact on obstructing the flow from source to sink is negligible. To address this, future studies may require engineering of more extensive feature set.

The model, functioning as a proof-of-concept, demonstrated promising outcomes in identifying the optimal target grid to minimize the maximum flow within a network. However, recognizing its potential application in real-world scenarios entails acknowledging certain limitations. Notably, the current model may benefit from enhancements to address scenarios involving the simultaneous targeting of multiple areas. Future iterations could involve exploring alternative modeling techniques for refining and extending the model's capabilities in this domain.

List of References

Orkun Baycik N (2022) Machine learning based approaches to solve the maximum flow network interdiction problem. *Computers & Industrial Engineering* 167:107873, https://doi.org/10.1016/j.cie.2021.107873.

Pedregosa F, Varoquaux G, Gramfort A, Michel V, Thirion B, Grisel O, Blondel M, *et al.* (2011) Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research* 12:2825–2830.

Acknowledgments

I would like to extend my heartfelt appreciation to my co-advisors, Dr. Ruriko Yoshida and Dr. Jefferson Huang, for their invaluable insights and patient guidance throughout the entire process. I am also grateful to Dr. Javier Salmeron for his knowledge and expertise on the subject, and providing critical inputs for my research.

I would like to express my gratitude to my friends I made during the 18 months of my studies. They have provided me invaluable advice throughout the journey. I would have been lost without their support.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1: Introduction

1.1 Background

Physical network infrastructures that facilitate the transportation of vital resources, including fuel, electricity, and water, play a crucial role in a nation's resilience. These infrastructures are susceptible to potential threats from adversaries, making them attractive targets. One method of attack involves the use of artillery to disrupt these networks. For example, in 2021, a rocket attack was launched by the Islamic State, targeting an Iraqi power station, Salah al Din Thermal Power Station (Reuters 2021). The power station has a load of 1,260 MW of power (SyriacPress 2021). Such attacks have the potential to cause significant disruptions, leading to power outages and economic damage. Mao Shuai et al. (2018) estimated that a load loss of 8000 MW of power could cause an economic loss of $60 million; Electricity Consumers Resource Council (2004) estimated that load loss of 61,800 MW resulted in economic loss between seven and ten billion of dollars.

An artillery attack can involve the launch of multiple rockets aimed at single or multiple targets. The attack can be modelled as a stochastic event, with a certain probability of success, influenced by factors such as the accuracy of the weapons used. A defender must ensure that critical networks are resilient against such interdictions to safeguard against potential disruptions.

1.2 Problem Statement

Traditional approaches to analyzing network interdiction often entail the removal of individual arcs to evaluate their impact on the overall flow from the source to the sink. However, this methodology may not be directly applicable to physical networks. While schematic representations may not reveal apparent connectivity among arcs, reality often portrays a different scenario, where arcs are closely situated geographically due to spatial constraints. An illustrative example is presented in Figure 1.1, where the substation is denoted by the blue box, and power lines are depicted as light blue lines. Despite some power lines appearing unconnected to the substation, their routing patterns reveal geographical proximity, emphasizing the interdependency created by the criss-crossing of multiple power lines.

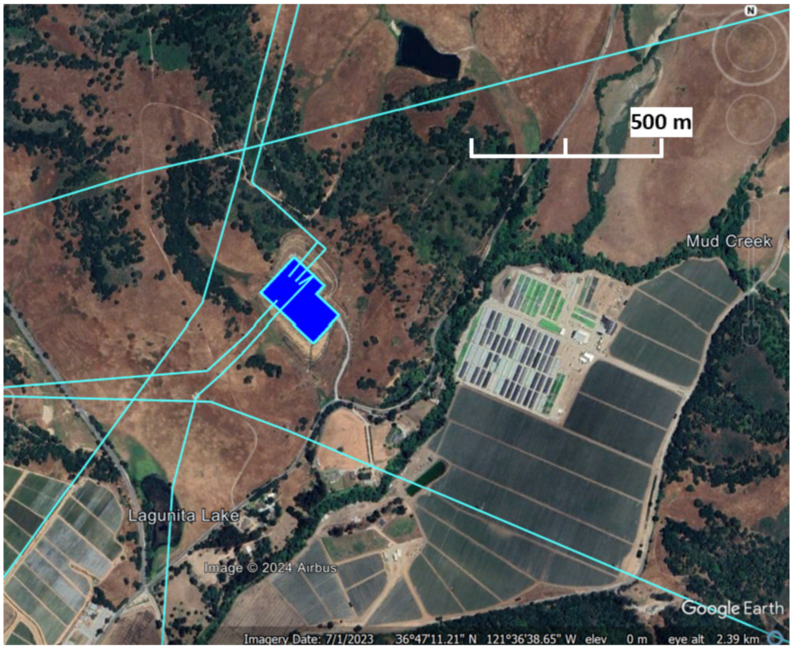

N
500 m
Mud Creek
Lagunita Lake
Image © 2024 Airbus
Google Earth
Imagery Date: 7/1/2023 36°47'11.21" N 121°36'38.65" W elev 0 m eye alt 2.39 km

Figure 1.1. Figure shows an example of geographical routing of electrical power network. The substation is represented by the blue box, and the power lines are highlighted as light blue lines. The criss-crossing of multiple power lines highlights the interdependencies among these lines.

This geographical proximity introduces a unique challenge, as an artillery attack has the potential to simultaneously disrupt multiple arcs. Consequently, networks that may appear to possess significant physical redundancy could, in fact, be geographically dependent. Thus, conducting an analysis solely based on the network's physical connectivity, without accounting for the geographic interdependencies of the arcs, may result in an overly optimistic assessment of the network's robustness.

1.3 Approach

We analyze the robustness of the network by assuming the role of an attacker with full knowledge of the network infrastructure. The attacker would identify aim points to target the network with the objective of minimizing the expected maximum flow of resources from the source to sink. A robust network would exhibit a minimal reduction in the maximum flow compared to its state before the disruption occurred. Chapter 3 provides details on the methodology.

1.4 Thesis Outline

This thesis comprises five chapters. The second chapter delves into review of relevant literature, exploring methodologies employed by similar studies. The third chapter provides an in-depth explanation of the methodology adopted in this thesis. In the fourth chapter, the results of the research are presented and analyzed. Finally, the fifth chapter serves as the conclusion, summarizing the key findings and insights obtained throughout the thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2:
Literature Review

2.1 Artillery Attacks

2.1.1 Weapon Delivery Errors

One of the key considerations of the thesis is the stochastic nature of the artillery attack. Artillery firing is associated with three primary types of errors in weapon delivery: fixed bias error, mean point of impact (MPI) error, and precision error. Lim (2016) provides explanation on each type of error. Fixed bias error is a consistent error present in every firing, which may be due to error in the weapon system's calibration. MPI error is the error that remains constant within a firing occasion, but may differ in another occasion. The change in occasion may be due to change in firing position. Precision error is a random error that varies based on a distribution away from the mean point of impact. This could be caused by the randomness in ammunition dispersion. Figure 2.1 illustrates the difference between MPI and precision errors. For simplicity, this thesis focuses on the precision error.

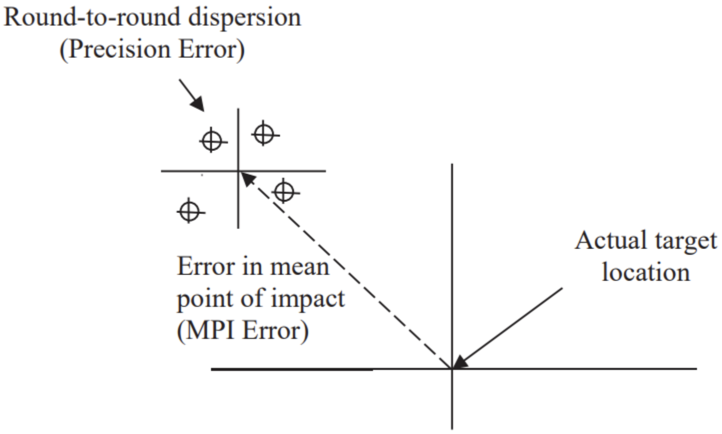


Figure 2.1. Illustration of MPI and precision errors in a single firing occasion. MPI error is fixed and causes rounds to be away from the actual target location. Precision error are random around the point of impact after accounting for MPI error. Source: Lim (2016).

2.1.2 Precision Error

The precision error can be simulated using Monte Carlo simulation, with the errors for the coordinates (latitude and longitude) following Gaussian distribution. A common error measure that is used is the circular error probable (CEP). When the CEP is stated to be 50m, it indicates that 50% of the rounds would land within 50m of the point of impact (POI) after accounting for the MPI.

2.2 Physical Network

In pursuit of the thesis objective to identify optimal locations for minimizing maximum flow within a physical network, we leverage insights on the geographical layout of power networks. These insights guide the artificial generation of sample networks, which we utilize as data points for our modeling. This section delves into the key features of power networks that we reference in the thesis.

2.2.1 Power Network

The power network comprises three essential layers: generation, transmission, and distribution. Figure 2.2 illustrates the components of the electrical power grid. While voltage levels of the electrical grid may vary among different countries, the overall process of power generation, transmission, and distribution to end-users remains largely consistent. Power generation occurs at various plants, utilizing diverse sources such as coal, hydroelectric, nuclear, and wind power. Following generation, the power undergoes a voltage step-up process at a substation, denoted by two overlapping circles in the figure. Subsequently, the high-voltage power travels through transmission lines covering extended distances before undergoing a step-down process when nearing end-users. The final stage involves distribution to end-users through the distribution network. To scope the analyses, this thesis specifically focused on the transmission aspect of the power network.

