The Thesis Committee for Kyungtack Oh
Certifies that this is the approved version of the following thesis:

Exploration of Border Security Systems of the ROK Army Using Agent-Based Modeling and Simulation

APPROVED BY

SUPERVISING COMMITTEE:

Supervisor:

David P. Morton, Supervisor

Jae-Yeong Lee

Exploration of Border Security Systems of the ROK Army Using Agent-Based Modeling and Simulation

by

Kyungtack Oh, B.S.

Thesis

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Engineering

The University of Texas at Austin

August 2010

ABSTRACT

Exploration of Border Security Systems of the ROK Army Using Agent-Based Modeling and Simulation

Kyungtack Oh, M.S.E.

The University of Texas at Austin, 2010

Supervisor: David P Morton

This thesis explores a border security system based on agent-based modeling and simulation (ABMS). The ABMS software platform, map aware non-uniform automata, is used to model various scenarios and evaluate the border security system given a set of infiltrators who have evolutionary behavior governed by a genetic algorithm (GA). The GA is used to represent adaptive behavior of the enemy when the friendly force has deployed our border security at a maximum level. By using a near optimal Latin hypercube design, our simulation runs are implemented efficiently and the border security system is analyzed using four different kinds of measures of effectiveness.

ABSTRACT IV

LIST OF FIGURES VIII

LIST OF TABLES X

LIST OF ACRONYMS AND ABBREVIATIONS XI

CHAPTER 1 INTRODUCTION 1

1.1 Background 3

1.2 Scope of the Thesis 5

1.3 Literature Review 6

CHAPTER 2 GOP BORDER SECURITY SYSTEM CONCEPT 10

2.1 Human Resources 12

2.1.1 Fixed Guard Post and Moving Guard Post 12

2.1.2 Reinforcement Troops 15

2.2 Platoon and Battalion Command and Control Center 15

2.3 Surveillance Equipment 16

2.3.1 Thermal Observation Device 16

2.3.2 PVS-7 Night Vision Goggle 18

CHAPTER 3 MODEL DEVELOPMENT **20**

3.1 Why Use Agent-Based Modeling and Simulation 20

3.2 Why Use MANA 22

3.3 Overview of MANA 24

3.4 GOP Border Security System Model with MANA 24

3.4.1 The Operational Environment 26

3.4.2 Infiltrator 28

3.4.3 Human Resources 29

3.4.4 Equipment 30

3.5 Results 31

CHAPTER 4 ANALYSIS UNDER OPTIMIZED INFILTRATOR BEHAVIOR **35**

4.1 The Infiltrator Optimization Problem 37

4.2 GA in MANA 40

4.3 Further Model Description 43

4.4 Simulation Analysis 47

4.5 Conclusion 52

CHAPTER 5 ANALYSIS OF THE GOP BORDER SECURITY SYSTEM **54**

5.1 Measure of Effectiveness 54

5.2 Design of Experiment 56

5.2.1 Overview 56

5.2.2 Important Factors and Range 56

5.3 Model Run 61

5.3.1 Overview 61

5.3.2 Analysis tools 61

5.4 Results Analysis with Statistical Tools 63

5.5 Results 65

5.5.1 Correlation analysis 65

5.5.2 Probability of Enemy Detected (MOE 1) 68

5.5.3 Probability of Enemy Killed (MOE 2) 76

5.5.4 Average Time Length to the Waypoint (MOE 3) 80

5.5.5 Probability of Red Mission Failed (MOE 4) 85

CHAPTER 6 CONCLUSION **89**

APPENDIX A. INPUT PARAMETERS FOR THE GOP BORDER SECURITY SYSTEM MODEL **92**

BIBLIOGRAPHY **96**

VITA **100**

LIST OF FIGURES

Figure 1. DMZ between South and North Korea 10
Figure 2. Configuration of the DMZ 11
Figure 3. Thermal Observation Device (TOD) body, controller, and TV monitor 17
Figure 4. Images of PVS-7 night vision goggles 19
Figure 5. Screenshots from several sample runs of EINSTein 23
Figure 6. Screenshot of the GOP border security system model; time, T, is reported in steps of 5-second unit 26
Figure 7. Terrain and elevation map of the GOP border security system model 27
Figure 8. Terrain edit table in MANA 27
Figure 9. Comparison of detection rates 34
Figure 10. Schematic diagram for the GA 41
Figure 11. Screenshot of GA running in MANA 42
Figure 12. Selecting genes and trigger states 43
Figure 13. Scenario 1 step 1: initiation screen 45
Figure 14. Scenario 1 step 2: blue force detects the infiltrator 46
Figure 15. Red force overcomes the GOP line 46
Figure 16. Results of scenario 1 over time steps 0 to 1000 48
Figure 17. MANA run results of scenario 2, MOE 1 $(w = 1.0)$ 49
Figure 18. MANA run results of scenario 2, MOE 2 $(w = 0.95)$ 49
Figure 19. MANA run results of scenario 2, MOE 3 $(w = 0.90)$ 49
Figure 20. Comparison of each scenario by using quantile box plot 52
Figure 23. Pairwise scatter plots for NOLH design with 20 factors in 129 runs 60
Figure 24. Data process flow 62
Figure 26. VIP score (left) and variable importance score (right) for MOE 1 69
Figure 27. Contour plot for MOE 1 correspond to the detection range and the number of TOD 70
Figure 28. Variability chart and box plot chart for each number of TOD 71
Figure 29. MOE 1 corresponding to the detection distance and the number of TOD 73
Figure 30. Regression tree output for MOE 1 (RSquare = 0.941) 75
Figure 31. Variable importance for MOE 2 76

