2023-03

AN EVALUATION OF RANDOMIZED ROUTING STRATEGIES FOR DECEPTION IN MOBILE NETWORKED CONTROL SYSTEMS

Plunkett, Kyle E.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN EVALUATION OF RANDOMIZED ROUTING STRATEGIES FOR DECEPTION IN MOBILE NETWORKED CONTROL SYSTEMS

by

Kyle E. Plunkett

March 2023

Thesis Advisor: Ruriko Yoshida
Co-Advisor: Jefferson Huang
Second Reader: Anthony Tai,
NAVAL SURF WAR CENT

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE AN EVALUATION OF RANDOMIZED ROUTING STRATEGIES FOR DECEPTION IN MOBILE NETWORKED CONTROL SYSTEMS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Kyle E. Plunkett	
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)

Networked unmanned autonomous systems will increasingly be employed to support ground force operations. Approaches to collaborative control can find near-optimal position recommendations that optimize over system parameters such as sensing and communication to increase mission effectiveness. However, over time these recommendations can create predictable paths that may provide leading indications of the force's operational intent. We assume that the adversary's goal is to identify a ground force's operational intent. Using randomized routing strategies to generate deception plans for unmanned systems against the adversary, this red methodology has the potential to change many aspects of military operational planning, including operational and strategic level planning and wargaming. This topic builds on research from L. Wigington in 2021, which developed an adversarial assessment of unmanned mobile networked control systems. From that and based on prior research, this thesis applies and potentially extends prior methodologies to analyzing adversarial behaviors and manipulating their behaviors to NCS using randomized routing strategies.

14. SUBJECT TERMS mobile networked control systems. randomized routing strategies	**15. NUMBER OF PAGES** 61
	16. PRICE CODE

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

NSN 7540-01-280-5500

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

AN EVALUATION OF RANDOMIZED ROUTING STRATEGIES FOR DECEPTION IN MOBILE NETWORKED CONTROL SYSTEMS

Kyle E. Plunkett
Lieutenant, United States Navy
BS, United States Naval Academy, 2016

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL
March 2023

Approved by: Ruriko Yoshida
Advisor

Jefferson Huang
Co-Advisor

Anthony Tai
Second Reader

W. Matthew Carlyle
Chair, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Networked unmanned autonomous systems will increasingly be employed to support ground force operations. Approaches to collaborative control can find near-optimal position recommendations that optimize over system parameters such as sensing and communication to increase mission effectiveness. However, over time these recommendations can create predictable paths that may provide leading indications of the force's operational intent. We assume that the adversary's goal is to identify a ground force's operational intent. Using randomized routing strategies to generate deception plans for unmanned systems against the adversary, this red methodology has the potential to change many aspects of military operational planning, including operational and strategic level planning and wargaming. This topic builds on research from L. Wigington in 2021, which developed an adversarial assessment of unmanned mobile networked control systems. From that and based on prior research, this thesis applies and potentially extends prior methodologies to analyzing adversarial behaviors and manipulating their behaviors to NCS using randomized routing strategies.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

AI	Artificial Intelligence
DDG	Guided Missile Destroyer
DFS	Depth First Search
DFT	Depth First Traversal
DOD	Department of Defense
DON	Department of the Navy
GAN	Generative Adversarial Network
GFT	Ground Force Triangulation
IAS	Intelligent Autonomous Systems
IDS	Multi-Thread Experiment (MTX) Infiltration Data Set
MTX	Multi-Thread Experiment
NCS	Networked Control System
NPS	Naval Postgraduate School
NSW	Naval Special Warfare
TTP	tactics, techniques, and procedures
UAV	Unmanned Aerial Vehicle
USN	U.S. Navy
USV	Unmanned Surface Vehicle
UxV	Unmanned Vehicle

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

This thesis builds upon prior Naval Postgraduate School (NPS) theses on UxV positioning in a mobile NCS to develop a deceptive UxV routing strategy in order to mask operational intent. Recent research concerning NCS has resulted in position optimization strategies and algorithms for the UxV components as well as identify vulnerabilities if an adversary were to obtain perfect position data from the UxV components of an NCS. With that knowledge, an adversary has the ability to construct a model capable of predicting the location of ground forces. This jeopardizes both the operational intent of the ground forces and the ground forces themselves.

This thesis explores a potential routing strategy to determine its effectiveness in deceiving an adversary with perfect information, aiming to maximize the position prediction error of ground forces by an adversary. The routing strategy is deterministic and uses random spanning trees and a Depth First Traversal (DFT) of a graph to generate a list of nodes that are then translated into grid coordinates. This list is then divided into candidate decoy UxV paths based on the desired path length. Using the time series multiple linear regression model that this thesis builds on, each candidate decoy path is tested in the place of the regression's predictors to produce a position prediction. The predicted position is then compared to the actual position of the ground forces, and a prediction error is determined.

The deceptive routing algorithm used in this thesis produced promising results, increasing the average prediction error from 39 meters regardless of the predictor variable tested. Incorporating the decoy paths resulted in an average position prediction error of 94, 345, and 392 meters for each predictor tested, respectively. This deceptive routing strategy introduces randomness to the paths taken by UxV's in a mobile NCS that can deceive an adversary's model and proposes a framework for generating decoys. The successful results indicate the potential that this and similar work has to further develop deceptive routing strategies that will benefit Department of Defense (DOD) operations now and in the future.

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

I would like to thank my advisors, Dr. Ruriko Yoshida and Dr. Jefferson Huang, for their advice and guidance during this research. Their expertise and experience was invaluable in directing my work and keeping me on track.

I would also like to thank my parents, David and Holly, for their support throughout my time at the Naval Postgraduate School. They were always there to talk and listen. Finally, I would like to thank my dog, Coco, for consistently reminding me that it was time to take a break.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

Intelligent Autonomous Systems (IAS) are rapidly changing the battle space in conflicts around the globe. The Department of the Navy (DON) is actively pursuing technological advancements in the field of IAS and has a stated vision to "seamlessly integrate IAS as trusted members of the Naval enterprise" (Department of the Navy 2021). The Navy's continued effort to make evolutionary and disruptive gains in IAS technology is a direct reflection of the President's National Security Strategy and Secretary of Defense's National Defense Strategy, which both state that advancements in Artificial Intelligence (AI) technologies is a top priority for the Department of Defense (DOD) moving forward (Office of the Secretary of Defense 2022). Unmanned systems developed by the Navy's research into this field will increasingly be paired with manned systems in order to optimize the battlefield. This was successfully demonstrated in 2017 during an Naval Special Warfare (NSW) exercise on San Clemente Island, where mobile Networked Control System (NCS) consisting of Unmanned Vehicle (UxV)s supported NSW ground forces. The Multi-Thread Experiment (MTX) revealed that while the DON is advancing its capability to integrate manned and unmanned systems, there remains potential vulnerabilities subject to exploitation.

1.1 Problem Statement

Malicious actors seeking to degrade DOD capabilities may have the capacity to obtain information on current tactics, techniques, and procedures (TTP). Recent work conducted by Wigington (2021) indicates that such an actor achieving that capacity can have significant detrimental impact on future mission planning and execution. An adversary with the ability to steal information can analyze that data to construct models indicative of DOD and DON capabilities. Research conducted by Wigington (2021) at the Naval Postgraduate School (NPS) using MTX data from the 2017 NSW exercise shows that a bad actor with the intent and adequate capability can develop predictive models of a mobile NCS using UxVs to track and forecast ground force locations. The model has the capability to accurately predict both current and future locations of ground forces, which is problematic for planners, operators, and the DOD as a whole. This thesis analyzes a deceptive routing strategy for

UxVs in a mobile NCS that can be used to deceive and decrease an adversary's ability to accurately gain insight into operator's position and intent.

1.2 Mobile NCS Position Optimization

Optimizing a mobile NCS of UxVs for mission accomplishment can be critical to mission success. However, it has the potential to produce unintended and undesirable consequences. Particularly, optimizing UxV positions for this purpose can enable an adversary to accurately predict the ground force's current and future positions as well as reveal the operational intent of the mission. It is vital to mission success that operational intent is sufficiently masked so that the adversary cannot determine the objective; therefore, the pros and cons between optimal UxV stationing and routing versus deceptive stationing and routing must be considered.

Lowry (2020) analyzed a distributed submodular optimization framework for optimal UxV routing during the MTX. Using that MTX data, Wigington (2021) demonstrated the accuracy with which a capable adversary can identify operational intent and track NSW ground forces using the MTX data set. His model illustrated vulnerabilities and introduced potential threats caused by mobile NCS mission planning when deception is not considered. Incorporating deception into UxV routing for mobile NCS is the focus of this thesis.

1.3 Proposed Analytical Framework

The goal of this research is to determine the effectiveness of utilizing a graph-based, randomized routing strategy that degrades a capable adversary's ability to predict the operational intent of a NCS. The algorithm produces a path that spans the operating area that is used to produce candidate decoy UxV routes. Incorporating this decoy route degrades the adversary's capability to predict the location and destination of the non-decoy units.

In order to investigate the effectiveness of this algorithm, multiple candidate decoy paths are generated. Each iteration produces a single path that traverses the operating area. Since the length of the generated path is an input, several path lengths are examined for each iteration of the algorithm. This varies the number of candidate paths for the decoy UxV and allows a deeper analysis of the utility of this algorithm for incorporating deception into mobile NCS

routing strategies.

1.4 Ongoing Research Effort

This thesis is part of an ongoing research effort at NPS to develop deceptive planning algorithms for mission planners utilizing UxVs in a mobile NCS. Other current research into this topic includes utilizing Generative Adversarial Network (GAN)s as a deceptive routing strategy and determining the best integration between optimal NCS positioning and routing and deceptive routing. This thesis is specifically focused on evaluating the randomized routing strategy proposed by Tsitsiklis and Xu (2018) against the Red Cell prediction model proposed by Wigington (2021).