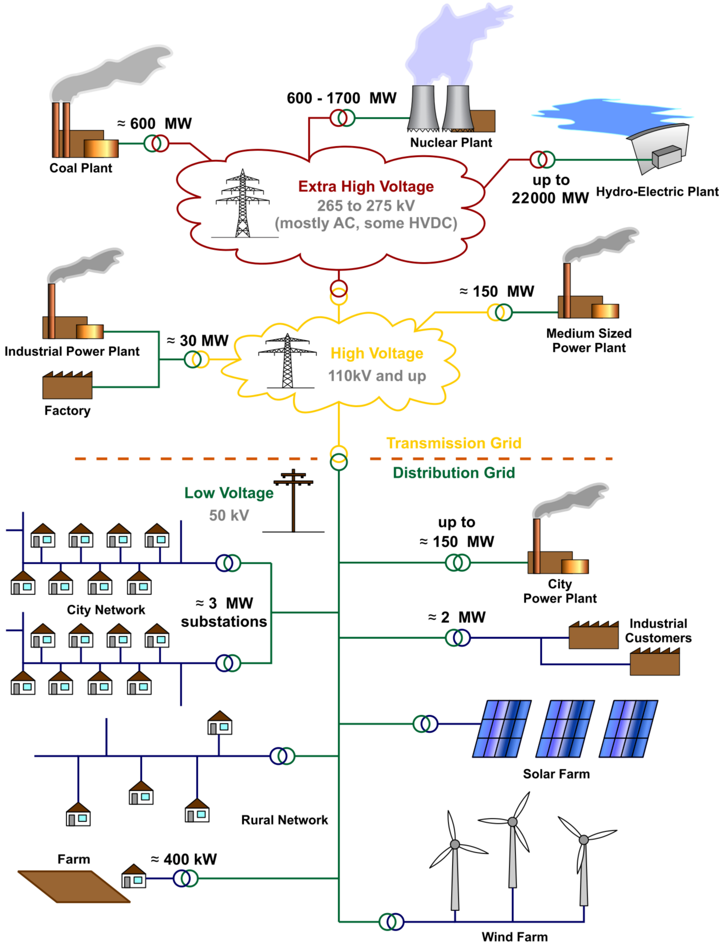


Figure 2.2. Electric power is generated at diverse plants using various sources, transmitted over long distances through the transmission network, then through the distribution network to reach end-users. Source: Electrical Grid (2024).

2.2.2 Geographical Dependency

There may be instances where arcs within a physical network exhibit geographical dependencies. For example, due to constraints on available corridors for setting up transmission towers, seemingly independent transmission lines may share geographical dependencies. To illustrate, Figure 2.3 shows the transmission lines connecting to the substation at Moss Landing, California. It can be observed that up to seven lines follow the same corridor as they approach the substation. This phenomenon of sharing corridors is not exclusive to power networks; for instance, under specific criteria, fuel pipelines might share the same corridor as transmission lines (Chan et al. 2022). This underscores the importance of considering geographical dependencies in the context of artillery attack scenarios for physical networks.

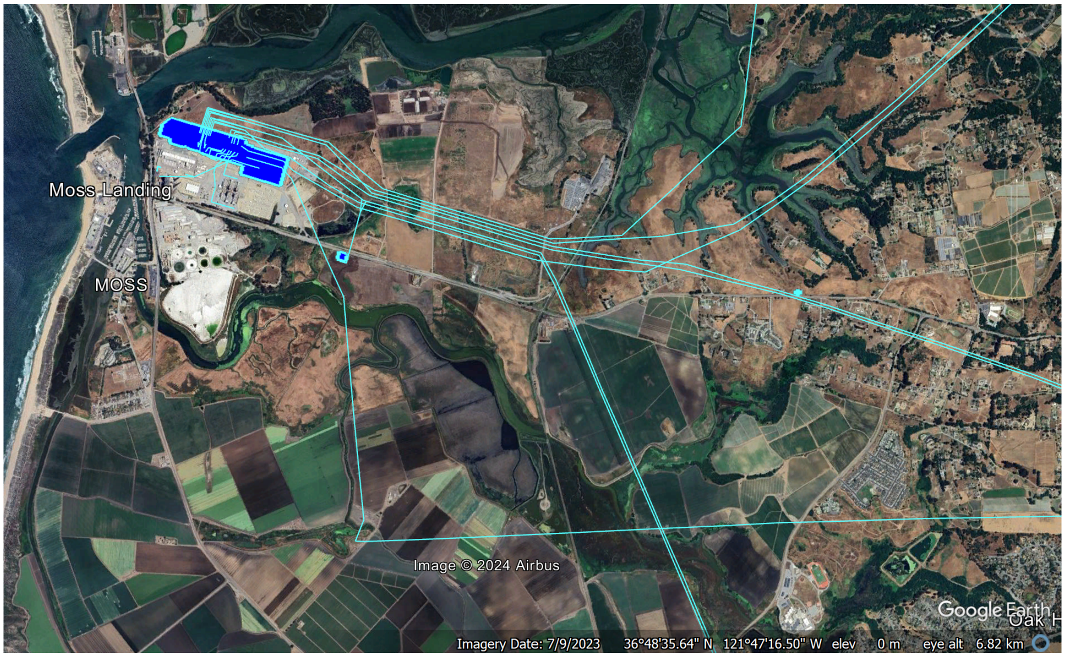

Moss Landing
MOSS
Image © 2024 Airbus
Google Earth
Imagery Date: 7/9/2023 36°48'35.64" N 121°47'16.50" W elev 0 m eye alt 6.82 km

Figure 2.3. Transmission lines connecting to the substation at Moss Landing, California, represented by blue block, showing geographical dependencies between power lines, represented by the light blue lines.

2.2.3 Assumptions on Physical Network

Interdicting physical networks, in particular power networks, requires careful consideration of their inherent physical attributes. Notably, in the context of network interdiction on power grids, Salmeron et al. (2009) explored physical characteristics like the series susceptance of power cables and the phase angle of the bus. However, for the purpose of this thesis, we opted for a substantial simplification, assuming that the interdiction of a specific arc does not impact the flow of resources along other arcs. Additionally, the assumption is made that the physical networks under consideration exhibit a tree-like structure, a characteristic often observed in the distribution networks of power networks.

2.3 Approaches to Solve Network Interdiction Problem

2.3.1 Max-flow Min-cut Theorem

The max-flow min-cut theorem proposed by Ford and Fulkerson (1962) establishes that the maximum flow through a network from source to sink is equal to the minimum capacity of a cut that separates the source from the sink. Essentially, the minimum cut represents the smallest total edge capacity needed to separate the source and sink. Therefore, given sufficient attack resource and assuming deterministic outcome of the attack, the solution to the network interdiction would be the set of arcs that forms the maximum flow from source to sink. Edmonds and Karp (1972) devised an algorithm that may be used to solve the maximum flow problem and obtain the set of arcs to cut. This forms a basis approach to solve a network interdiction problem. However, this approach does not account for the scenario in which the attack resources available are less than the number of cuts required.

2.3.2 Brute Force Method

The brute force method is the naïve approach to address the network interdiction problem. It systematically assesses all potential combinations of aim points to discern the most optimal interdiction strategy. Despite its conceptual simplicity, the brute force method encounters computational impracticality when applied to large networks due to the exponential increase in the number of combinations. This is especially so when aiming at geographical coordinates as the coordinates are tuples of continuous latitude and longitude values. This complexity underscores the need for more efficient and scalable strategies. The following subsections explore the use of integer linear program (ILP) and machine learning techniques to solve network interdiction problems.

2.3.3 Deterministic Network Interdiction Problem

Wood (1993) introduced ILP implementation to solve the deterministic network interdiction problem. The formulation for this problem is provided in (2.1). Wood has also provided other implementations to solve interdiction problems for networks with multiple sources and sinks, undirected networks, or networks with multiple resources. However, an alternative approach would be needed to solve interdiction problems with attacks that have stochastic outcomes.

Data:

R : Total attack resource to interdict arcs

r_{ij} : Units of resource required to interdict arc (i, j)

u_{ij} : Capacity of arc (i, j)

γ_{ij} : 1 if (i, j) is a forward arc across the cut to be broken

α_i : 1 if node i is on the t side of the cut

β_{ij} : 1 if (i, j) is a forward arc across the cut but it is not to be broken

Formulation:

$$\min \sum_{(i,j)\in A} u_{ij}\beta_{ij} \tag{2.1}$$

$$\begin{aligned}
\text{s.t.} \quad & \alpha_i - \alpha_j + \theta_{ij} \geq 0 && \forall (i,j) \in A \\
& \alpha_t - \alpha_s \geq 1 && \\
& \beta_{ij} + \gamma_{ij} - \theta_{ij} \geq 0 && \forall (i,j) \in A \\
& \sum_{(i,j)\in A} r_{ij}\gamma_{ij} \leq R && \\
& \alpha_i \in \{0,1\} && \forall i \in N \\
& \theta_{ij} \in \{0,1\} && \forall (i,j) \in A \\
& \beta_{ij}, \gamma_{ij} \in \{0,1\} && \forall (i,j) \in A.
\end{aligned}$$

2.3.4 Stochastic Network Interdiction Problem

The stochastic network interdiction problem (SNIP) is a variant of the network interdiction problem where the interdiction successes are uncertain. The objective of SNIP is to minimize the expected maximum flow by identifying the optimal set of arcs to target. Cormican et al. (1998) first illustrated the pitfall of using expected value together with deterministic network interdiction to solve the SNIP. Cormican et al. (1998) then provide a K-scenario minimization model (2.2) which would solve SNIP exactly. However, the problem becomes increasingly difficult to solve as the number of scenarios becomes larger. Therefore, Cormican et al. (1998) proposed a sequential approximation algorithm which approximately solve (2.2) via Benders decomposition.