Figure 32. Contour plot for MOE 2 corresponding to the shooting range and the detection range (default) 77
Figure 33. Variability chart and box plot chart for shooting range 78
Figure 34. Regression tree output for MOE 2 (RSquare = 0.72) 79
Figure 35. Variable importance for MOE 3 81
Figure 36. Contour plot for MOE 3 corresponding to the number of FGP and shooting range as the number of TOD increases 82
Figure 37. Variability chart and box plot chart for number of TOD 82
Figure 38. Variability chart and box plot chart for shooting range 83
Figure 39. Variability chart and box plot chart for number of FGP 83
Figure 40. Regression tree output for MOE 3 (RSquare = 0.705) 84
Figure 41. Variable importance plot for MOE 4 85
Figure 42. Contour plot for MOE 4 corresponding to the number of FGP and shooting range as the number of TOD increases 86
Figure 43. Bivariate Fit and Variability chart for number of TOD and MOE 4 86
Figure 44. Bivariate fit of MOE 4 for the number of FGP as the number of TOD increases 87
Figure 45. Regression tree output for MOE 4 (RSquare = 0.765) 88

LIST OF TABLES

Table 1. The defense readiness condition of the ROK Army (Security, FM 32-1, 2003).....13
Table 2. Number of posts in platoon level at each type of border security (Exact number of post is classified).....13
Table 3. Information on TOD.....17
Table 4. Information on PVS-7 night vision goggles.....18
Table 5. Confidence interval of each design point.....34
Table 6. Detection range of blue and red forces.....44
Table 7. The results of GA for values of three weights in the objective function.....50
Table 8. The results of 500 simulation runs with the best solution for scenario 2 and comparison between scenario 1 and 2.....51
Table 9. Important factors and range of the GOP border security system.....57
Table 11. Requirement for NOLH design (Sanchez, 2007).....58
Table 12. NOLH design with 20 factors and 129 runs.....59
Table 13. Pair-wise correlations between MOEs.....66

LIST OF ACRONYMS AND ABBREVIATIONS

ABMS	**Agent Based Modeling and Simulation**
CCC	**Command Control Center**
C2	**Command and Control**
DMZ	**Demilitarized Zone**
GOP	**General Outpost**
GP	**Guard Post**
ISAAC	**Irreducible Semi-Autonomous Adaptive Combat**
ISR	**Intelligence Surveillance and Reconnaissance**
MANA	**Map Aware Non-uniform Automata**
MDL	**Military Demarcation Line**
MOE	**Measure of Effectiveness**
NOLH	**Nearly Orthogonal Latin Hypercube**
ROK Army	**Republic of Korean Army**
TOD	**Thermal Observation Device**

CHAPTER 1 INTRODUCTION

"We can see how many factors are involved and have to be weighed against each other; the vast, the almost infinite distance there can be between a cause and its effect, and the countless ways in which these elements can be combined."

- Carl von Clausewitz, Prussian military theorist (1780 - 1831)

Border security systems are currently receiving significant attention internationally because of illegal immigrants, drug smuggling and armed conflict. In the U.S., most border security studies aim to optimize the detection rate with diverse assets for preventing such illegal activities on the border between the U.S. and Mexico and between the U.S. and Canada.

Some countries have serious potential for direct armed conflict, which can expand from small-sized engagements to regular war, as exemplified by South and North Korea, Israel and its neighbors and the Kashmir province between India and Pakistan. This study focuses on the border between South and North Korea, the so-called the Demilitarized Zone (DMZ). The DMZ has attracted special interest, particularly in Northeast Asia. In 1950, the Korean War broke out after a surprise attack from North Korean military forces on the west side of the border line. Since 1953, when United Nations (UN) Forces and the

ROK Army recovered the current border line and installed the DMZ to deter physical conflict, this area has historically had a high frequency of skirmishes. Currently, North Korea is still pursuing its national objectives, which are the unification of Korea by force and the construction of one communist country.

In this study, part of the border security system in the DMZ is modeled in MANA (Map Aware Non-uniform Automata) (Galligan et al., 2005), a software system for agent-based modeling, to explore the effects of the current security systems. Past research for the DMZ border security system has calculated detection rates of the enemy using human resources and Thermal Observation Devices (TODs) via probabilistic methods and heuristic algorithms (Sung, 2005). This previous study gives theoretical results with limited surveillance resources but it also has several limitations which cannot represent real DMZ circumstances.

The primary tool we employ in this study, Agent Based Modeling and Simulation (ABMS), has features which overcome these shortcomings. The ABMS approach takes into account the circumstances of warfare, which include networks of agents, adaptation and non-linearity of the battlefield. The major features of ABMS such as interactions between agents and triggered behaviors of agents help formulate the border security model by framing the model in the perspective of the overall system.