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2:
Background

This chapter reviews prior work on NCS and their use in supporting expeditionary forces. Section 2.1 describes Networked Control Systems and optimized positioning. Section 2.2 describes the Ground Force Triangulation (GFT) model used to locate NSW forces. Finally, Section 2.3 describes the randomized routing strategy used in this thesis.

2.1 Networked Control Systems

A networked control system NCS is a system comprised of multiple components that are connected via communication links to control the overall system (Lowry 2020). An NCS can be static or dynamic, however this thesis focuses "primarily on a dynamic NCS implementation, which contains one or more agents whose state varies" (Wigington 2021, p. 5). Further, the NCS agents examined in this thesis consist of multiple UxV assets. This thesis expands specifically on work by Wigington (2021), which in turn built upon optimization of UxVs in a mobile NCS research conducted by Wachlin (2020) and Lowry (2020).

2.1.1 Optimizing Networked Control Systems

Lowry (2020) presents a distributed submodular optimization framework for the MTX NCS to allow efficient communication between UxVs in the network. Submodularity is "a set function $f : 2^v \rightarrow$ is submodular for any A and B, with $A \subset B \subset V$, and any $s \notin B$, $f(A \cup s) - f(A) \geq f(B \cup s) - f(B)$" (Wigington 2021, p. 7). The distributed submodular optimization approach uses the submodular utility function, J, and is defined as

$$\begin{aligned} J(S) &= a_s f_s(S) + a_r f_r(S) \\ s.t. a_s &+ a_r = 1 \\ a_r, a_s &\geq 0, \end{aligned} \tag{2.1}$$

where "J is composed of a weighted sum of two submodular functions: one that evaluate the NCS for some sensing utility f_s and one that evaluates it for some communications robustness utility f_r" (Lowry 2020, p. 14). Wachlin (2020) provides a deeper description of the development of this submodular utility function.

The submodular utility function consists of two subfunctions, sensing and robustness or $f_s(S)$ and $f_r(S)$, respectively. The sensing subfunction uses the quality of UxV input into the network to ensure accurate and reliable measurements and information. The robustness subfunction ensures that the distributed submodular optimization algorithm is resistant to uncertainty or noise (Lowry 2020).

The distributed submodularity approach seeks to find the optimal position set S for UxVs from V possible locations using the submodular utility function, Equation 2.1. This allows the NCS control algorithms to provide position recommendations that are near-optimal (Lowry 2020). This method was used by Lowry (2020) to optimize the positioning of the NCS's UxV components from the MTX data.

2.2 Red Cell Analysis

Wigington (2021) presents a red cell analysis of the MTX, assuming full and correct visibility of all UxV's comprising the NCS. The terms red cell and adversary will be used interchangeably in this thesis. His analysis examined various models that used positional data of UxV's to predict the location of NSW forces. The goal of his work was to uncover whether or not and how well an adversary can predict the location of ground assets with perfect knowledge of the mobile NCS. The best model from an adversary's perspective comes in a time series regression model. This thesis uses his results to develop a counter-routing strategy for UxVs in the mobile NCS to reduce the predictive accuracy an adversary with perfect knowledge of the network.

One important factor in this red cell analysis is the interdependence of UxVs. The UxVs are constantly communicating and adjusting based on input and parameters of the other UxVs in the network. Correlation is to be expected, but ignoring it "allows for a simple analysis of the relationships between the individual coordinate components" (Wigington 2021, p. 30). Wigington (2021) explored more complex models to analyze interdependence among

predictors, but the most successful model resulted from the ignorance of all interdependence, therefore this section will focus on those models.

UxV Forecast Model

An univariate Auto-Regressive Integrated Moving Average (ARIMA) model is created for UxV position data during the MTX. The data consist of 7005 observations across twelve UxVs and is split into a training and test set of 5604 and 1401 observations, respectively. Samples are taken at 120-second intervals, reducing the training set to 37 observations (Wigington 2021). According to Wigington (2021), six steps were taken to evaluate the model.

1. Data is split into a training and test set;
2. Data is broken down to observe time series components;
   (a) Trend: long-term component of change.
   (b) Seasonality: changes in data during known/fixed periods.
   (c) Cycle: changes in data not during fixed periods.
   (d) Noise: variance after consideration of the above components.
3. Model built with appropriate method (ARIMA in this case);
4. Use ARIMA model to predict x-steps into the future for each UxV;
5. Compare position forecast based on training set data to test set data;
6. Calculate performance metrics.

Ground Force Triangulation Model

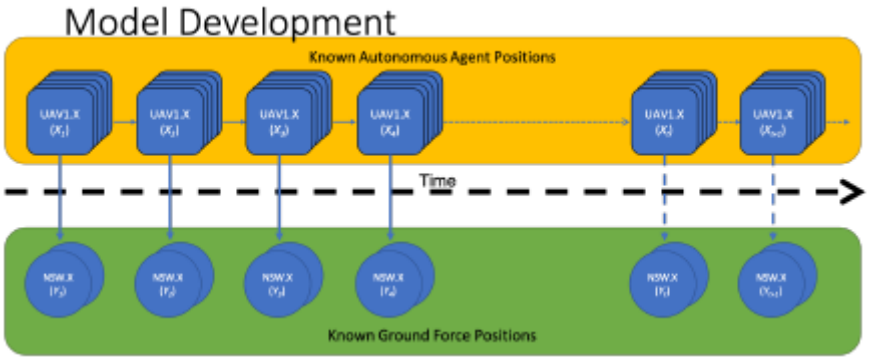
The Ground Force Triangulation GFT Model is a multiple linear regression designed to calculate NSW position as a function of UxV positions. As with the ARIMA model, the GFT is constructed from the training set and then tested using forecast predictions from the time series. The GFT model represents the relationship that the red cell or adversary has established between UxVs and the mobile NCS with the ground forces. The GFT produces results in two output data points, measured in local coordinate units, which combine to produce a single two-dimensional coordinate point, (X,Y). This is the estimated position created by the red cell. Using the Euclidean distance between the red cell's position estimation and the true position of the NSW forces, the adversary's prediction error in meters is calculated. Chapter 3 discusses how the randomized routing strategy described in

Section 2.3 is incorporated into the MTX data set and used in the GFT.

Time Series Multiple Linear Regression Model

In general, time series regression models take the output from a time series forecast model and use it as the input for a regression model to make a prediction. The ARIMA time series model and GFT comprise the time series multiple linear regression model that predicted the location of NSW forces in Wigington (2021). Figure 2.1 shows a visualization of the time series regression model.

Figure 2.1. Overview of time series regression model. Source: Wigington (2021).



The model developed by Wigington (2021), represents a red cell with modelling capabilities that accurately predict the location of NSW forces within 75 meters. The models in equations 2.2 and 2.3 represent the final product of the time series linear regression used to predict the x and y-coordinates of the NSW team during the MTX. These models are the target of deceptive randomized routing strategies in this thesis. They are

$$\text{NSW}.X = \beta_{11} \cdot UAV1.X + \beta_{12} \cdot UAV3.X + \beta_{13} \cdot USV1.X \tag{2.2}$$

and

$$\text{NSW}.Y = \beta_{21} \cdot UAV1.Y + \beta_{22} \cdot UAV3.Y + \beta_{23} \cdot USV1.Y, \tag{2.3}$$

where $\beta_{i,j} \in \mathbb{R}$, for $i = 1,2$ and for $j = 1,2,3$, are coefficients of predictors (Wigington 2021). β_{ij} represents the coefficients determined by the time series multiple linear regression

for each data point, the predictors $UAV1.X, UAV1.Y, UAV3.X, UAV3.Y, USV1.X$, and $USV1.Y$ and the response variables $NSW.X$, and $NSW.Y$

This thesis uses models 2.2 and 2.3 as a baseline and examines randomized deceptive routing strategies to obfuscate an adversary's ability to accurately predict the location of ground forces supported by the NCS. However, there are limitations to fully randomized strategies. Notably, the UxV's sensing range, communications range, and mobility constraints may preclude some randomized routes from being viable. In the MTX example, these constraints are illustrated in Table 2.1 (Lowry 2020). Based on Wigington (2021)'s regression, only the Unmanned Surface Vehicle (USV) and Unmanned Aerial Vehicle (UAV) elements of the NCS are relevant predictors.

Table 2.1. MTX agent characteristics. Source: Lowry (2020).

Agent	Speed (m/s)	Sensing Range (m)	Comms Range (m)
NSW Team	2	-	5000
DDG	5	-	5000
UUV	2.6	200	5000
USV	15	200	5000
UAV	35	500	5000

2.3 Randomized Routing Strategies

This thesis draws from previously studied graph or network-based routing strategies. Tsitsiklis and Xu (2018) described a "Goal Prediction Game" in which undirected graphs are traversed by an agent that randomly selects a goal node that an adversary attempts to discover and reach first.

2.3.1 The Model

The randomized routing strategy investigated in this thesis uses the goal prediction game studied by Tsitsiklis and Xu (2018) in which an adversary attempts to predict the goal destination of the agent. The game consists of the following elements:

1. an undirected graph, $G = (V, \mathcal{E})$ with n vertices, where V represents the possible states of the agent (nodes in the agent's route) and ε is the number of transitions allowed at each step;
2. an initial agent state $x_1 \in V$;
3. a probability distribution π, used to generate a V-valued random variable D, with components $\pi_v = P(D = v)$;
4. auxiliary collections of independent random variables R_A and R_D, used for randomization for the agent and adversary, respectively.