Data:

A : Set of all arcs in network

A' : $A \cup \{(t, s)\}$

p^k : Probability of Scenario k occuring

α_{ij}^k : 1 if node i is on the t side of the cut, for Scenario k

u_{ij} : Capacity of arc (i, j)

π_i^k : Dual variable for conservation of flow for Node i in Scenario k

γ_{ij} : 1 if (i, j) is a forward arc across the cut to be broken

e_{ij} : 0 if $(i, j) \neq (t, s)$, and 1 if $(i, j) = (t, s)$

$\bar{I}_{ij}^k$: Indicator random variable that is 1 with probability p_{ij}
and 0 with probability $1 - p_{ij}$ for Scenario k

r_{ij} :Units of resource required to interdict arc (i, j) and

R : Total attack resource to interdict arcs

$$\Gamma : \left\{ \gamma \middle| \sum_{(i,j) \in A'} r_{ij}\gamma_{ij} \leq R, \gamma_{ij} \in 0, 1 \forall (i, j) \in A' \right\}, \text{ where } r_{t,s} = R + 1$$

Formulation:

$$\min_{\gamma,\pi,\alpha} \sum_{k=1}^{K} \sum_{(i,j)\in A'} p^k \alpha_{ij}^k u_{ij} \tag{2.2}$$

$$\begin{aligned}
\text{s.t.} \qquad & \pi_i^k - \pi_j^k + \alpha_{ij}^k + \bar{I}_{ij}^k \gamma_{ij} \geq e_{ij} && \forall k, (i,j) \in A', \\
& \alpha_{ij}^k \geq 0 && \forall k, (i,j) \in A', \gamma \in \Gamma.
\end{aligned}$$

While the approach is effective in selecting target arcs for disruption, it falls short in accounting for scenarios where multiple arcs may be affected by a single interdiction event. This limitation necessitates a deeper exploration of methodologies that can address such complexities. Additionally, the implementation of SNIP demands the generation of probabilities associated with arc disruption, a process that can be particularly time-consuming, especially when utilizing Monte Carlo simulations to simulate artillery attacks.

2.3.5 Machine Learning Method

In addressing the network interdiction problem, an innovative approach utilizes machine learning techniques, as presented by Orkun Baycik (2022). This method, termed machine learning based approach (MLBA), specifically targets the deterministic network interdiction problem within hierarchical network structures. The core of this methodology involves leveraging decision trees along with seven key features extracted from each network arc. These features encompass tail in-degree, tail out-degree, head in-degree, head out-degree, distance from the source node, distance from the sink node, and capacity ratio.

The creation of a labeled dataset follows a systematic process. Small network instances are generated, assigning random capacities to each arc within a range of one to 20. Subsequently, individual arcs are interdicted, and the network is iteratively solved to determine the maximum flow. Normalization of flow values is performed considering the solved maximum flow and the maximum flow before interdiction. The resulting dataset captures normalized total flow and the seven features.

Two models, a decision tree, and a random forest, are trained on this dataset. In testing against small network instances (up to 582 nodes and 1248 arcs), the decision tree model proves efficient, finding solutions within 0.6 seconds, while the random forest model achieves this within 17 seconds. However, model performance varies, with instances of optimal solutions and optimality gaps as high as 70%.

The MLBA's effectiveness shines particularly in large network instances (up to 56502 nodes and 268832 arcs). The decision tree and random forest models demonstrate exceptional speed, finding optimal solutions within 1.4 seconds and 21 seconds, respectively. In contrast, the integer linear program solver, CPLEX, may take considerably longer, from minutes to over an hour. However, the optimality gap increases with the interdiction budget, ranging from 0.1% to 73.6%.

There are numerous advantages for this approach, including short computation times, interpretability, and ease of implementation. Despite these strengths, it is essential to acknowledge potential trade-offs, where it may underperform in certain scenarios as compared with other methods. The robustness of MLBA across various network structures and its scalability for extremely large networks make it a compelling avenue for further exploration. Building on the success of MLBA in deterministic settings, this thesis aims to leverage similar machine learning techniques to address the stochastic network interdiction problem, incorporating considerations for geographical dependencies identified earlier.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3:
Methodology

This chapter describes the steps to generate data points for training of the machine learning model. The goal of the model is to predict the optimal target location to minimize maximum flow from source to sink.

3.1 Assumptions and Data Generation

In this section, we describe the assumptions used and procedure to generate labelled data set for training of machine learning model.

3.1.1 Challenge

One significant challenge in addressing the thesis problem is the availability of data. While open-source, crowdsourced data such as OpenStreetMap (OSM) is accessible, its crowdsourced nature necessitates thorough cleaning to rectify any broken network components that might introduce errors. For the application of machine learning techniques, a substantial volume of diverse networks is essential for training purposes. As a proof of concept on using MLBA to identify target locations, this thesis opts to generate artificial networks instead of relying on open-source data.

3.1.2 Study Parameters and Key Assumptions

Building on the observations of the geographical layout of power networks in Chapter 2, our approach involves generating artificial networks by incorporating a set of simplifying assumptions. This not only overcomes the limitations associated with incomplete data but also allows for more straightforward analyses, providing flexibility in crafting diverse scenarios for comprehensive machine learning training. Actual physical networks may be used to validate the model for future studies.

To facilitate generating of artificial networks and conducting of analyses, we used the following study parameters and key assumptions in this thesis:

1. Network is modelled as a tree;
2. There is only one source and one sink;
3. The source have more than sufficient supply to deliver to the sink, i.e., bottleneck is on the arcs;
4. Only arcs are destructible;
5. There is only one desired POI, and one weapon error with 20 rounds.

More details are provided in the subsequent sections of this chapter. These assumptions may be subsequently addressed in future work on similar topic.

3.1.3 Generating Artificial Network

In this section we describe the algorithm used to generate artificial networks that emulates the geographical layout observed in power networks. Given a set of nodes, $N = 1, 2, \ldots, n$, threshold value p, and bounding box of coordinates, consider the following algorithm:

1. Initialize $N = 1, 2, \ldots, n$ nodes by assigning each node a random coordinate (lat/lon) within the bounding box.
2. For each node $i \in N$,
    (a) Randomly assign arcs to other nodes $j \in N$ with probability p if $i < j$.
    (b) After assignment, identify the arc that has the shortest distance between nodes i and j. Remove other arcs.
    (c) Modify the arc into a random bi-direction path between nodes i and j.

The first step initializes each node randomly located within a specified area. Step 2a assigns the arcs connecting between each nodes with probability p. Step 2b prunes the arcs to convert the network into a tree, while ensuring minimal criss-crossing of arcs. Step 2c creates a random path between the two nodes to emulate a geographical path. Figure 3.1 shows an example of a network generated from the algorithm. The network consists of 20 nodes, constrained within the coordinates (36.65, -121.8) and (36.85, -121.6) or an area of approximately 22.2 km by 17.8 km.

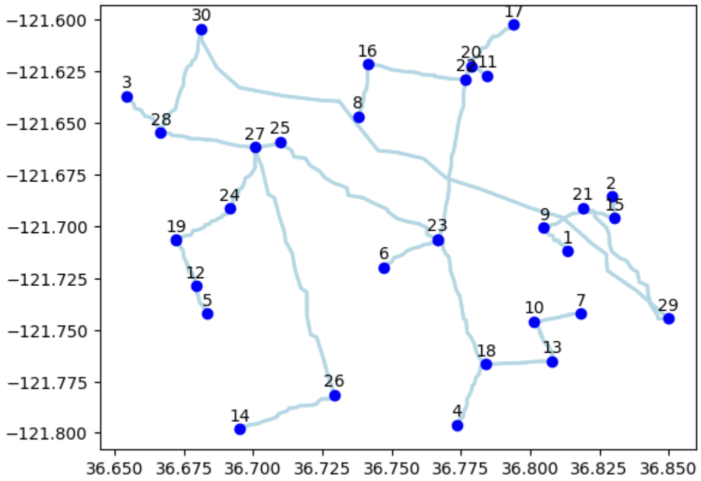


Figure 3.1. Example of network generated from algorithm. The network consists of 20 nodes, constrained within the coordinates (36.65, -121.8) and (36.85, -121.6) or an area of approximately 22.2 km by 17.8 km.

3.2 Evaluating Maximum Flow After Attack

3.2.1 Determine Arc is Destroyed

In reality, assessing the destruction of a structure involves multifaceted considerations, including factors such as the amount of explosives within the rounds fired from the weapon, the structural resilience of the target, and the POI of the round. To simplify and streamline the analysis, we adopt the assumption that an arc is considered destroyed based solely on the POI. Specifically, if the round lands within a certain distance from an arc, it is deemed destroyed. This approach allows us to focus on the spatial relationship between the round impact and the power network components.

Figures 3.2 and 3.3 visually illustrate the criteria for determining whether an arc is considered destroyed. In these figures, the orange point denotes the round's POI, while the red circle represents the 1000-meter radius around the POI. The arcs are deemed destroyed if the weapon lands within this radius. Figure 3.2 indicates a scenario where the round missed the arcs, while Figure 3.3 demonstrates the destruction of two arcs connecting nodes 9 and 21, and nodes 29 and 30. This example illustrates how a single round may destroy multiple arcs, emphasizing their geographical dependence.