1.1 Background

The DMZ is a strip of land running across the Korean Peninsula that serves as a buffer zone between South and North Korea. The DMZ is 155 miles (248 km) long and approximately 2.5 miles (4 km) wide, and is the most heavily militarized border in the world. It cuts the Korean Peninsula roughly in half, crossing the 38th parallel on an angle, with the west end of the DMZ lying south of the parallel and the east end lying to its north.

The 38th parallel was the boundary between U.S.-occupied and Soviet-occupied areas of Korea at the end of World War II. The DMZ was created after the ceasefire of July 27, 1953, when each side agreed in the armistice to move their troops back 2 km from the front line. Since the armistice agreement was never followed by a peace treaty, the two Koreas are still technically at war (Salon Wanderlust, 2000).

Due to this stalemate, a large number of troops are still stationed along both sides of the DMZ with each side guarding against potential aggression from the other. Soldiers from both sides may patrol inside the DMZ, but they may not cross the Military Demarcation Line (MDL). Between 1953 and 1999, over 500 South Korean soldiers and 50 U.S. soldiers were killed along the DMZ due to North Korean hostilities and sporadic outbreaks of violence (Dick, 2008).

Although the North Korean government never acknowledges direct responsibility for any incidents which occurred near the DMZ, these include (Dick, 2008):

- Jan. 1968: Thirty one North Korean commandos crossed the border disguised as South Korean soldiers in an attempt to assassinate President Park Chung Hee at the Blue House. 29 commandos were killed, one committed suicide, and one was captured in this failed mission.

- Nov. 1974: The first of series of North Korean infiltration tunnels under the DMZ was discovered.

- Mar. 1980: Three North Korean infiltrators were killed attempting to enter the South across the estuary of the Han River.

- Jul. 1997: Fourteen North Korean soldiers crossed the MDL line, causing a 23-minute exchange of heavy gunfire.

- May 2006: Two North Korean soldiers entered the DMZ and crossed into South Korea. They returned after South Korean soldiers fired warning shots.

1.2 Scope of the Thesis

This thesis develops and analyzes a model of the ROK Army's border security system, which aims to prevent infiltration of the enemy in the DMZ. The analysis uses a 10×7 km section of the DMZ, representing the area of responsibility of a battalion in the 5th infantry division. This area has been chosen for this simulation experiment for a variety of reasons. First, it is representative of the general terrain and weather of the DMZ. This area is also a place where the ROK Army experimented with a general outpost (GOP) border security system. In addition, this area was infiltrated by an anonymous person in 2003. This event prompted the ROK Army to reorganize the entire border security system.

We develop our border security system model using agent-based simulation (ABS), and formulate our simulation model using the software platform Map Aware Non-uniform Automata (MANA). Our model in MANA is formulated with Fixed Guard Posts (FGPs), Moving Guard Posts (MGPs), TODs, platoon Command and Control Centers (CCCs) and a battalion CCC as available agents. We analyze the border security system in terms of an overall system instead of considering these assets individually.

Our model exploration analyses an efficient experimental design methodology to capture a large number of interactions between agents that may potentially affect the scenario outcomes. The controllable factors mainly include guard post parameters (detection

range), equipment parameters (for the TODs), network parameters (latency and reliability of network) and reinforcement troop parameters (response time, maneuver speed). The only uncontrollable parameters are the enemy parameters (detection range) that characterize infiltration behavior.

The model is run multiple times, varying a large number of design points, i.e., values for the controllable and uncontrollable factors. Then regression analysis, a statistical technique, is used to provide insights to the following questions:

- What is the near optimal behavior of the infiltrator given the maximum border security system?
- Given the limited resources, what are the optimal combinations of sensors, surveillance and command and control (C2) systems to detect, classify and prevent enemy infiltrations into the DMZ?

1.3 Literature Review

Since the 9/11 terrorists attacks, there have been many different kinds of studies on border security systems and other security systems in the U.S., but few studies have been conducted in South Korea. Berner (2004) analyzes the best combination of broad area maritime surveillance, Unmanned Aerial Vehicle (UAV) and Vertical Take-off UAVs

(VTUAVs) through ABMS. Given particular scenarios, Berner explores the validity of future UAV requirements and evaluates the effectiveness of different UAV combinations for the Navy's surface search and control mission. He gives insights into the best number of UAVs, types of UAVs, and tactics that provide increased capabilities. Although this study is not strictly a border security problem, this search and detection problem suggests a methodology to obtain an optimal combination of assets by using ABMS.

In his thesis, Pulat (2005) develops a two-sided optimization model using a mixed integer linear program to minimize the maximum achievable probability of infiltrator escape. He focuses his analysis on the U.S.-Mexico border near Yuma, Arizona. Pulat assumes that the infiltrator can see the U.S. border patrol's preparation and the intruder acts to maximize his probability of escape. Minimizing this maximum probability produces a U.S. border patrol action plan for the worst-case scenario where the infiltrator follows the minimum-risk path. However, this study has two limitations. First, this method does not consider the dependency between more than two surveillance assets, obtaining the detection rate instead simply by summing all the assets. Second, in this model, the infiltrator only moves along a determined path which the friendly force predicted. In contrast to the circumstances on the border between U.S. and Mexico, roadways are not developed in the DMZ area and the infiltrator uses any direction and path to avoid detection.