2.3.2 Agent Trajectory and Strategy

Tsitsiklis and Xu (2018) define both a trajectory and a strategy for an agent. The agent's trajectory is a sequence of random variables that is set prior to the departure of the agent from X_1. This strategy does not change as the agent proceeds from its start node to goal node. The strategy, Ψ, creates the agent's path based on the value of the random variables D and R_A (Tsitsiklis and Xu 2018).

Ultimately, the agent's goal is to reach the destination node prior to the adversary. The measure of effectiveness of the goal prediction game is the goal-reaching time, denoted by

$$T_\Psi = min(t \in \mathbb{N} : X_t = D) \tag{2.4}$$

and $T_\Psi = \infty$ if the agent does not reach the goal. If the agent does not reach the goal, then the adversary has discovered the agent's goal and reached it first. In all cases where the agent succeeds in reaching its goal, the agent is successful but incurs some delay due to the directness of the path by which it reached the goal. Shorter paths result in increased predictability and a lower probability that the agent will succeed, while longer, less direct paths increase the delay by which the agent succeeds, but decrease the probability that the adversary can successfully identify the goal destination. The delay of the agent's strategy is represented by $E(T_\Psi)$ and is fully dependent on the randomness of D and R_A (Tsitsiklis and Xu 2018).

2.3.3 Adversary Trajectory and Strategy

Unlike the agent's strategy, which is set from time step $t = 1$, the adversary considers all previous agent actions before determining its next step. That is, at time t, the adversary knows the layout of the graph, all previous positions of the agent $X_1, ..., X_t$, and the random variable R_D. Using this information, the adversary evaluates an associated decision random variable, $\hat{D}_t \in V \bigcup \{0\}$. $U_{\Psi,\mathcal{X}}$ represents the respective strategies of the agent and adversary at the first time the adversary allows $\hat{D}_t$ to become an element of V (Tsitsiklis and Xu 2018). In other words,

$$U_{\Psi,\mathcal{X}} = inf(t : \hat{D}_t \in V). \tag{2.5}$$

The adversary's prediction of the agent's destination, $\hat{D}_{U_{\Psi,\mathcal{X}}}$, is correct if it occurs prior to the goal-reaching time of the agent. The probability of the adversary correctly identifying the destination, D, is the prediction risk, denoted by

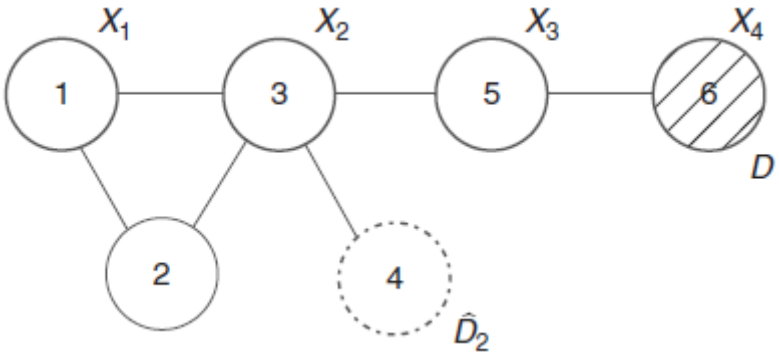
$$q(\Psi, \mathcal{X}) = \mathbb{P}(\hat{D}_{U_{\Psi,\mathcal{X}}} = D \text{ and } U_{\Psi,\mathcal{X}} \leq T_\Psi). \tag{2.6}$$

Ultimately, the adversary seeks to maximize the prediction risk while the agent seeks to minimize the prediction risk based on the amount of time that it attempts to reach the destination in. The result produces a trade-off between the speed at which the agent can reach its destination versus the risk of the agent being unsuccessful (Tsitsiklis and Xu 2018).

Figure 2.2 is a graphical representation of deterministic randomized routing as described in the goal prediction game.

Tsitsiklis and Xu (2018) demonstrated that the randomized routing strategy can be detrimental to an adversary's ability to accurately predict the agent's goal destination. This thesis incorporates a similar routing algorithm to generate a set of candidate paths for a potential decoy UxV to follow. Once the candidate path is selected, the data is incorporated into the MTX data set and GFT model to determine the effectiveness of this strategy in a real-world environment.

Figure 2.2. An example of the goal prediction game. Source: Tsitsiklis et al (2018).



CHAPTER 3:
Methodology

The ultimate goal of this research is to produce routes for a decoy UxV that worsen an adversary's ability to accurately predict the true location of ground forces. We assume that the adversary uses the prediction model by Wigington (2021). Using this method, 75 meters is the maximum error between red cell predicted location of NSW forces and the actual location of NSW forces. Any results from randomized routing strategies that increase this prediction error indicate some level of success. In order to accomplish this, the randomized routing strategy developed by Tsitsiklis and Xu (2018) described in Section **??** is used to create a series of decoy paths. The routes of the decoy UxV are translated from a discrete, graphical format, to continuous, and then incorporated into the GFT model which uses UxV positions to predict the ground force positions. The time series linear regression model represents the Red Cell's attempt to locate ground forces whereas the randomized routing strategy represents is used by the Blue Cell in order to deceive the Red Cell model.

Section 3.1 introduces the MTX data set used to develop the time series linear regression model and in this thesis. Section 2.3 provides a discussion of graph theory as it applies and describes the application of the deterministic routing strategy introduced in Chapter 2 to randomized decoy UxV path generation and selection. Section 3.4 illustrates the fully incorporated routing strategy, required data transformation, and implementation through the time series linear regression model. Finally, Section 3.5 provides a summary of the methodology used to conduct this algorithm.

3.1 MTX Data Set

(Wigington 2021) focuses on the examination of the MTX dataset from the viewpoint of an adversary who has gained unauthorized access to the data, with the intention of uncovering the TTP employed by U.S. military forces. Here, the data set is analyzed from the perspective of the blue cell in order to thwart any information gained by an adversary. Assuming that the adversary was able to capture vital information, the data is used to counter and combat any maliciously actions that may be taken against DOD forces. The MTX data set consists

Table 3.1. MTX data set "X" and "Y" coordinate components. Data for each agent comprising the NCS is broken down into two-dimensional coordinates. Adapted from Lowry (2020), Wigington (2021).

X-coord	Y-coord
NSW.X	NSW.Y
UAV1.X	UAV1.Y
UAV2.X	UAV2.Y
UAV3.X	UAV3.Y
USV1.X	USV1.Y
USV2.X	USV2.Y
DDG1.X	DDG1.Y

of 7005 observations, taken every second, of 14 components. There are three UAVs, two USVs, one Guided Missile Destroyer (DDG) and the NSW ground forces. Observations for each component are recorded in two-dimensional X and Y coordinates. Table 3.1 shows the original data set. This data will be supplemented by the decoy UxV path determined from the randomized routing algorithm.

Table 3.1 variables are shown in pairs. Each row represents the X and Y coordinates for the NSW unit, UAV1, UAV2, UAV3, USV1, USV2, and DDG units.

To illustrate the space and scale in which the MTX occurred, the full data, showing both predictors and excluded variables, appears in Figure 3.1. Note that UAV2 is stationary at the point (91,122) for the duration of the exercise.

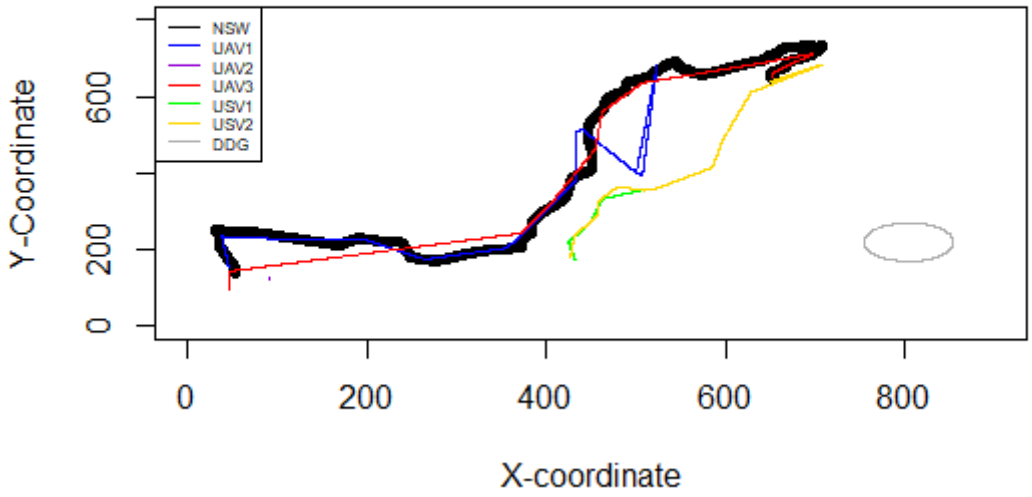
3.2 Randomized Routing

This section discusses the implementation of the randomized routing strategy from Tsitsiklis and Xu (2018). First, relevant aspects of graph theory will be discussed and the algorithm demonstrated on a two-dimensional 3x3 lattice graph shown in Figure 3.2.

3.2.1 Graph Theory

Graph Theory is the study of how mathematical relationships can be represented and studied through the use of graphs and their characteristics. For a detailed discussion of graph

Figure 3.1. Visualization of MTX data. The thick black line shows the NSW's path during the exercise. Each colored line represents one of the five UxVs and the DDG.