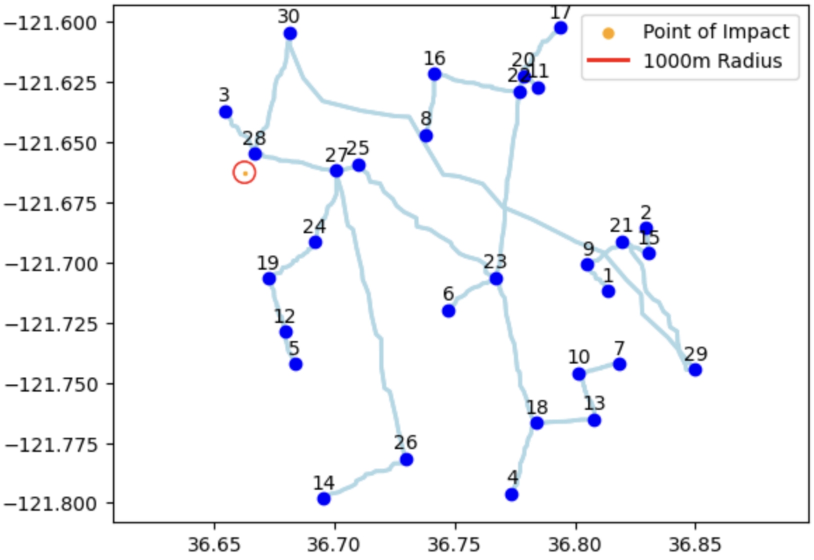


Figure 3.2. Example of no arc is destroyed. Orange point represents the POI of the round, and the red circle represents the 1000-meter radius around the POI. As the round landed more than 1000 meters away from the nearest arc, no arc is destroyed.

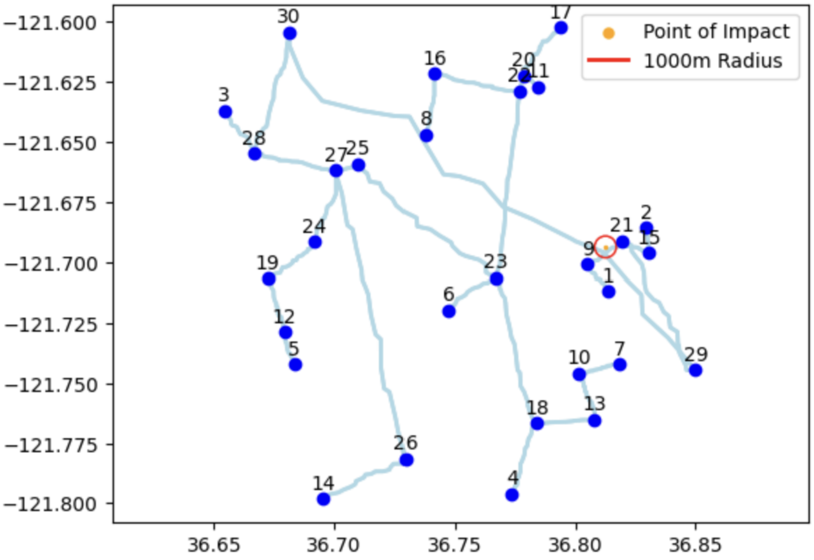


Figure 3.3. Example of multiple arcs are destroyed. Orange point represents the POI of the round, and the red circle represents the 1000-meter radius around the POI. The round landed within 1000 meters of two arcs, destroying the two arcs connecting nodes 9 and 21, and nodes 29 and 30.

An artillery attack may involve firing multiple rounds at the same desired POI. Figure 3.4 illustrates an example of an artillery attack pattern generated from 20 rounds using Monte Carlo simulation. Blue dots represent the POI of the rounds. 50%, 93%, and 99% of all rounds would land within the red circle, yellow circle, and black circle, respectively. Any one of the rounds landing within the specified distance in proximity to the arc results in the destruction of that arc.

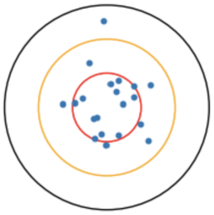


Figure 3.4. Monte Carlo Simulation of 20 rounds of a weapon with a CEP. Blue dots represent the POI of a weapon. 50%, 93%, and 99% of all rounds would land within the red circle, yellow circle, and black circle, respectively.

For this thesis, the artillery is assumed to fire 20 rounds with CEP of 1000 meters, and any rounds landing within 100 meters of the arc is considered destroyed. Figure 3.5 shows an example of a simulated attack on the generated network, where the arc connecting node 29 and node 30 is deemed destroyed.

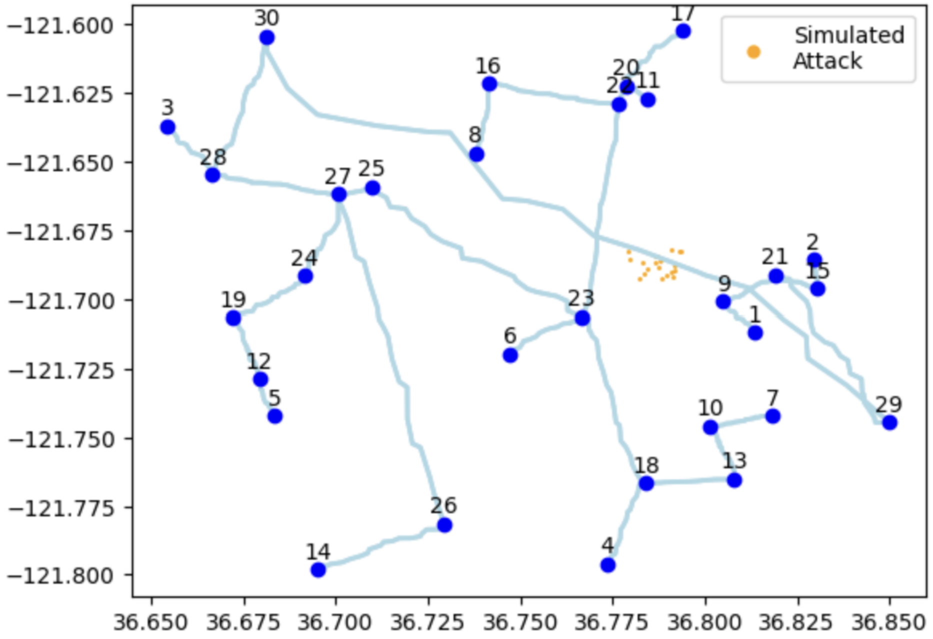


Figure 3.5. Simulated attack of 20 rounds from an artillery with CEP of 1000 meters. The orange nodes represents the POI of each round. Under this simulation, the arc connecting node 29 and node 30 is deemed destroyed.

3.3 Decision Tree Model

In this section we briefly describe the decision tree model which we used for our experiments and simulations.

3.3.1 Grid-based Feature Extraction

To facilitate the feature collection process of the network, a 9×9 grid division is employed. To calculate flow values, the first and last nodes of the network are designated as the source and sink nodes, respectively. Figure 3.6 illustrates a 30-node network with the grid layout, highlighting the source and sink nodes in red and green, respectively. In this figure, node 1 serves as the source, and node 30 functions as the sink.

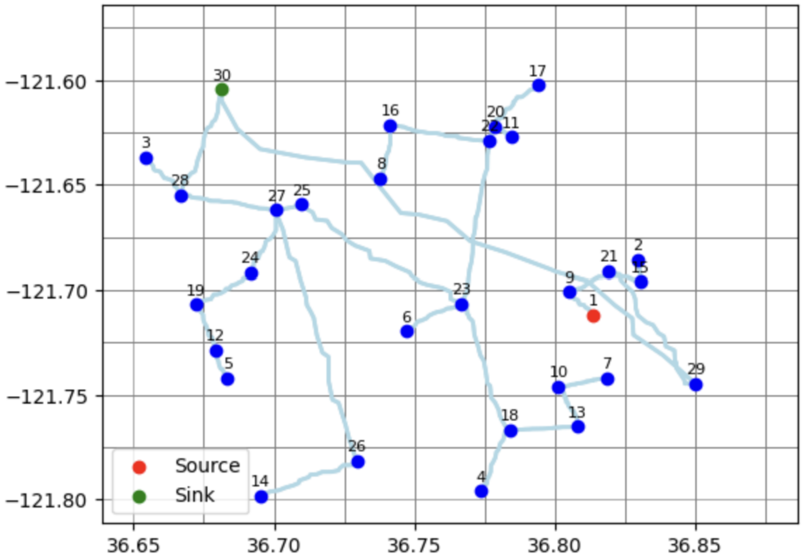


Figure 3.6. Network with Grid. The first and last nodes of the network are chosen to be the source and sink nodes, and are highlighted in red and green, respectively.

For each grid, a set of features is collected to serve as the training data for the decision tree model. The following list summarizes these features:

1. Number of arcs (|A|);
2. Number of nodes (|N|);
3. Number of arcs in-between the source and sink (B); and
4. Ratio of flow against maximum flow (R).

The first two features extracted are the number of arcs and number of nodes within each grid. When mentioning arcs 'in-between' the source and sink, it signifies arcs with distinct paths connecting each node separately. The path to the source node should exclude the sink node, and vice versa. For example in Figure 3.6, arc (3, 28) is not in-between, whereas arc (9, 21) is in-between. Ratio of flow against maximum flow is referring to the expected flow from the source to sink after an attack over the maximum flow if there is no attack. The attack is simulated 300 times at the center of the grid and the resulting maximum flows from source to sink are recorded. The expected flow is the average of these resulting maximum flow. Figure 3.7 shows an example of the feature values obtained. At the highlighted grid, the feature values would be 4, 2, 4, 0 for |A|, |N|, B, R, respectively.