Yildiz (2009) uses ABMS to explore the effects of using a hand-launched mini UAV along with other assets, such as border patrol agents, surveillance towers, and communication centers. In his research, the results from the different scenarios are created by a nearly-orthogonal Latin hypercube (NOLH) design. He used this sampling technique to find an efficient number of design points, which allow for maximum information to be gained from the smaller simulation experiment. Yildiz makes use of an Excel spreadsheet developed by Sanchez (2005) to construct a NOLH experimental design. Yeldiz also uses comparison tests, linear regression, and regression trees. There are limitations to this analysis, stemming from the fact that Yildiz considers only whether UAVs are present, not the number of UAVs.

Sung (2005) develops a security guard model to calculate the enemy detection rate and develops a TOD model to optimize the location of new equipment for the Korean DMZ border security system. Based on these two models, Sung suggests an integrated model which incorporates the security guard model and the TOD model. The TOD model is in the form of a location-allocation problem and this problem is known to be NP-hard. For this reason, he uses Lagrange relaxation method to find a near optimal solution by using a heuristic algorithm. The results of Sung's security guard model can be compared with the results of the simulation in our preliminary study. While Sung obtains the detection rate of the TOD model, he also comments that a simulation model would have given better results for this problem because his model does not consider the enemy. Instead, his

model solves the location problem given the detection capability of the TOD and a location constraint.

CHAPTER 2 GOP BORDER SECURITY SYSTEM CONCEPT

Along the border between South and North Korea, which is also commonly called the GOP (general outpost) line, six corps guard each sector. The geographic terrain varies significantly along the border. For example, the eastern half of the Korean peninsula consists mostly of mountains. So, the area of responsibility for each of these corps, along with their security systems, also varies. In this thesis, we consider a conventional border security system which is widely used by border security troops. We develop our model based on the security system of the ROK Army field manual (Security, FM 32-1, 2003) and collect information from officers who are currently work in this capacity.

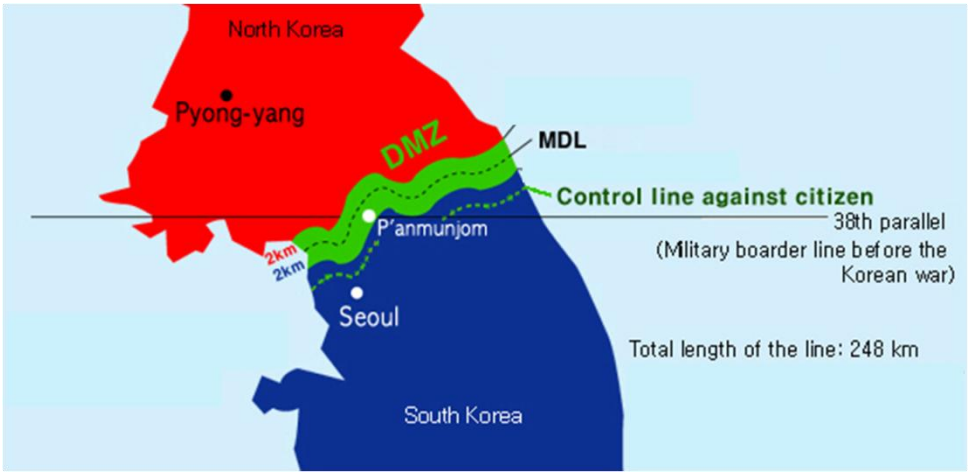


Figure 1. DMZ between South and North Korea

The overall shape of the Korean DMZ is depicted in Figure 1. The length of the DMZ is approximately 248 km (155 miles) and its maximum width is 4 km. About 70% of the Korean peninsula is mountains. The eastern half of the area is especially rugged with multiple peaks in excess of 1000 m. This feature of the terrain makes it difficult for the enemy to traverse and more difficult for the friendly forces to defend. For this study, we selected an area in the middle of the DMZ.

As Figure 2 depicts, GOP lines are formed on each side of the DMZ from the center line, the military demarcation line (MDL). A guard post (GP) depicted in the Figure 2 is a type of security element which is located between the MDL and GOP lines. A GP allows for continuous surveillance and observation of local provocation and infiltration, and can provide the ROK Army with some advanced warning for a surprise attack by the enemy. We do not consider GPs in our study due to their sensitive and classified nature.