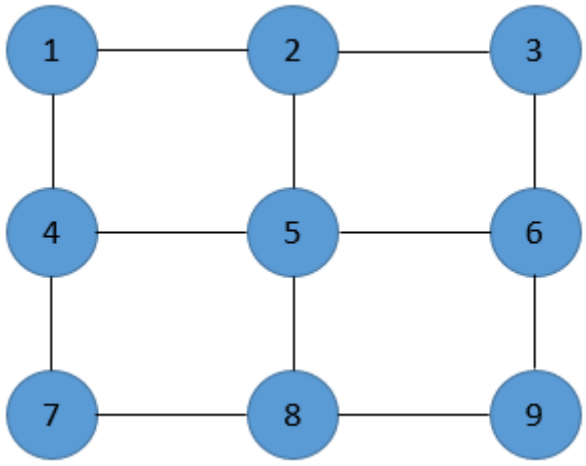
theory, see Mesbahi and Egerstedt (2010). As discussed in Chapter 2.3, graph theoretic modelling is a very useful tool when discussing randomized routing strategies. NCS can easily be represented through graph theory either by establishing nodes as agents and agent connectivity as edges or by laying out the physical environment in which the agents operate as nodes in order to develop routing for the agents. This thesis uses graph theory in the latter way, where nodes and edges represent the physical environment in which the NCS agents operate. In this thesis, we have several assumptions on graphs we use.

First, the graph that we use in this research must be connected. That is, for each node there must exist some path to every other node in the graph (Ahuja et al. 1993). The graph constructed here represents the physical environment in which the NCS operates and is a connected graph. Figure 3.2 illustrates a small-scale version of the connected graph used for this analysis. Figure 3.9 shows the full scale graph. The full-scale graph represents a 300 x 300 node graph based on theMTX data in which the total scale is 750 meters x 750 meters.

Second, the graph which we use in this research must be undirected. An undirected graph is defined as a graph in which edges are unordered pairs of connected nodes. Every arc (i, j) can also be represented as arc (j, i) (Ahuja et al. 1993). Figure 3.2 illustrates an undirected graph, that is, the UxV traversing the graph between any pair of adjacent nodes can travel in either direction. For example, the UxV can travel between nodes 1 and 2 either by way of edge $(1, 2)$ or edge $(2, 1)$. A connected and undirected graph establish the basic elements of the graph from which randomized routing strategies can be generated. The graph is defined by Equation 3.1, where G represents the graph, V represents the nodes of the graph, and $\mathcal{E}$ represents the edges between nodes as

$$G = (V, \mathcal{E}). \tag{3.1}$$

Figure 3.2. Small-scale graph example consisting of nine nodes connected by edges represented as lines.

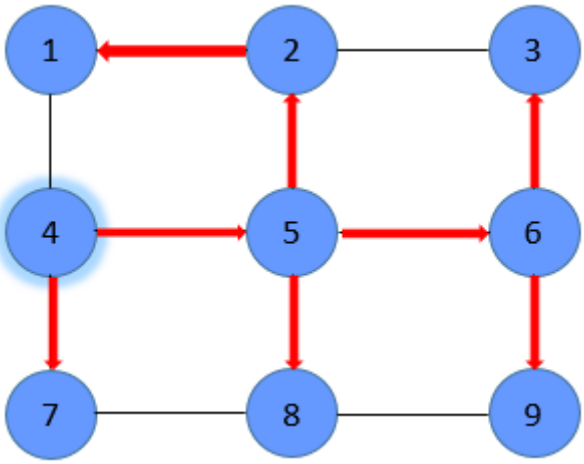


Third, we state definitions of cycles, trees, and spanning trees. A cycle is a path in a graph, or a sequence of edges that connect a sequence of nodes that begins and ends on the same node (Ahuja et al. 1993). Cycles can be either directed or undirected. A tree is an acyclic, connected graph with one path between any two nodes. Finally, a spanning tree is defined as "a tree (i.e., a connected acyclic graph) that spans (touches) all the nodes of an undirected network" (Ahuja et al. 1993, p. 8). The spanning tree is the crux of the random routing strategy analyzed in this thesis. In order to establish the framework for the UxVs randomized

route, a random spanning tree of the graph is generated. The spanning tree of graph, G is defined by Equation 3.2, where H represents the spanning tree, V represents the nodes of the spanning tree, and $\mathcal{E}_H$ represents the edges of the spanning tree as

$$H = (V, \mathcal{E}_H). \tag{3.2}$$

Figure 3.3. Small-scale spanning tree example. Red arrows represent the tree overlaid on top of the nine-node graph from Figure 3.2.



The degree of each node in a graph is also relevant to implicitly understand how the UxV is allowed to traverse the graph. The degree of a node in an undirected graph is the number of arcs incident to the given node (Ahuja et al. 1993). Figure 3.9 shows the graph we used in this research. It illustrates that a majority of the nodes have a degree of four while the nodes that comprise the "border" of the graph have a degree of two for the four corners of the graph and three for those in between the corners. In other words, the only directions in which the UxV is allowed to move at each timestep are north, south, east, or west.

The diameter of a graph is the length of the shortest path across the entire graph. In other words, it is the largest distance between two nodes in the graph. The diameter is an important metric for determining the length of the randomly generated routes for the UxV. It provides a lower bound for the length of the randomized routes from which are sampled. This is for several reasons. First and most importantly, it is a tuning parameter for how far the decoy is allowed to move. This tuning parameter can be based on a variety of characteristics,

depending on the specific type of UxV being used, including fuel and speed. Second, this ensures some minimum coverage across the graph when establishing a set of candidate decoy UxV paths. The diameter of the graph in Figure 3.2, which will be used to illustrate the route generating algorithm is four. This means that the minimum path length for routing in the example is four. The maximum path length is undefined in the example shown in Figures 3.2 to 3.5 because the example is not correlated to any real world data set. Therefore, path length is set to $r = 4$ for the purpose of visualizing the algorithm on a conceivable scale.

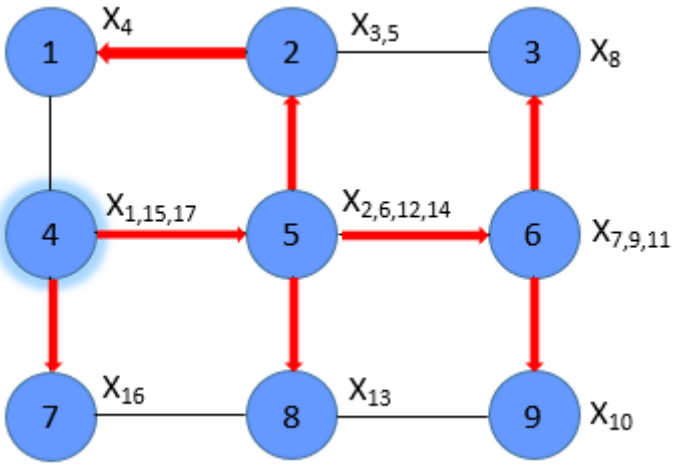
3.2.2 Depth First Traversal

The next step is to conduct a Depth First Traversal (DFT) of spanning tree H. The DFT algorithm is very similar to the Depth First Search (DFS) algorithm. In both DFS and DFT, a recursive algorithm is used to search the entire graph. Each time that a node is visited, DFS and DFT examine that nodes adjacency list and transits to an adjacent node depending upon whether the adjacent nodes have already been visited or not. If one or more nodes in the adjacency list have not yet been visited, the DFT algorithm will transit to the lowest numbered unvisited node. For example, in Figure 3.4, node 4 is the start node, X_1. Its adjacency list consists of nodes 5 and 7, which have not yet been visited. Therefore, the next step, X_2, will be to node 5. If node 5 had been explored, but not node 7 (i.e., at X_{15} = node 4), then the next step would be X_{16} = node 7. If all nodes have been explored previously, such as at X_{16}, the next step would be to return up the tree to the parent node, $X_{17} = node4$. However, whereas DFS simply keeps track of the order in which all nodes are visited, DFT keeps track of all nodes in the order they are visited, and regardless of how many times they have been previously visited, not only the order of visitation. This results in a list of all nodes as they are visited, starting and ending at the start node (node 4 in this example). The DFT, h, produces a list of nodes of length $2n - 1$, where n is the number of nodes in graph G.

3.2.3 Path Generation

The path generation process produces a set, S, of candidate UxV paths from which to choose. After creating a list of nodes via DFT, a path length must be determined in order to create the set of candidate paths to choose from. Path length is defined by r, which is

Figure 3.4. Small-scale tree traversal algorithm example (start node = 4). X_i represents the position of the UxV at time i.



restricted on the lower bound by the diameter of the graph and on the upper bound by the number of observations in the data set. The path length, r determines the number of possible routes to sample from. Smaller r values generate a larger quantity of routes whereas larger r values generate fewer possible routes. The number of candidate paths is equivalent to the length of h divided by r. We conduct a path generation where candidate routes are defined as $p(i)$ and it is represented by the sequence as