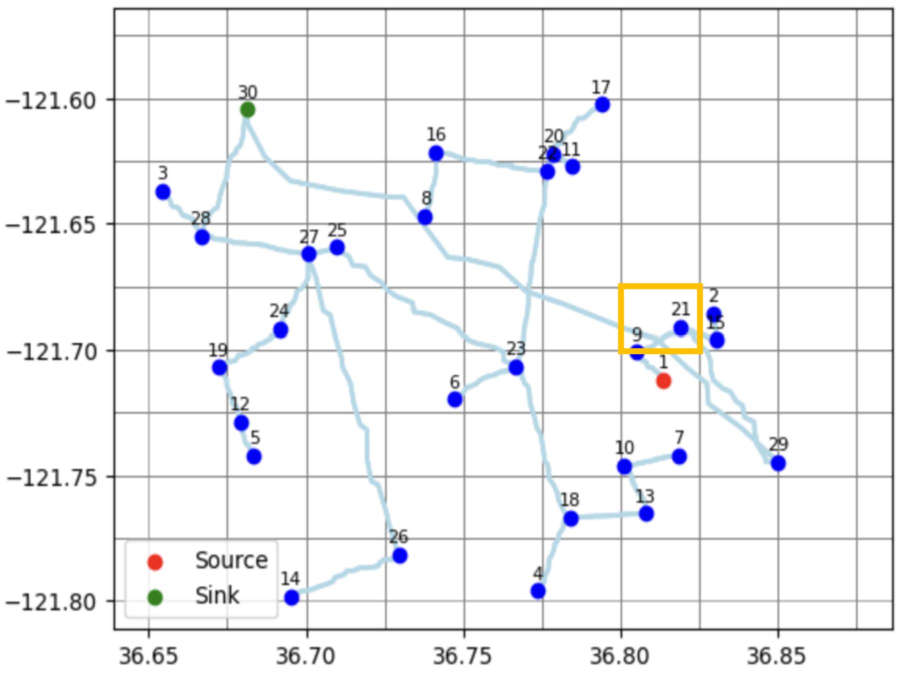
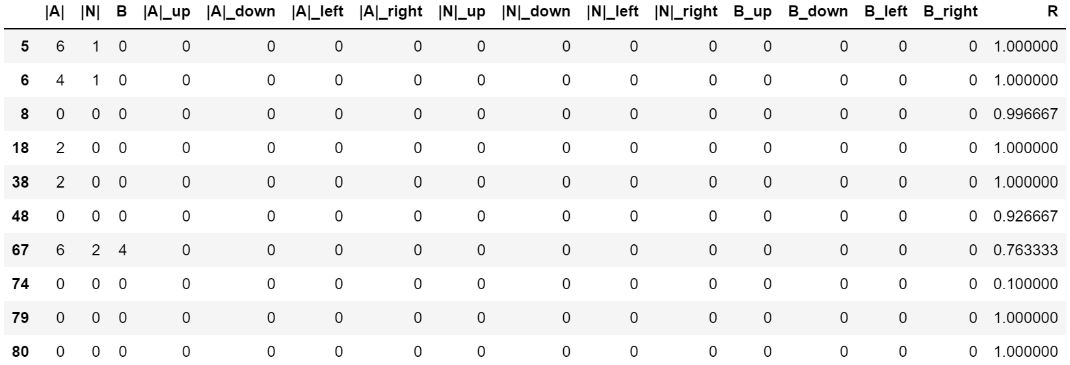


Figure 3.7. Example of feature values in grid. The highlighted grid has feature values of 4, 2, 4, 0 for |A|, |N|, B, R, respectively.

The formation of a data point involves the extraction of features from the target grid and its four neighboring grids (up, down, left, and right of the target grid). This process is repeated for each grid, resulting in a total of 81 data points derived from a single network. Incorporating the feature values of neighboring grids is crucial to enable the model to account for geographical dependencies. While the arcs may not fall within the same grid as the simulated attack location, there exists a non-zero probability that arcs in neighboring grids could be affected by a round due to their relative proximity to the attack location. Figure 3.8 shows a sample of ten such data points from the network depicted in Figure 3.7.

The sample data comprises of 16 columns. The first 15 columns represent the features, while the last column represents the response. As shown in Figure 3.8, it may be possible for R to be below 1 despite having no arcs and nodes present in the target grid. As there are 9×9 grids, each network would provide total of 81 data points for model training.



	|A|	|N|	B	|A|_up	|A|_down	|A|_left	|A|_right	|N|_up	|N|_down	|N|_left	|N|_right	B_up	B_down	B_left	B_right	R
5	6	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1.000000
6	4	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1.000000
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.996667
18	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1.000000
38	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1.000000
48	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.926667
67	6	2	4	0	0	0	0	0	0	0	0	0	0	0	0	0.763333
74	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.100000
79	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1.000000
80	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1.000000

Figure 3.8. Sample of data points obtained from the network shown in Figure 3.7. The first 15 columns are the features, and the last column is the response.

3.3.2 Train/Test Split

For this thesis, we generate 1500 networks, encompassing 300 networks each with 10, 20, 30, 40, 50 nodes (hereinafter referred to as 'networks with varying node counts'), resulting in a grand total of 121,500 data points. Data points obtained from 200 of each network with varying node counts are used for training a decision tree model. The remaining 100 from each network are used to test the accuracy of the model. The decision tree model is trained and implemented using Python's Sklearn library (Pedregosa et al. 2011). The training time takes less than two minutes to complete on a system with AMD Ryzen 9 7940HS w/ Radeon 780M Graphics and 32 GB random access memory.

3.4 Measure of Effectiveness

Once the model is trained, it can be deployed to predict the flow values for each grid in a network under simulated attack. The predicted optimal target location corresponds to the grid with the smallest predicted flow value. For the primary measure of effectiveness (MOE), if both the model and test data indicate that the same grid has the lowest R value, then the model is considered successful; otherwise it is not. The secondary MOE involves calculating the difference in R values between the model-predicted grids and the actual test data grids. Additionally, the model's performance across networks with different node counts can be analyzed to assess its robustness and generalizability. The next chapter delves in with more details on the application of the trained model, the measures of effectiveness, and insights gained from the results.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4:
Results and Analysis

4.1 Model

4.1.1 Decision Tree Model

The decision tree model is trained on a dataset of 8100 data points using Scikit-learn. It exhibits a total depth of 34 and underwent 22936 splits during the training process. In Figure 4.1, a snapshot of the decision tree is depicted, focusing on a subset with a depth of three. Each rectangular block symbolizes a decision node, indicating a specific feature and a corresponding threshold value. The feature acts as the variable guiding the decision, and the threshold signifies the value at which the decision is determined. As the decision tree progresses, it culminates in final predictions based on the extracted features related to the target grid.

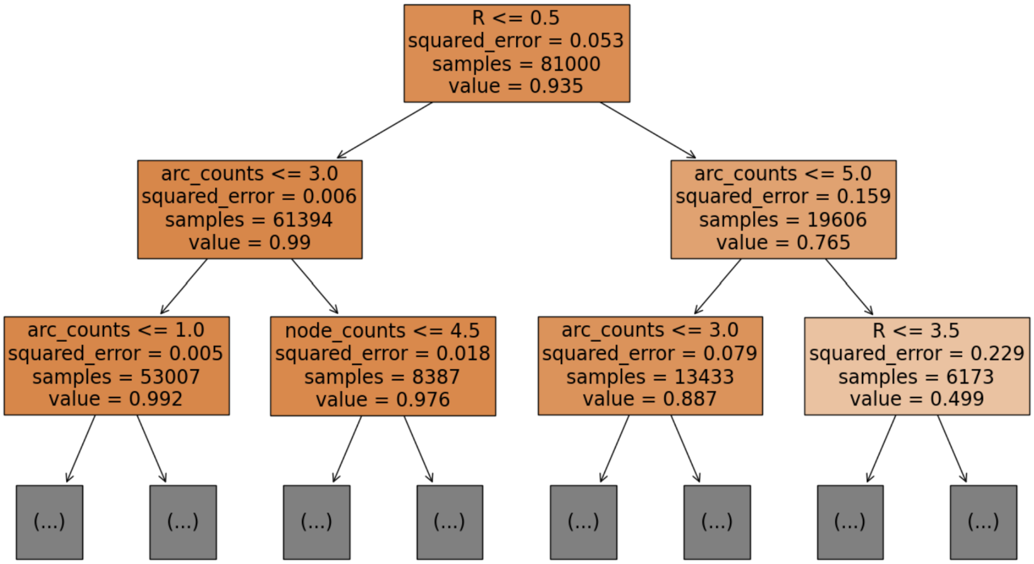


Figure 4.1. Subset of Decision Tree Model. The rectangle blocks represent the nodes in the tree, with darker colored orange representing higher R value. Each node represents a decision based on a feature.

The feature importance score of each feature is extracted from the model using the 'feature_importance_' attribute available from Scikit-learn's library. Table 4.1 showcases the feature importance scores of each feature. Each feature is measured using Gini importance and represents the normalized total reduction of criteria. The sum of all scores in the table equates to one. These scores indicate the relative significance of each feature in making predictions and provide insights into which features contribute the most to the model's performance.

Table 4.1. Feature importance scores, with each row representing importance of a feature, based on Gini index reduction (Hastie et al. 2001).

Feature	Importance Scores
R	0.301
$\lvert A\rvert$	0.245
$\lvert A\rvert$_down	0.045
$\lvert A\rvert$_right	0.045
$\lvert A\rvert$_up	0.045
R_right	0.042
$\lvert A\rvert$_left	0.042
R_up	0.037
R_left	0.036
R_down	0.035
$\lvert N\rvert$	0.032
$\lvert N\rvert$_up	0.027
$\lvert N\rvert$_left	0.023
$\lvert N\rvert$_right	0.023
$\lvert N\rvert$_down	0.022

4.2 Results

4.2.1 Overall Model Accuracy and Gap

Based on the primary MOE, for each network, the model is considered successful if the predicted grid with the lowest R value matches grid with lowest R value in the test data. Figures 4.2 and 4.3 illustrate instances where the model predictions align and diverge from the test data results on the target grid, respectively. The blue cross signifies the predicted grid by the model, while the orange cross indicates the actual grid according to the test data. In summary, the model accurately identified the same grid for 427 out of 500 test networks, achieving an accuracy of 85%. For the secondary MOE, the average gap across all networks is 0.0833. However, the model exhibits a significantly higher average gap of 0.570 in the 130 instances where incorrect predictions were made. This suggests that the model does not perform well in cases where it makes inaccurate predictions. Section 4.3 attempts to to address this by looking into the causes and possible improvements.