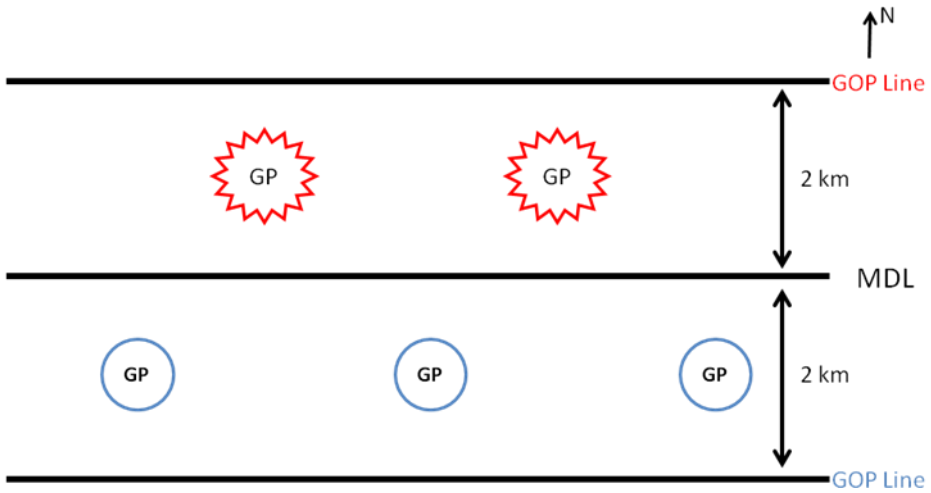


Figure 2. Configuration of the DMZ

The GOPs belong to the division level of the ROK Army, and are located along the GOP line of Figure 2. The GOP's mission is to provide surveillance and warning of the enemy's infiltration through both land and air, and the GOP's mission is also to capture and destroy the enemy before he can reach the GOP line. The security forces in the GOP area combine all the available assets, including human resources, security equipment, border installations and obstacles. With these resources the GOP echelons capture or destroy the enemy before the GOP line and destroy the enemy who passed the GOP line with an interdiction or blockade operation.

2.1 Human Resources

2.1.1 FIXED GUARD POST AND MOVING GUARD POST

There are two different kinds of guard post, fixed guard post (FGP) and moving guard post (MGP). From the FM 32-1, the GOP border security system is operated by platoons, each of which takes responsibility of a width of 2 km. The intensity of the border security system is differentiated by the defense condition as indicated in Table 1, based on the enemy's threat and the current condition of the border (e.g., weather) which affects the surveillance distance.

Defense Condition	Exercise Term	Condition
DEFCON 5	Fade Out	This is the condition used to designate normal peacetime military readiness
DEFCON 4	Double Take	This refers to normal, increased intelligence and the heightening of national security measures
DEFCON 3	Round House	This refers to an increase to force readiness above normal
DEFCON 2	Fast Pace	This refers to a further increase in force readiness just below maximum readiness
DEFCON 1	Cocked Pistol	This refers to maximum readiness.

Table 1. The defense readiness condition of the ROK Army (Security, FM 32-1, 2003)

Using the DEFCON status, the ROK Army adapts the security level to the prevailing condition. For example, at night the border is vulnerable to enemy infiltration due to restricted visibility. For this reason, the number of FGPs and MGPs is increased or decreased depending on the moonlight or thickness of the woods as indicated Table 2.

Border Security Level	Number of Post	Condition
Type A	Day: 0, Night: 0	When enemy detected
Type B	Day: 0, Night: 0	Line of sight is limited (5 days a month)
Type C	Day: 0, Night: 0	Line of sight is good

Table 2. Number of posts in platoon level at each type of border security (Exact number of post is classified)

A platoon is divided into two groups for border security, daytime duty and night time duty. An FGP consists of two sentinels, and after they occupy the FGP for a certain amount of time, they move to the next post in a clockwise fashion. In this way, the group consists of two sentinels who finish their duty and return to their origin, the platoon CCC. The distance between each FGP is different based on the terrain and the predicted route of the enemy's infiltration. A mountain or valley area has a relatively larger number of FGPs, which means one platoon takes charge of less width than the 2 km standard.

The surveillance of sentinels at an FGP is usually fulfilled by their naked eyes. Each sentinel in an FGP separates their surveillance restriction and observes the front along with the predicted infiltration routes and the blind spot. When they use a PVS-7 night vision goggle, it helps to observe up to a range of 200 m at night. Each FGP has one PVS-7 but the sentinels cannot use it continuously because it causes eye fatigue.

The MGP also consists of two sentinels in each group and they patrol along the GOP line periodically. This includes patrol of commanders at levels from the platoon to the battalion. They play a role that complements FGP surveillance, covering blind spots and checking that security wires have not been breached. MGPs are not usually equipped with PVS-7. We return to discuss night vision goggles in greater detail in Section 2.3.2.

2.1.2 REINFORCEMENT TROOPS

When an infiltrator is detected, or a similar situation emerges, the rest of the security forces of the platoon occupy a certain number of predetermined posts based on the operational plan. In our model, the number of soldiers in a reinforcement platoon is assumed to be 30 and they are dispatched when an alarm by a TOD, FGP or MGP triggers them. The reinforcement troops are assumed to have identical capability such as detection rate, weapon range, etc. as the original FGP once they occupy their predetermined post.

2.2 Platoon and Battalion Command and Control Center

A platoon's CCC maintains the situational awareness for the platoon's area of responsibility and maintains constant control and command the border security system. The platoon's CCC maintains the combat readiness for potential emerging situations such as enemy detection or engagement between each force. When the border security level is adjusted upward, the rest of the soldiers in platoon play the role of a reinforcement force, according to the pre-decided operations. Each platoon's CCC also shares situational awareness with the battalion's CCC by reporting through communication equipment and takes orders from the battalion's CCC.

The battalion's CCC plays an analogous role as the platoon's CCC, as a middle level between a platoon and the regiment. They operate surveillance equipment, including the TOD. Based on information from the platoon's CCC and information from the TOD, they observe, assess circumstances, decide and direct rapidly. This command and control (C2) system is a significant part of the border security system because when information, surveillance, and reconnaissance (ISR) assets and striking assets are well connected, the state of the overall border security system is enhanced.