$$p(i) = h_{(i-1)\cdot r+1}, ..., h_{ir}, \tag{3.3}$$

where i is a uniform random variable between

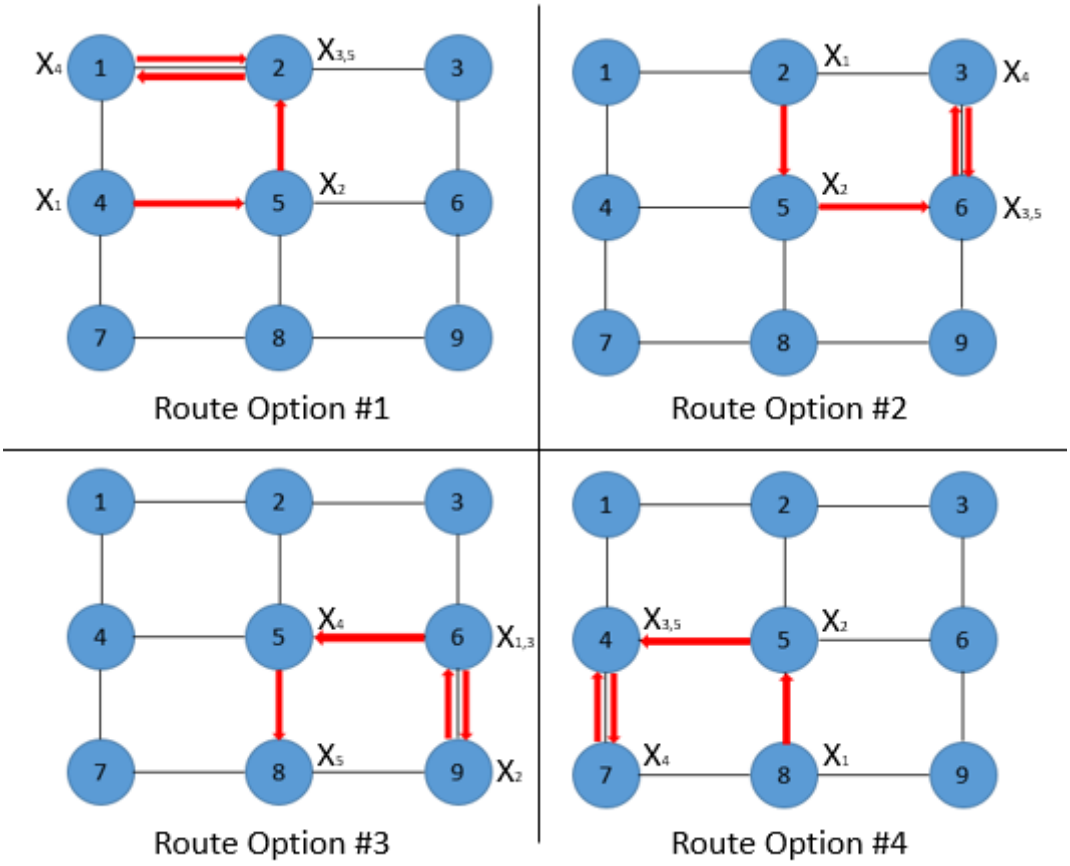
$$i \sim U(1, \frac{(2n-1)+(r-1)}{r}). \tag{3.4}$$

Each candidate UxV path has a goal state, defined by D. This is the final node in every candidate path. Naturally, the fastest path for the UxV to reach its destination is through the shortest path algorithm. However, following the shortest path is often much more indicative of the true goal destination. Randomized routing seeks to perturb the route from the simple shortest path between the start node and goal node in order to increase the adversary's

prediction error. By constructing a spanning tree and varying the path length, wildly variant paths of different shapes and sizes are generated that all ultimately reach the UxVs goal state, D, and provide unique candidate paths. The UxVs goal state is set to the last node of each candidate path to maintain consistency between candidates.

The sequence in Equation 3.3 represents the first r terms of h, second r terms of h, etc, and the $i^t h$ route in the set of routes $p(i)$ then becomes the route that the decoy UxV will take. In the small-scale example provided in Figure 3.5, path length, r, was simply set to $r = 4$ for illustrative purposes. If the uniform random variable in the small scale example is $i = 3$, then "Route Option 3" becomes the route taken by the decoy UxV.

Figure 3.5. Sample of four candidate paths from set of candidates, where r = 4. Red arrows show individual candidate paths and X_i shows the time, $i > 0$, at which the UxV is present at each node along the candidate path.



In the small-scale example provided, there is no translation to the GFT model. This section serves to provide the algorithm that generates the decoy UxV route and use an illustrative example for clarity.

3.2.4 Path Length Restrictions

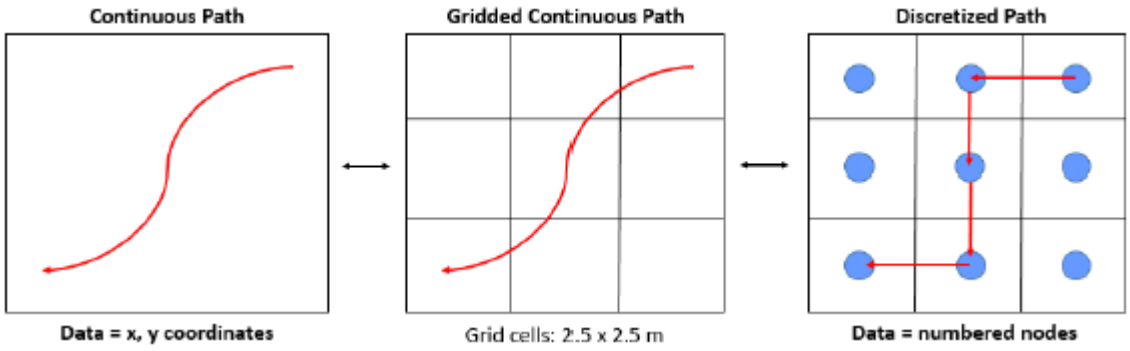
The diameter of the 300 by 300 nodes graph used in this analysis, shown in Figure 3.9, is 598. As implemented in the Tsitsiklis and Xu (2018) algorithm, this sets the lower bound of the path length, r to 598. The upper bound for the length of the route is determined by the number of observations in the MTX data set. This is because the route can be no longer than number of observations in the original data, 7005, in order to test the GFT. The bounds of r are therefore set by the inequalities in Equation 3.5.

$$598 \leq r \leq 7005. \tag{3.5}$$

3.3 Data Transformation

In order to use the decoy UxVs path generated from the randomized routing strategy, each node of the path must be transformed from a list of numbered nodes to the continuous space in which the MTX data set exists. This is accomplished through the procedure illustrated in Figure 3.6. The framework for this transformation an established grid system that encompasses both the entire MTX data set and all nodes of the graph. This grid is 750 meters by 750 meters with an equal number of grid squares as nodes in the graph. The 90,000 nodes (300×300 graph) is laid on top of the grid system, creating 2.5 meter by 2.5 meter individual grid squares. Since the focus is testing the decoy UxV against the established adversarial model, this transformation only occurs on the routes and data generated by the randomized routing strategy. The transformation is conducted consistently for all nodes by always using the centroid of the grid square as the position of any given node. Importantly, the coordinate data is not used in terms of longitude and latitude. MTX coordinate data is based on a local point in the exercise area, therefore the data transformation converts nodes into the desired format. For example, if the decoy were to traverse from node 1 to node 2, the decoy will transit from coordinates (1.25, 748.75) to (3.75, 748.75).

Figure 3.6. Data transformation procedure. Data transformation takes overlays the graph onto the coordinates used in the MTX and converts UxV candidate paths from a list of discrete numbered nodes into coordinates.



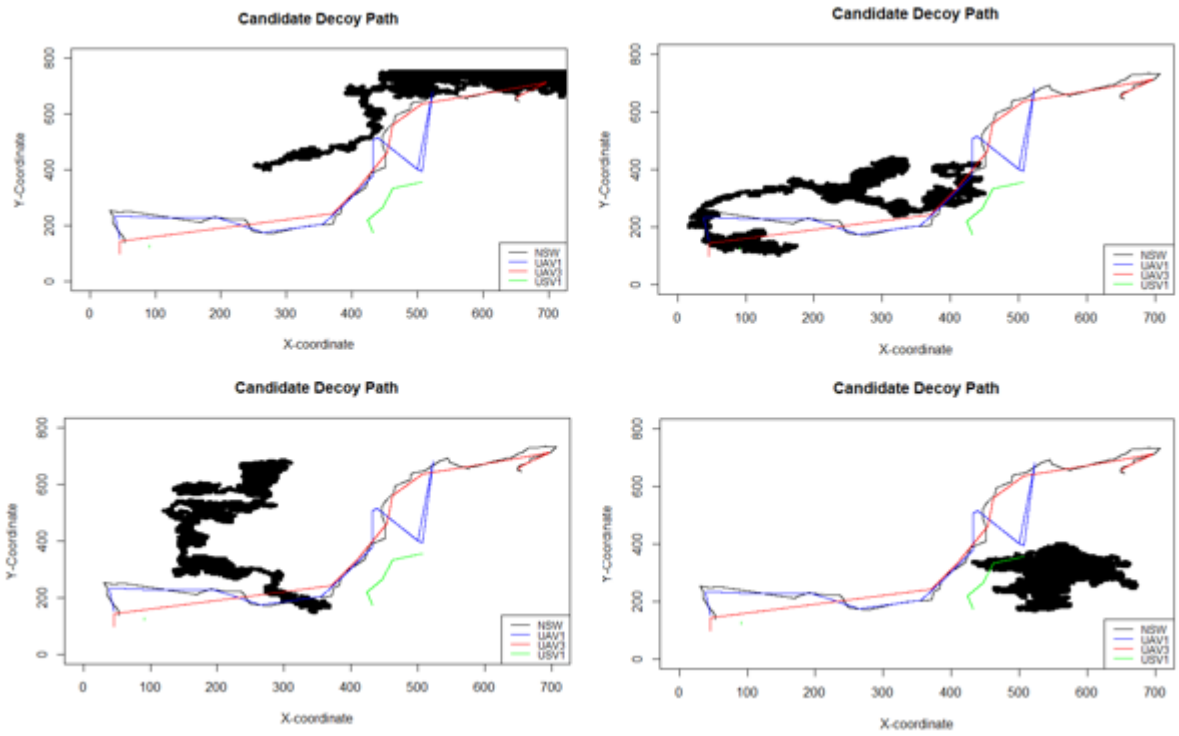
Once the data transformation process is complete, the candidate decoy UxV paths are in an x and y-coordinate format compatible with the MTX data and incorporated into the data set. Figure 3.8 illustrates a single candidate path after data transformation and plotted with the predictors used in the red cell analysis.

3.4 Implementation

Once $p(i)$ is determined via Equation 3.4 and transformed as shown in Figure 3.6, the decoy route is then tested at every $t = 120$ time steps. Using a path length of 7005, there are 58 observations tested.