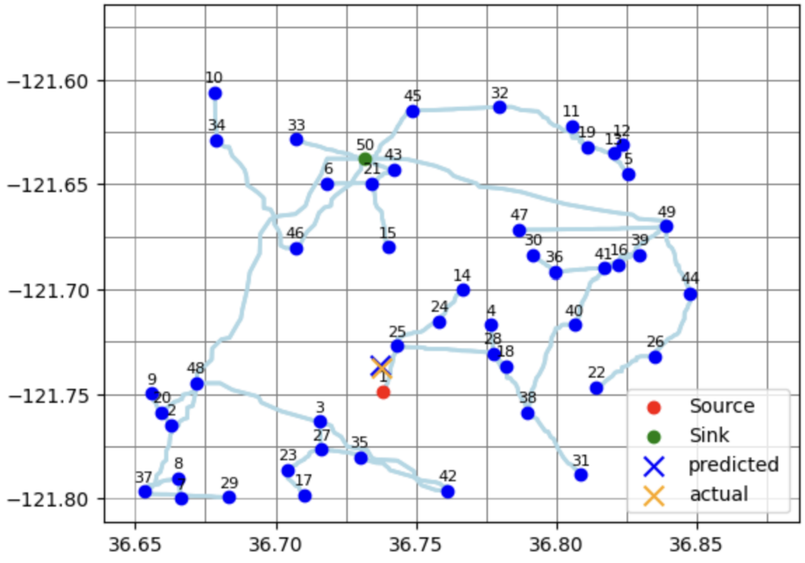
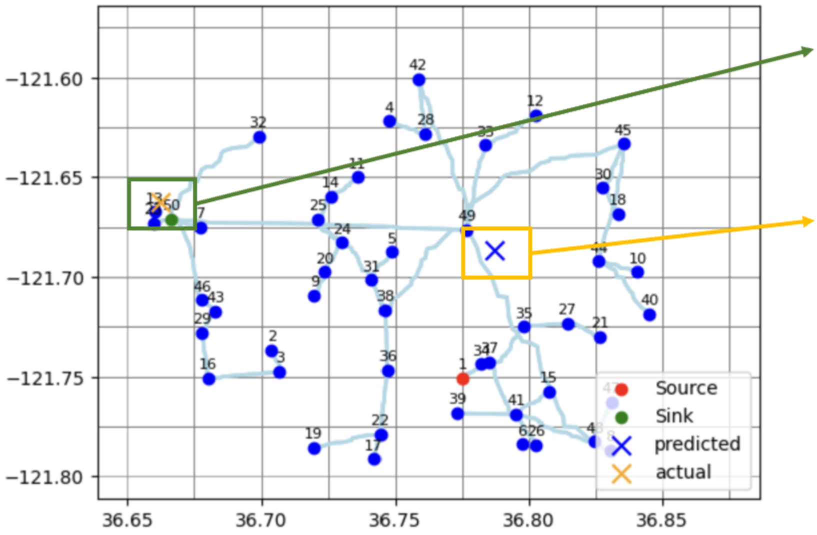


Figure 4.2. Example of model prediction align with test data. Both model and test data have the same grid that have the lowest R value.



Actual Grid
Actual value: 0
Predicted value: 0.131

Predicted Grid
Actual value: 0.217
Predicted value: 0.123

Gap
0.217 – 0 = 0.217

Figure 4.3. Example of Incorrect Model Prediction.

In Figure 4.2, both the model and test data show the same grid with the lowest R value, indicating a successful prediction. Figure 4.4 illustrates this decision-making process, which presents an example decision path leading to the final prediction of 0. However, in Figure 4.3, discrepancies arise. The test data indicates an R value of 0 for the grid with the lowest R value (highlighted in the green box), while the model predicts 0.131 for the same grid. Additionally, the model identifies a different grid (highlighted in the orange box) as having the lowest R value (0.123), whereas the test data records an R value of 0.217 for that grid. This discrepancy results in a 0.217 difference in R values between the model's prediction and the actual test data.

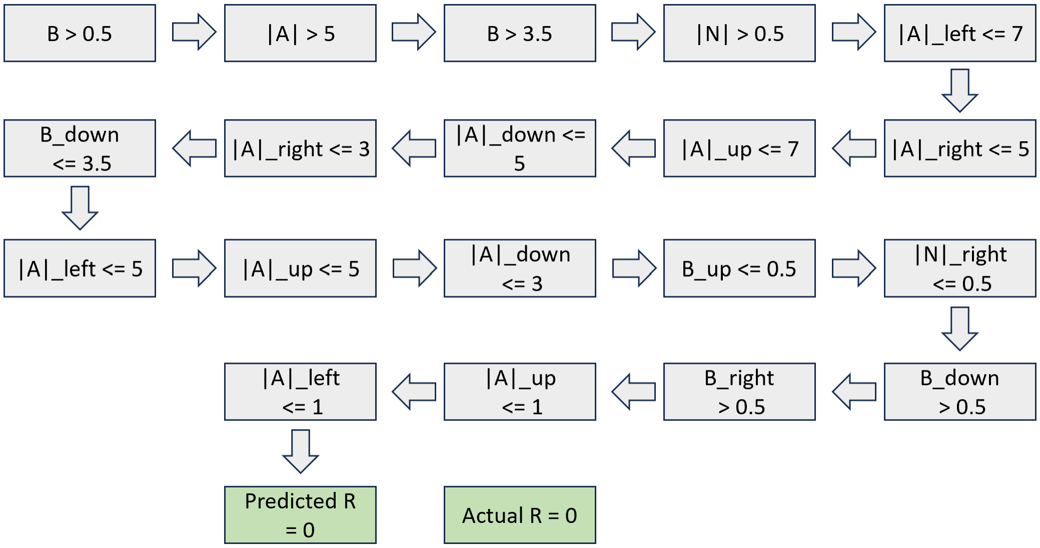


Figure 4.4. Example of decision path to reach the prediction of 0. Each block contains the feature and its threshold value, leading to the final prediction in the last block.

4.2.2 Results for Network with Varying Nodes

Rather than assessing the model's accuracy across all networks in general, we aim to gauge its generalizability and scalability by examining performance on networks with varying numbers of nodes. Table 4.2 shows the accuracy values for the networks with varying nodes. Figure 4.5 summarizes the results for networks with varying nodes, depicting the mean gap and variance values along with a 95% confidence interval.

Table 4.2. Accuracy of Model on Networks with Varying Number of Nodes

# Nodes	Accuracy
10	0.67
20	0.81
30	0.88
40	1.00
50	0.91

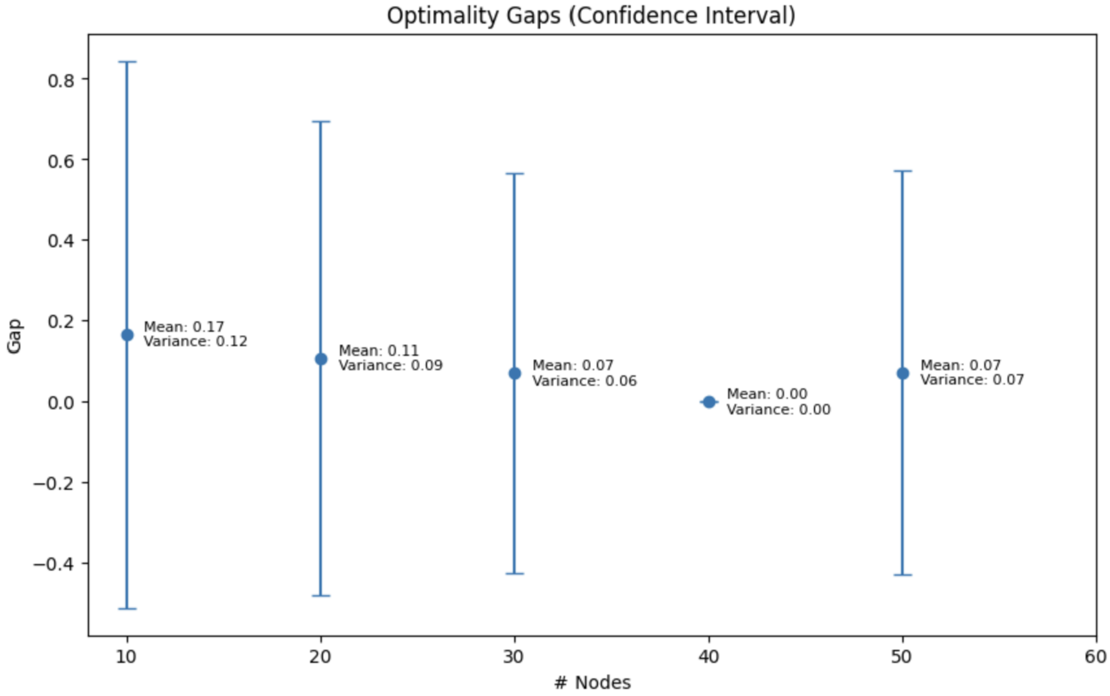


Figure 4.5. Confidence Interval of Model Performance on Networks with Varying Number of Nodes. Each error bar shows the mean and the 95% confidence interval of the gap.