2.3 Surveillance Equipment

2.3.1 THERMAL OBSERVATION DEVICE

A TOD is a thermal screening machine that senses infrared radiation and transforms such signals to a human-readable monitor (Army, Republic of Korea, 2009). TOD equipment is pictured in Figure 3. The TOD equipment allows observation of regions near the border including major access points of routes and blind spots.

Figure 3. Thermal Observation Device (TOD) body, controller, and TV monitor

Table 3 provides further details on the TOD used by the ROK Army. The TOD is attractive in part because of its consistent detection range regardless of weather and other factors that typically degrade range capability. The TOD is battalion level equipment in the current GOP border security system.

Detection Range	Personnel: 3 km Vehicle: 8 km
Operating Temperature	-35~50 °C
Weight	72 kg
Magnification	X 3~10
Unit Price	$180,000

Table 3. Information on TOD

In peacetime, the TOD is operated during the night time. It operates for 2 hours segments with 30-minute breaks for maintaining the equipment's lifetime. It is expensive

equipment as indicated in Table 3, but the ROK Army is currently considering purchasing additional TODs because of their powerful surveillance capability.

2.3.2 PVS-7 NIGHT VISION GOGGLE

PVS-7 represents the current state of the art in night vision goggles which have a single-tube. The goggle assembly is a head-mounted self-contained night vision system containing a binocular unit. The PVS-7 is also currently used by U.S. soldiers in Iraq. Each team of security guards including FGP and reinforcement troops makes use of equipment PVS-7 for border security purposes. But in reality, security soldiers are limited in their use of the PVS-7 because it brings fatigue of the eye easily. Further details of the PVS-7 are as shown in Table 4 and Figure 4.

Detection Range	0.35 km
Operating Temperature	-51 to 52 °C
Weight	0.68 kg
Magnification	X 1
Battery Life	40 hours
Field of View	40°

Table 4. Information on PVS-7 night vision goggles

Figure 4. Images of PVS-7 night vision goggles

CHAPTER 3 MODEL DEVELOPMENT

"War is … not the action of a living force upon lifeless mass … but always the collision of two forces."

- Carl von Clausewitz

3.1 Why Use Agent-Based Modeling and Simulation

For the study of the GOP border security system as described in Chapter 2, we employ the concept of ABMS, which is characterized by agents. In our context, the concept of an agent has important modeling features such as the ability to make a decision, to change its behavior based on a sensor, and to interact with other agents to satisfy certain objectives. ABMS uses multiple agents in a simulation environment. In our model, the surveillance assets and infiltrators in the DMZ are agents. An example of the outstanding effectiveness of ABMS is revealed in its ability to capture group dynamics such as the flocking of birds (Reynolds, 1987). Furthermore, several ABMS software tools such as NetLogo, StarLogo, AnyLogic, etc. are already commercially available.

The features of a complex adaptive system, which is an extension of the concept of a multi-agent system, has much in common with the nature of warfare in that the attrition of forces represent an interaction between agents. Some studies of the Center for Naval Analysis (CNA Analysis & Solutions, 2010), the Seed Center (SEED Center for Data Farming, 2010) and the pioneering work of Ilachinski (2004) demonstrate the possibility

of ABMS to overcome the limitations of the conventional mathematical approach used to model the time-dependent strength of two opposing forces (Lanchester, 1916). The main properties of ABMS that allow it to contribute insight to solve the GOP border security system include the following (Ilachinski, 2004):

- Nonlinear interaction: The contact between infiltrators and security assets occurs based on the nonlinear interaction induced by the surveillance assets, and the agents' decision making process through a hierarchical system;
- Network of agents: A networked system between human resources and surveillance equipment helps share information and triggers the behavior of other agents;
- Triggered behavior: Certain events such as detection and direct or indirect contact with the enemy trigger the behavior of both friendly forces and infiltrators;
- Hierarchical structure: The border security system is organized from the platoon to the battalion with C2 hierarchy; and,
- Adaptation: Both infiltrators and the border security assets continuously sense the environment and change their behavior.

For further discussion of these five properties, along with further properties that can be captured by ABMS, see Ilachinski (2004). The five properties listed above differentiate

this study from previous work (Sung, 2005) for the GOP border security system. Chapter 4 shows that ABMS can be effectively used to analyze the GOP border security system when combined with a genetic algorithm to approximately optimize the infiltrator's behavior and data farming techniques to effectively implement the simulation experiments.

3.2 Why Use MANA

For the purpose of using ABMS to model a battle environment, the Center for Naval Analysis developed the ISAAC model (Ilachinski, 1997) and its extended model EINSTein (Ilachinski, 1999). The MANA system was developed by New Zealand's Defense Technology Agency (McIntosh et al., 2007). This study makes use of the software package MANA version 4 since we find some limitations in the alternatives, including ISAAC, EINSTein and Pythagoras, all of which were developed for military purposes. EINSTein has simple and powerful features but may lack the level of detailed modeling capability needed to reflect the GOP border security environment as indicated in Figure 5. This figure represents the scenario that the red force tries to reach the blue force's flag and tries to minimize the reds' casualties, whereas the blue force defends against the reds' infiltration.