The route is fed into the adversary's GFT model in equations 2.2 and 2.3. This suggests that there are three possible UxV positions that the decoy can be implemented in the model. The decoy route can either be incorporated into the GFT model in the $UAV1.X$ and $UAV1.Y$ position, $UAV3.X$ and $UAV3.Y$ position, or $USV1.X$ and $USV1.Y$ position. Assuming that it is unknown where the decoy UxV will be incorporated into the model, the decoy UxV route is analyzed three times, replacing $UAV1$, $UAV3$, and finally $USV1$ in order to determine the range of possible outcomes. Equations 3.6 through 3.11 depict how the decoy UxV route is tested. The selected path is simply implemented in the position of each predictor variable independently. In all equations, $\beta_{i,j}$ is unchanged and are the same regression coefficients determined by Wigington (2021)'s time series linear regression model.

Figure 3.7. Sample from set of candidate paths, r = 7005. This figure shows four of 25 candidate paths available when using a path length of 7005.



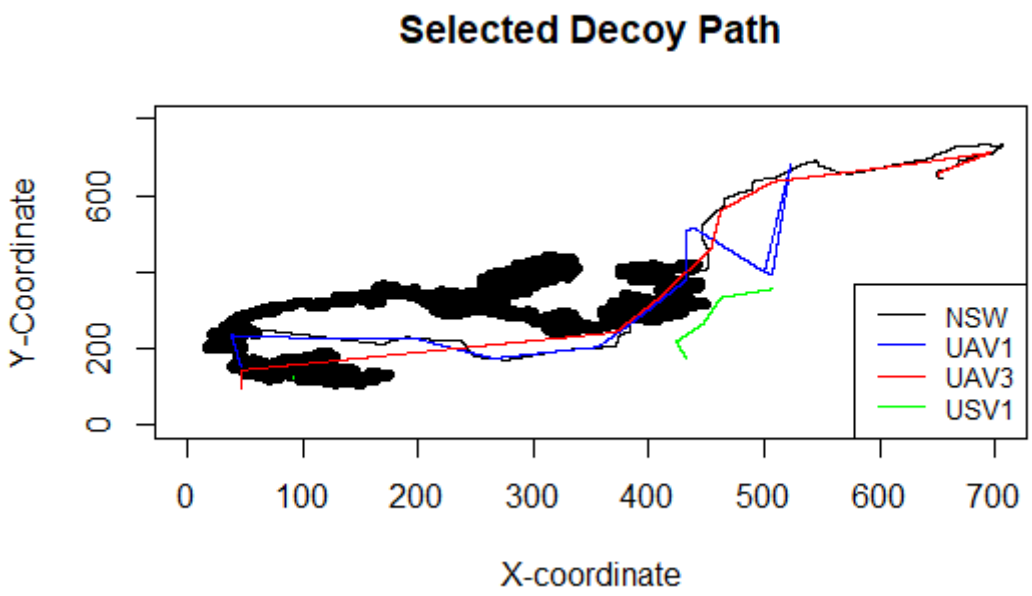
The X and Y coordinates of the candidate paths are tested through the GFT model as denoted in 3.6 and 3.7, respectively, to provide results position predictions of the GFT model where UAV1 is replaced by decoy data. This is one of three iterations of the GFT model through which candidate paths are tested,

$$NSW.X = \beta_{11} \cdot decoyUxV.X + \beta_{12} \cdot UAV3.X + \beta_{13} \cdot USV1.X, \tag{3.6}$$

where $\beta_{11}, \beta_{12}, \beta_{13} \in \mathbb{R}$ are coefficients for predictors $decoyUxV.X, UAV3.X, UAV1.X$, respectively, and

$$NSW.Y = \beta_{21} \cdot decoyUxV.Y + \beta_{22} \cdot UAV3.Y + \beta_{23} \cdot USV1.Y, \tag{3.7}$$

Figure 3.8. Selected decoy UxV path from set, S, r = 7005. This figure shows the randomly selected candidate path from the set of candidate paths overlaid onto the MTX data.



where $\beta_{21}, \beta_{22}, \beta_{23} \in \mathbb{R}$ are coefficients for predictors $decoyUxV.Y, UAV3.Y, UAV1.Y$, respectively.

The second iteration of the GFT model is shown in equations 3.8 and 3.9. Here, the candidate paths are ran through the model in the position of the UAV3 predictor. The $\beta_{i,j}$ coefficients for each predictor, including UAV3 replaced with decoy data, are not changed.

$$NSW.X = \beta_{11} \cdot UAV1.X + \beta_{12} \cdot decoyUxV.X + \beta_{13} \cdot USV1.X \tag{3.8}$$

$$NSW.Y = \beta_{21} \cdot UAV1.Y + \beta_{22} \cdot decoyUxV.Y + \beta_{23} \cdot USV1.Y \tag{3.9}$$

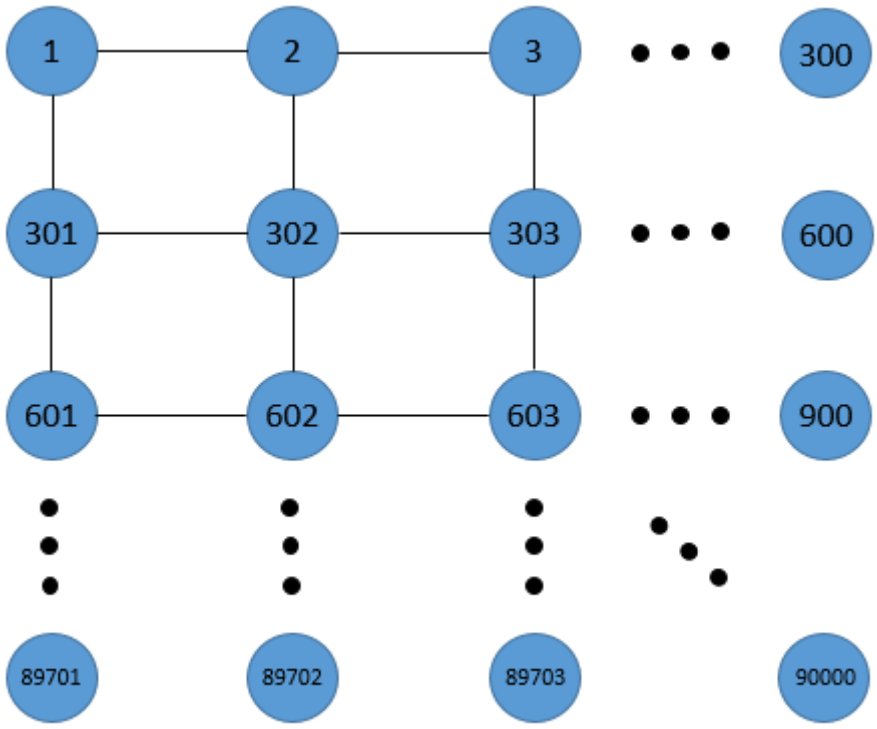
Lastly, the candidate paths are tested in the GFT model in the position of the USV1 predictor. $\beta_{i,j}$ coefficients remain unchanged.

$$NSW.X = \beta_{11} \cdot UAV1.X + \beta_{12} \cdot UAV3.X + \beta_{13} \cdot decoyUxV.X \tag{3.10}$$

$$NSW.Y = \beta_{21} \cdot UAV1.Y + \beta_{22} \cdot UAV3.Y + \beta_{23} \cdot decoyUxV.Y \tag{3.11}$$

Further, testing this randomized routing strategy on the single UxV may not encompass the quality or lack thereof of this deceptive approach due to randomness. There is a significant amount of randomness inherent in the generated spanning tree, the path length being tested, and in the uniform random variable, i, that determines which candidate route is selected. Due to this, one candidate route, if selected, may perform much worse than a different candidate route. With the ultimate goal of testing the routing strategy as a whole, it is therefore necessary to analyze each and every candidate path through equations 3.6 to 3.11.

Figure 3.9. Actual graph dimensions. The graph used for analysis is 300 by 300 nodes, totalling 90,000 nodes, overlaid onto the 750 by 750 meter space the MTX occurred.



3.5 Summary

This chapter uses the randomized routing strategy from Tsitsiklis and Xu (2018) to counter an adversary who maliciously acquired DOD exercise data to develop a forecasting and prediction model of ground forces. Randomized routing has the ability to add a layer of deception in U.S. Navy (USN) and DOD planning and execution that is not present in the MTX data acquired and used by an adversary. This strategy is used to determine an UxV route to be used as a decoy and incorporated into TTP. The algorithm is explicitly defined in the Appendix.

CHAPTER 4:
Application, Results, and Analysis

This chapter takes the randomized routing strategy discussed in Chapter 3 and applies the resulting candidate paths to the GFT model to determine the effectiveness of incorporating decoy UxVs into mission planning. In Wigington (2021) the mean red cell position prediction error was 39 meters and the maximum prediction error was 75 meters. Therefore the measure of success is to achieve greater than a 75 meter prediction error when incorporating randomized routing strategies, with the goal of producing the highest possible red cell prediction error.

Section 4.1 describes the methods of evaluation for this randomized routing strategy. Section 4.2 discusses the application of random routing to the GFT model. Section 4.3 introduces the resulting prediction errors produced from the application of randomized routing strategies. Section 4.4 provides a summarized overview of Chapter 4

4.1 Methods of Evaluation

The effectiveness of randomized routing strategies to prevent an adversary from tracking and predicting ground force positions can and should be observed in several ways. First, a destination focused approach reveals the adversary's ability to predict and determine the target destination of NSW forces. Second, a holistic approach identifies an adversary's ability to track NSW forces throughout a mission or exercise from start to finish. Both methods of evaluation are important and provide relevant information on an adversary's capabilities and the effectiveness of introducing deceptive routing strategies in UxV route planning.