From a conventional perspective, one might anticipate decline in the model performance with growing complexity of network, characterized by an increasing number of nodes. However, our observations challenge this intuition. Remarkably, the model exhibits poorest performance on networks with only ten nodes. One reason for such observation could be due to the feature importance of the model. As seen in Table 4.1, the number of arcs in the target grid plays an important role in determining the prediction values. Simpler networks tend to have less arcs in each grid, making it harder for the model to distinguish the optimal grid to target. Section 4.3 shows an example of how high arc counts may confuse the model's predictions.

4.2.3 Grid Distance

Instead of measuring gap between R values, an alternative measure of error would be the grid distance gap, which is the number of adjacent grids between the actual and predicted grids. Figure 4.6 shows an example of the grid distance between the two grids. The grid distance gap in this figure is six, as it takes six adjacent grids to reach the actual grid from the predicted grid. The measure of error plays a crucial role in evaluating the model's spatial accuracy. Figure 4.7 shows the grid distance gaps for networks with varying number of nodes.

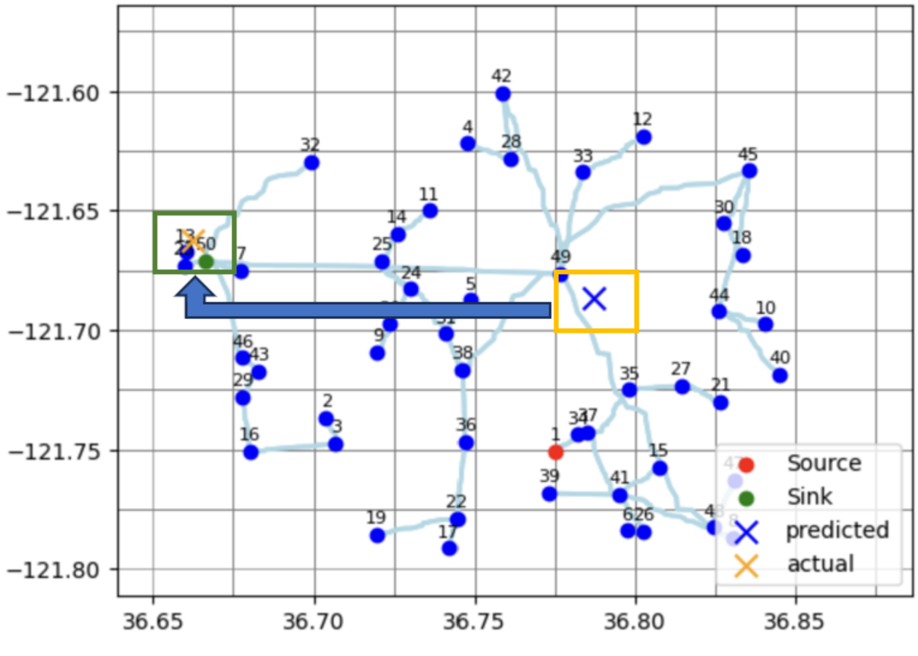


Figure 4.6. Grid distance gap is the number of adjacent grids between the actual and predicted grids. The gap in this figure is six.

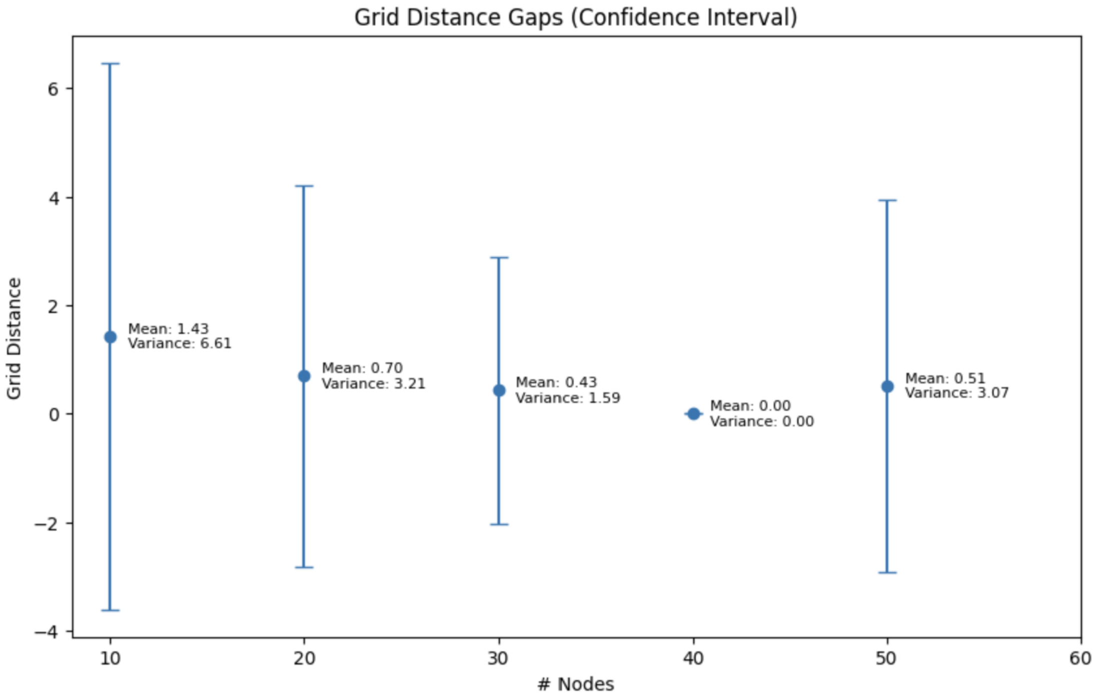


Figure 4.7. Confidence Interval of mean grid distance gap on Networks with Varying Number of Nodes. Grid distance gap refers to the number of adjacent grids between the actual and predicted nodes. Each error bar shows the mean and the 95% confidence interval of the gap.

4.2.4 Analysis

From Figure 4.7, it is observed that the model's predictions exhibit larger grid distance gaps for networks with a lower number of nodes. This trend in grid distance gaps aligns with the patterns observed in the gaps of R values under Subsection 4.2.2. To quantify this relationship, the Pearson Correlation Coefficient of the two gaps is calculated to be 0.718, indicating a fairly strong positive correlation. For a visual representation, refer to Figure 4.8, which illustrates the scatter plot of the two gaps, showcasing the positive correlation.

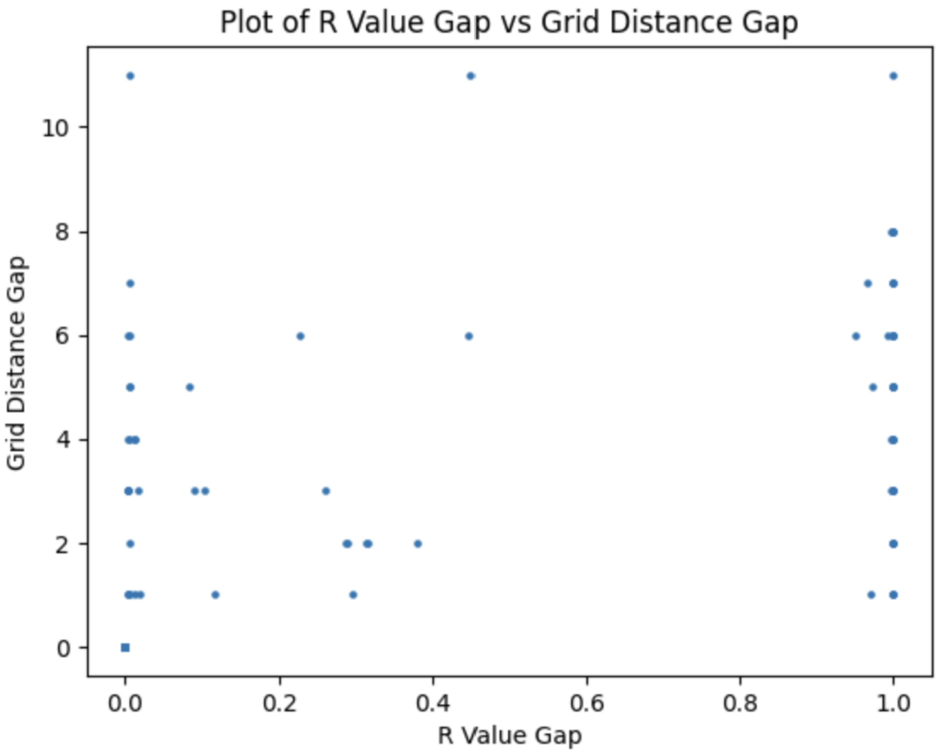


Figure 4.8. Scatter Plot of R Value Gap vs Grid Distance Gap. The Pearson Correlation Coefficient of the two gaps is calculated to be 0.718, indicating a fairly strong positive correlation.

4.3 Insights for Model Improvement

4.3.1 Model Emphasis on Arcs and Its Implications

As we discussed earlier and highlighted in Table 4.1, the model pays a lot of attention to the number of arcs within the target grid. This means that it might predict grids with a large number of arcs as having a low R value, which could lead to some challenges. Figure 4.9 illustrates an extreme example of this phenomenon. Based on the figure, by visual inspection, grids positioned horizontally between nodes 1 and 2 are the likely targets that could disrupt the flow. However, the model's prediction diverged due to the elevated importance score assigned to arc counts. Consequently, the model predicted the grid with large number of arcs to have a low R value, even when it has no practical significance in obstructing the flow from source to sink.