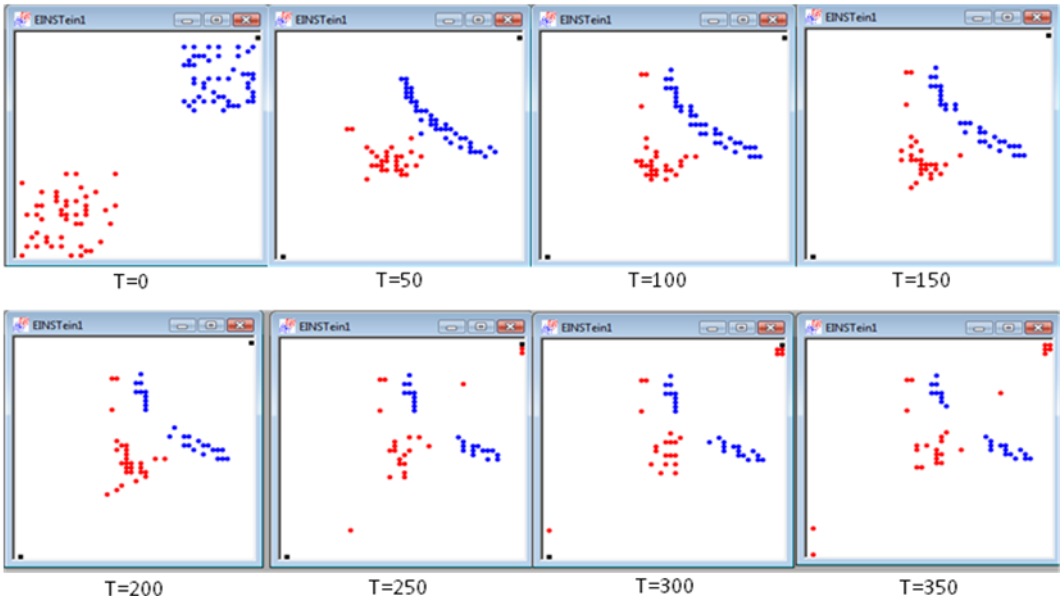


Figure 5. Screenshots from several sample runs of EINSTein

We note that version 5 of MANA is available (McIntosh, 2009). It is largely similar to MANA 4, with some changes to the algorithm that governs agent movement. Although there is some criticism of MANA (e.g., Straver et al., 2006) and we also find bugs related to the genetic algorithm tool, MANA is constantly updating both its software and its website (Defence Technology Agency-Project MANA, 2010) and fixes such problems. The overview of MANA and its key concepts for our model are explained in the following sections.

3.3 Overview of MANA

It is necessary to understand some definitions and terms that MANA uses prior to explaining how we formulate our model of the GOP border security system. As its name indicates, MANA can be interpreted as follows (Anderson et al., 2007):

- Map aware: Agents are aware of the battlefield which consists of terrain and an elevation map and a description of how it affects agent movement, line of sight, shooting range, etc.;
- Non-uniform: Heterogeneous agents have different behavior; and,
- Automata: All agents can act differently based on the events.

Based on these concepts, we must specify a scenario, a terrain map, and an elevation map for our model. Among them, scenario specification is the critical component which dictates the behavior of the agents for the possible outcomes they may face.

3.4 GOP Border Security System Model with MANA

Based on the problem description given in Chapter 2, and information on how the security system is implemented in reality, we develop the GOP border security system model using MANA. This model primarily includes an operational battlefield, human resources, equipment, communication and infiltrators. Our description of the GOP border

security system model does not dwell on minor details. Rather, we aim to formulate a model in which we can flexibly develop scenarios so that we can obtain insight as to how different scenarios behave. To change the variables specifying these scenarios we use data mining tools as described in Chapter 5, and as a result, it is more efficient to formulate model in as simple a form as possible. All of the data used in this model are based night operation in the DMZ.

Figure 6 shows a simple scenario from the border security model when the numbers of FGPs are 3, MGPs are 3 and reinforcements are 8 per platoon and the number of TODs is 2 per battalion without a terrain map. In this scenario, one infiltrator with default state is detected by a TOD and killed by reinforcements in the screenshot at the bottom right. As Figure 6 shows, the color of an agent changes when a changed state of the agent is triggered. In this simple scenario, the TOD detects the infiltrator, sends the information to the battalion CCC, then the battalion CCC directs the platoon CCC to dispatch reinforcements along the GOP line. In our model, artillery assets, mines, and GPs in the DMZ area are not considered but could be included if necessary. The Major input parameters for implementing our model in MANA are detailed in Appendix A.