4.1.1 Destination Effectiveness

One of the goals of incorporating randomized routing strategies into UxV paths is to reduce an adversary's capability to identify the ground force's ultimate destination. In order to determine the effectiveness of randomized routing specifically concerning the goal destination, all observations other than the final observation are ignored. This leaves the

decoy UxV route's destination node and other associated predictor UxV goal nodes as the only considered observation. In short, the last time step is the only observation considered to determine the red cell prediction of the NSW team's destination. Analyzing only the final observation provides results that indicate the usefulness or lack thereof of using randomized routing strategies to obfuscate the ground force's ultimate destination.

4.1.2 Entire Route Effectiveness

Another useful method of evaluation examines the effectiveness of deceptive routing applied to the entire exercise. That is, all observations for a candidate path are tested through the GFT model. This provides a red cell prediction of the NSW position at every observation. Using a path length of 7005, the set of resulting 25 candidate paths are tested at every 120 seconds, providing 58 observations to test against the GFT model.

4.2 Randomized Routing Strategy Applied

There are several elements of randomness that necessitate an "overall" approach to analyzing this deceptive routing strategy. First, due to the random nature of selecting a single path from a set of candidate paths, it is prudent to analyze this routing strategy as a whole. That is, each candidate path is analyzed individually as opposed to analyzing the single selected candidate path. Analyzing each candidate path reveals the overall viability of the routing strategy whereas analyzing the single randomly selected path provides a lone result that may not be indicative of the true nature of this strategy. Figure 4.1 illustrates the variability between individual candidate paths.

Also, each candidate path is tested against the GFT three times. The GFT model uses three predictors to forecast the NSW team's position, UAV1, USV1, and UAV3. Each candidate path is tested as a decoy for each of three predictors.

4.3 Analysis of Randomized Routing Strategy

The bounds on r provide a wide variety of possible candidate path lengths. Determining the most effective r is a trial and error process. In practice, as r is adjusted, results vary drastically. Lower values of r tend to result in very localized UxV routes. That is, routes

are generally confined to a small portion of the 300 x 300 graph, G. This tends to produce worse results than a more geographically dispersed path length. With longer path lengths, the decoy UxVs route is much broader across graph G and produces better prediction results for ground forces.

Since the GFT identifies three predictors, UAV1, UAV3, and USV1, the blue cell can not be certain how the decoy will be incorporated into the red cell model. To determine the effectiveness of the decoy UxV, the decoy is tested against the model three times by replacing each predictor from the original GFT model. This provides a best and worst case scenario for the red cell's incorporation of the candidate paths into the GFT.

4.3.1 Entire Route Prediction Error

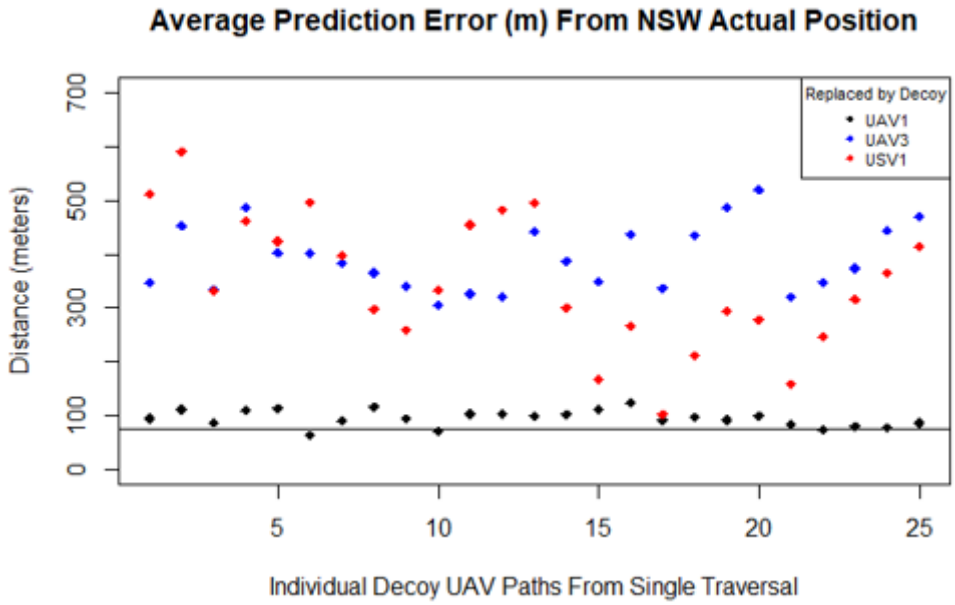
Figure 4.1 illustrates each candidate path from the set of candidate paths tested through each predictor to provide the average red cell prediction error over the course of the entire exercise. The results shown in Figure 4.1 are derived from a path length, $r = 7005$, as testing indicated this to be the most successful path length. Using this path length, the resulting number of candidate paths is 25, limited by the length of the depth first traversal described in Chapter 3. Therefore, each of the 25 paths is tested three times, for a total of 75 possible route/model combinations.

In Figure 4.1, the red dots show the average prediction error of each individual candidate path incorporated into the GFT through the USV1 predictor, the blue dots as UAV3, and the black dots as UAV1. The horizontal black line represents the maximum position prediction error, 75 meters, determined by the GFT during Wigington (2021)'s research, or the target to beat.

Of the 75 route/model combinations, only two routes resulted in an average prediction error of less than 75 meters over the course of the entire exercise and none of the candidate paths produced results less than the mean prediction error of 39 meters. This suggests that the deceptive routing strategy, regardless of implementation into the red cell model, can be effective. In this case, using the MTX data set, this deceptive routing algorithm is often very effective over the course of the exercise.

The inherent randomness between individual candidate paths can also be seen in Figure

Figure 4.1. Average red cell prediction error of all observations for each candidate path tested in place of each predictor from the GFT model. Red, blue, and black points show the results when the decoy replaces USV1, UAV3, and UAV1, respectively.



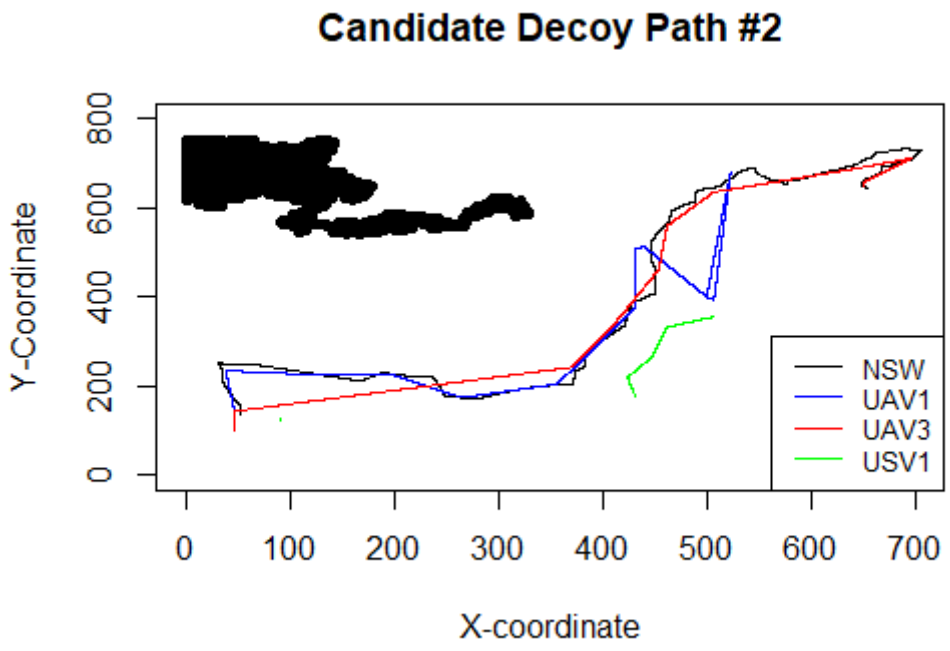
4.1. Notably when observing the decoy UxV implemented via USV1. Candidate paths two and 17 clearly illustrate this potential disparity between paths, where Path 2 produces an average position prediction error of over 600 meters and Path 17 produces an average error of just 100 meters. This is an important consideration when analyzing the effectiveness of deceptive routing strategies from the range of possible candidate paths. Here, both paths indicate an improvement from the original GFT model, however, there are clearly better and worse candidate paths.

4.3.2 Path Length

The disparity between these two candidate paths also reveals why longer path lengths are generally preferable to shorter path lengths using this deceptive routing strategy. Figures 4.2 and 4.3 illustrate the "geographic spread" of each candidate path across the operating area, where Path 2 is spans half of the operating area and Path 17 is essentially confined to a small region of the operating area. When observed individually, a significant majority

of the more "geographically isolated" candidate paths produced smaller red cell prediction errors. With shorter candidate paths, the decoy UxVs were more stationary resulting in a smaller spread across the operating area and ultimately produced worse results for the blue cell. That is, the red cell prediction of blue ground forces was much more accurate.