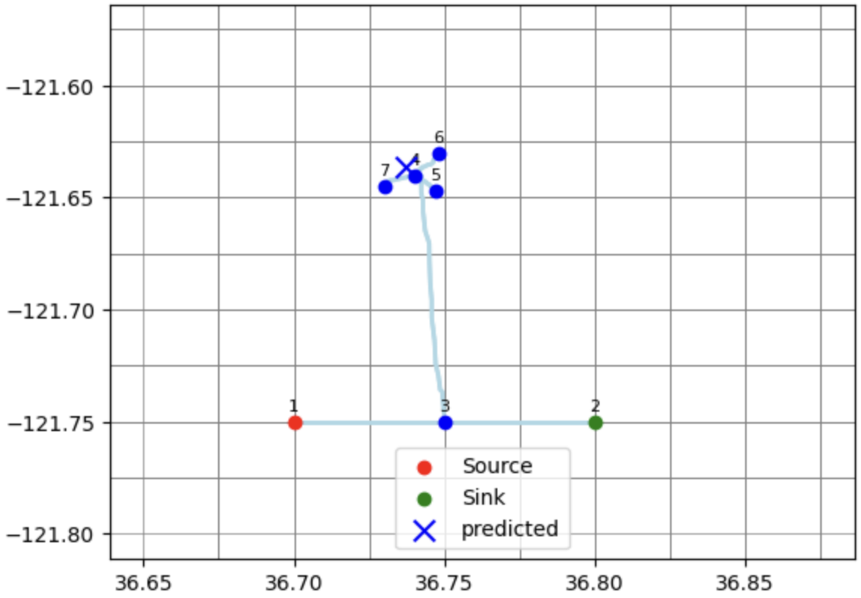


Figure 4.9. Due to high importance score of arcs, model would predict grids with large number of arcs, even though visually it is never going to affect the flow from source to sink.

To mitigate the challenge posed by the model's heightened attention to arc counts, a potential refinement involves the expansion of the feature space. An evident strategy is to integrate a more extensive array of neighboring grids, providing the model with a holistic spatial context. This broader perspective aims to enhance the model's discernment of the significance of arcs within the target grid. By encompassing a wider range of neighboring grids, the model has the potential to capture additional spatial dependencies, resulting in more refined predictions. This approach seeks to diminish the undue emphasis on seemingly irrelevant features, such as the sheer count of arcs within a single grid.

Moreover, another avenue for increasing the feature space entails considering the distance of the grid from both the source and sink. While this avenue holds promise, its direct impact on enhancing results remains to be conclusively established. Further experiments will be essential to validate the potential benefits of incorporating distance-related features into the model.

4.3.2 Optimizing Grid Size for Enhanced Targeting Precision

An identified challenge in our current model is the substantial grid size, which may introduce inaccuracies in targeting. The model currently centers its focus on the grid, potentially overlooking optimal disruption points. The large grid size, with its emphasis on the grid's center, may cause the model to miss potentially effective aim points. To address this, a reduction in grid size may be implemented to enhance targeting precision. However, this improvement would come with a trade-off in data generation for model training. The increased number of grids necessitates longer simulation times for artillery attacks on the network. Additionally, a reduced grid size implies the need for a larger number of neighboring grids, as suggested in Section 4.3.1, potentially leading to an exponential increase in training time. Achieving an optimal balance between grid size and model training time is crucial.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5:
Conclusion

5.1 Summary of Key Findings

5.1.1 Decision Tree Model

The decision tree model, trained on a dataset of 8100 data points, showcased a depth of 34 and underwent 22936 splits. Feature importance analysis emphasized the significance of the number of arcs within the target grid in determining prediction values. However, this introduced a challenge, as the model demonstrated sensitivity to the count of arcs, leading to potential inaccuracies in its predictions.

5.1.2 Model Performance

In terms of performance, the model achieved a commendable accuracy, correctly predicting the same grid for 370 out of 500 test networks, resulting in an overall accuracy of 74%. Spatial accuracy assessments, based on gap and grid distance measures, revealed intriguing trends, especially for networks with varying numbers of nodes.

Contrary to initial expectations, the model's performance did not follow the anticipated pattern of decreasing with an increase in network complexity. Rather surprisingly, networks with higher complexity, characterized by a greater number of nodes, exhibited better performance. This unexpected result challenged the intuitive assumption that increased network complexity would negatively impact the model's predictive capabilities. Notably, the simplest networks with only ten nodes demonstrated the poorest performance, prompting further exploration into the underlying factors contributing to this counter-intuitive trend.

5.2 Future Research

This section provides avenues for future research based on the insights gained and limitations identified in the current study.

5.2.1 Enhancing Model Sensitivity to Network Complexity

Building on the unexpected findings regarding network complexity, future research could delve into strategies to enhance the model's sensitivity to varying network complexities. This may involve refining the feature space or exploring alternative modeling techniques to better capture the nuances of simpler and more complex networks.

5.2.2 Refinement of Feature Importance

Given the model's pronounced focus on the number of arcs within the target grid, future research could explore ways to refine feature importance. Investigating additional features or modifying the weighting assigned to different features may contribute to a more nuanced understanding of network characteristics, potentially improving the model's predictive accuracy.

5.2.3 Optimizing Grid Size for Precision

The identified challenge related to the large grid size suggests an avenue for optimization. Future research could focus on refining the grid size to enhance targeting precision. This might involve experimenting with different grid sizes and assessing the trade-offs between model performance and computational efficiency.

5.2.4 Exploring Alternative Model Architectures

Considering the limitations of the decision tree model, future research could explore alternative model architectures. Neural networks or ensemble methods might offer improved predictive capabilities, especially in handling the complexities and spatial dependencies inherent in the network flow prediction problem.

5.2.5 Modelling Multiple Aim Points and Diversifying Weapon Types

Future research could explore methods to simultaneously incorporate multiple aim points and using different weapon types. This approach aims to enhance the model's usability framework for strategic planning. Addressing both multi-target scenarios and a variety of weapon characteristics would contribute to a more robust decision-making tool. The challenge lies in carefully refining the decision tree model to accommodate these additional complexities while maintaining its predictive accuracy.

5.2.6 Real-world Validation and Deployment

Conducting real-world validation is crucial to affirm the model's applicability in practical scenarios. Future research should focus on acquiring authentic network data and validating the model's predictions against real-world network flow data. Furthermore, investigating deployment strategies and seamless integration with decision-support systems in military or critical infrastructure settings represents a pivotal step toward practical implementation and operational effectiveness.

5.3 Conclusion

In conclusion, this thesis establishes a proof-of-concept for the utilization of a machine learning model, specifically a decision tree model, in identifying the optimal location to target a network. With a notable accuracy rate of 85%, the model demonstrates its potential applicability in strategic planning. Despite encountering challenges related to feature importance and observing unexpected performance trends in simpler networks, the decision tree model emerges as a promising tool for identifying vulnerabilities within a physical network. This work lays the groundwork for the development of more sophisticated models in the future. Moving forward, research avenues may include enhancing model features, validating using real-world data, and exploring scenarios involving multiple aim points and diverse weapon types. The continuous refinement of such models holds promise for advancing network analysis using machine learning techniques.

THIS PAGE INTENTIONALLY LEFT BLANK

List of References

Chan K, Baguley C, Madawala U (2022) A novel approach to touch voltage risk assessment for gas pipelines in shared transmission corridors. *IET Science, Measurement & Technology* 17:n/a–n/a (09), https://doi.org/10.1049/smt2.12127.

Cormican KJ, Morton DP, Wood RK (1998) Stochastic network interdiction. *Operations Research* 46(2):184–197, https://doi.org/10.1287/opre.46.2.184.

Edmonds J, Karp RM (1972) Theoretical improvements in algorithmic efficiency for network flow problems. *J. ACM* 19(2):248–264 (apr), https://doi.org/10.1145/321694.321699.

Electrical grid (2024) *Wikipedia*. Accessed Jan 18, 2024, https://en.wikipedia.org/wiki/Electrical_grid.

Electricity Consumers Resource Council (2004) The economic impacts of the august 2003 blackout. February 9, https://syriacpress.com/blog/2021/06/28/salah-al-din-thermal-power-station-in-iraq-targeted-by-isis/.

Ford LR, Fulkerson DR (1962) *Flows in Networks* (Princeton University, Princeton, NJ).

Hastie T, Tibshirani R, Friedman J (2001) *The Elements of Statistical Learning*. Springer Series in Statistics (Springer New York Inc., New York, NY, USA).

Lim WY (2016) Predicting the accuracy of unguided artillery projectiles. Master's thesis, Naval Postgraduate School, Monterey, CA.

Orkun Baycik N (2022) Machine learning based approaches to solve the maximum flow network interdiction problem. *Computers & Industrial Engineering* 167:107873, https://doi.org/10.1016/j.cie.2021.107873.

Pedregosa F, Varoquaux G, Gramfort A, Michel V, Thirion B, Grisel O, Blondel M, *et al.* (2011) Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research* 12:2825–2830.

Reuters (2021) Islamic state claims responsibility for rocket attack on iraqi power station. June 27, https://www.reuters.com/world/middle-east/islamic-state-claims-responsibility-rocket-attack-iraqi-power-station-2021-06-27/.

Salmeron J, Wood K, Baldick R (2009) Worst-case interdiction analysis of large-scale electric power grids. *IEEE Transactions on Power Systems* 24(1):96–104.

SyriacPress (2021) Salah al-din thermal power station in iraq targeted by isis. June 28, https://syriacpress.com/blog/2021/06/28/salah-al-din-thermal-power-station-in-iraq-targeted-by-isis/.

Mao Shuai, Chengzhi W, Shiwen Y, Hao G, Jufang Y, Hui H (2018) Review on economic loss assessment of power outages. *Procedia Computer Science* 130:1158–1163, https://doi.org/https://doi.org/10.1016/j.procs.2018.04.151.

Wood R (1993) Deterministic network interdiction. *Mathematical and Computer Modelling* 17(2):1–18, https://doi.org/10.1016/0895-7177(93)90236-R.

Initial Distribution List

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California