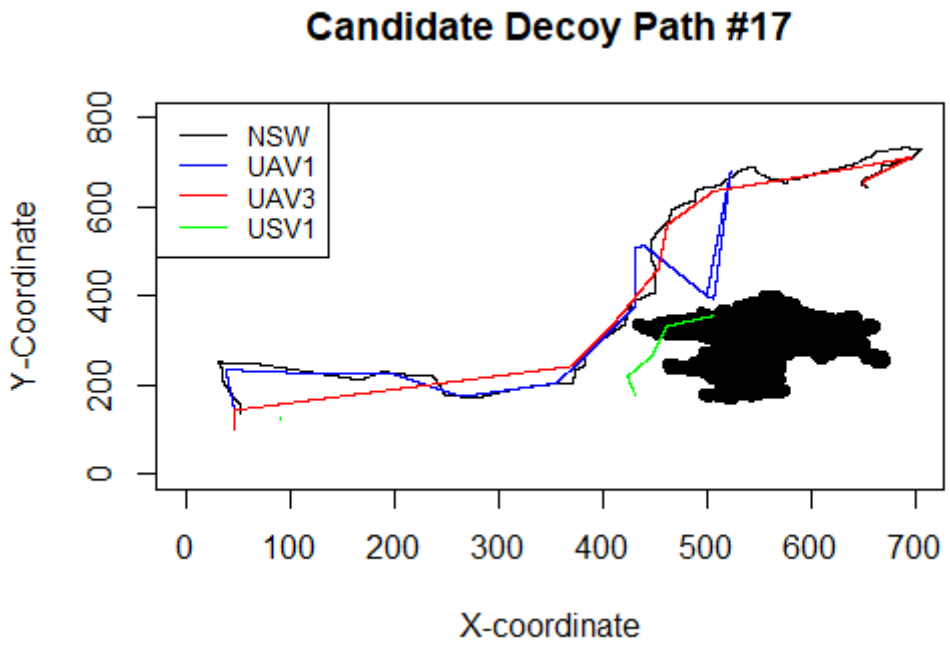
Figure 4.2. Candidate Path 2 plotted with MTX data. The thick black line shows the candidate path. The thin black, blue, red, and green lines show the path of the NSW team, UAV1, UAV3, and USV1, respectively. Note the spread of this path across the geographic space.



4.3.3 Destination Error

One of the primary purposes of this thesis is to develop a deceptive UxV routing strategy to prevent an adversary from identifying ground force's goal destination. This is accomplished by analyzing the final observation for each of the 75 route/model combinations. Figure 4.4 is a box plot of the red cell's final destination prediction error. Each box plot consists of the 25 candidate paths replacement of UAV1, UAV3, and USV1, respectively. The 75-meter maximum position prediction error from Wigington (2021) is shown in red. As with the

Figure 4.3. Candidate Path 17 plotted with MTX data. The thick black line shows the candidate path. The thin black, blue, red, and green lines show the path of the NSW team, UAV1, UAV3, and USV1, respectively. Note the isolation of this path in the geographic space.



average prediction error over the entire path, only two candidate paths result in a prediction error worse than 75 meters. Candidate path decoy data inserted into the GFT in place of UAV1 provided the worst results on average; however, the absolute worst results come from candidate paths replacing USV1 and UAV where that result was 83 and 40 meters, respectively.

Table 4.1 provides the mean red cell prediction error for the NSW team's destination, or final position. On average the 25 candidate paths perform exceptionally well at reducing the adversary's ability to predict the ground force's destination.

Figure 4.4. Boxplot of red cell prediction error at final destination for each candidate path. Red line indicates 75 meters.

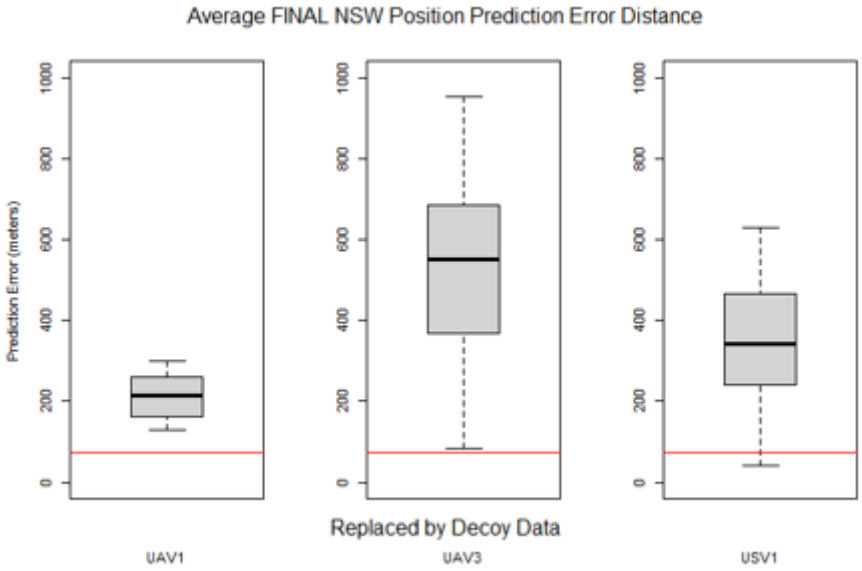


Table 4.1. Mean red cell prediction error of NSW team's final destination using all 25 candidate paths

Replaced by Decoy Data	Mean Prediction Error at Final Destination (m)
UAV1	212.5
UAV3	537.1
USV1	356.1

4.4 Summary

There is a notable degradation in the performance of the time series multiple linear regression, GFT model, when deceptive routing strategies are incorporated. Overall, implementing the randomized routing as each of the three predictors in the GFT produced favorable results for the blue cell and very unfavorable results for the red cell. The UAV3 and USV1 predictors were the most susceptible to deceptive routing, however, UAV1 still resulted in improvements over the initial GFT. The routing algorithm's restrictions on path length also heavily impact results. In most cases, longer path lengths result in larger red cell prediction errors.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5:
Conclusion

This chapter discusses the findings of this research in Section 5.1 and potential future work in Section 5.2.

5.1 Discussion

The DOD and DON will continue to employ UxVs in mobile NCS into the future. To prevent an adversary from gaining an edge on US forces, it is necessary that deceptive UxV routing paired with UxV route optimization continue to develop. This thesis continues work from Wigington (2021) regarding an adversary's ability to accurately track and predict the location of ground forces by exploiting the UxV components of a mobile NCS.

The deceptive routing strategy provides a generic approach to determine if randomness introduced into mobile NCS route planning can be an effective strategy to mask the true position of ground forces. There is a significant amount of variability in the deceptive strategy presented. Each iteration of the algorithm produces a different tree and while the traversal algorithm approaches each tree in the same way, the selected path length introduces additional randomness that can significantly change the adversary's resulting prediction errors.

In this thesis, we did not assume the model developed by Wigington (2021) for the randomized routing strategy. We did not take advantage of any weaknesses inherent in the time series multiple linear regression model. In this research we incorporated the deceptive routing strategy into the GFT and added the decoy data individually as each predictor UxV from the original MTX data to generally observe how the strategy performed. However, if we know that an adversary is using a similar architecture, the approach explored in this thesis presents opportunities for exploitation.

While in this thesis we introduced an application of randomized routing to the MTX data and the Wigington (2021) model, there are potential limitations. Sensing and communications characteristics of each agent in the NCS restrict the viability of some candidate paths on

a large scale. Here, the scale of the exercise was small enough as to not restrict candidate paths, however, if the exercise occurred over a longer period of time or on a larger scale, limitations of the individual UxV sensing and communications ranges could preclude some candidate paths. Table 2.1 shows the limitations of each component in the MTX NCS.

5.2 Future Work

An extension to this work would be a deeper analysis into what types of candidate paths work and what types do not. This strategy, in one or several iterations, generates a wide range of candidate paths with their shapes and sizes. Identifying which types of paths perform better than others can lead to a more exploitative approach to applying this and other deceptive routing strategies. This information could be used to develop a more targeted approach to applying deceptive routing strategies, which could improve the overall effectiveness of the strategy.

Another approach to an adversary known to use a similar model structure would be further examination of which predictors are easiest to target and manipulate. Understanding the weakest component of the adversary's capabilities would allow further exploitation of the model. For example, if it is found that the adversary is particularly susceptible to deception in certain types of data, then the deceptive routing strategy can be optimized to exploit these weaknesses.

APPENDIX: Randomized Routing Algorithm

A.1 Randomized Routing Algorithm

Result: Create a set of randomized candidate paths;

Instruction 1: Create a square graph of size n x n;

Instruction 2: Find a spanning tree of the graph;

Instruction 3: Perform a depth first traversal that starts and ends from the root of your spanning tree and traverses each node in the graph;

Instruction 4: Determine the diameter of the graph;

Instruction 5: Select a path length between the diameter and number of observations in the original data set;

Instruction 6: Add the first path length - 1 nodes of the traversal to the end of the traversal (total length will be: traversal length + path length - 1);

Instruction 7: Generate a set of candidate paths of the path length;

Instruction 8: Randomly sample from the set of candidate paths.

THIS PAGE INTENTIONALLY LEFT BLANK

List of References

Ahuja R, Magnanti T, Orlin J (1993) *Network Flows: Theory, Algorithms, and Applications* (Prentice-Hall, Hoboken, NJ).

Department of the Navy (2021) Science & technology strategy for intelligent autonomous systems. Technical report, Washington, DC, https://nps.edu/web/slamr/-/intelligent-autonomous-systems-science-and-technology-strategy-issued.

Lowry B (2020) Distributed submodular optimization for a uxv networked control system. Master's thesis. Department of Mechanical and Aerospace Engineering, Naval Postgraduate School. Monterey, CA. https://apps.dtic.mil/sti/pdfs/ad1114256.pdf.

Mesbahi M, Egerstedt M (2010) *Graph Theoretic Methods in Multiagent Networks* (Princeton University Press, Princeton, NJ).

Office of the Secretary of Defense (2022) *National Security Strategy* (The White House, Washington, DC).

Tsitsiklis J, Xu K (2018) Delay-predictability trade-offs in reaching a secret goal. *Operations Research* 66(2):587–596, https://doi.org/10.1287/opre.2017.1682.

Wachlin N (2020) Robust time-varying formation control with adaptive submodularity. Master's thesis. Department of Mechanical and Aerospace Engineering, Naval Postgraduate School. Monterey, CA. https://apps.dtic.mil/sti/pdfs/ad1060097.pdf.

Wigington L (2021) Red cell analysis for mobile networked control systems. Master's thesis. Department of Operations Research, Naval Postgraduate School. Monterey, CA. https://hdl.handle.net/10945/69125.

THIS PAGE INTENTIONALLY LEFT BLANK

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California