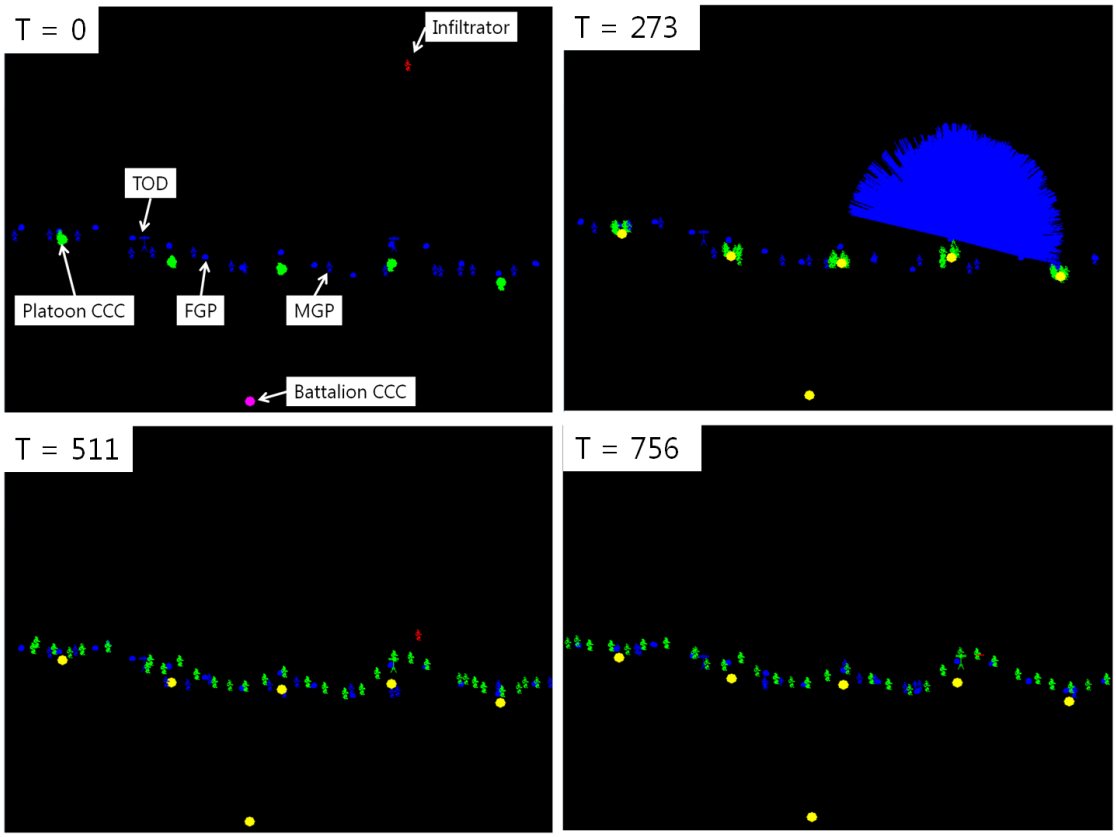


Figure 6. Screenshot of the GOP border security system model; time, T, is reported in steps of 5-second unit

3.4.1 THE OPERATIONAL ENVIRONMENT

In our scenario, we use a 10 × 7 km size of the DMZ area and the battlefield consists of 10000 × 7000 cells, i.e., each cell is 10 × 10 m. This size represents the operational area of the battalion level which is assigned five platoons. As mentioned earlier, MANA uses a standard bitmap to define battlefield terrain and distinct colors are used to identify various terrain features. As indicated in the picture on the left of Figure 7, main roads and

wires in the DMZ area are described with yellow and grey color respectively. The movements of agents are affected by the defined value of each color as indicated in Figure 8. Also, the picture on the right in of Figure 7 is the elevation map in the model, ranging from black (lowest point) to white (highest point). The elevation map affects the line of sight when the agents detect and shoot in the scenario.

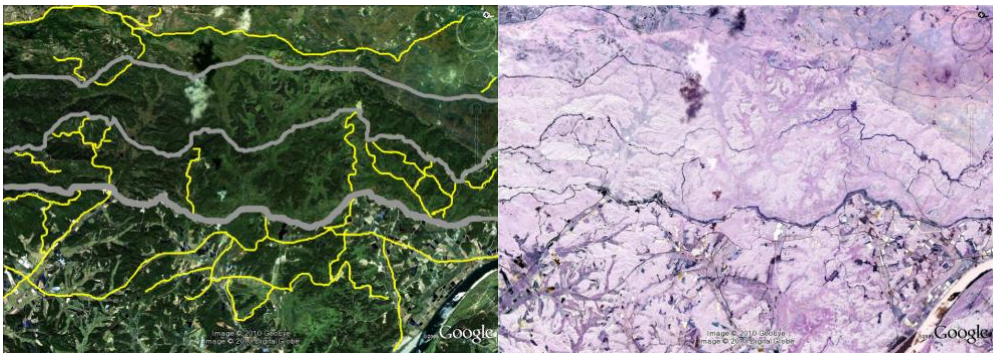


Figure 7. Terrain and elevation map of the GOP border security system model (Google map)

	Going	Cover	Conceal	Red	Green	Blue
BilliardTable	1.00	0.00	0.00	0	0	0
Wall	0.00	1.00	1.00	192	192	192
Hilltop	0.90	0.10	0.95	64	64	64
Road	1.00	0.00	0.00	255	255	0
LightBush	0.75	0.10	0.30	10	255	10
DenseBush	0.20	0.30	0.90	40	180	40
Wire	0.20	0.00	0.00	149	149	149

Figure 8. Terrain edit table in MANA

3.4.2 INFILTRATOR

The behavior of the infiltrator is a significant variable which affects results such as the probability the enemy is detected or killed, the probability the infiltrator's mission fails, and the (conditional) expected length of time for the enemy to reach their waypoint, but there are many uncertainties and it is very difficult to describe the enemy's behavior. Because of this difficulty, in Chapter 4, we use a genetic algorithm to approximate near optimal behavior of the infiltrator given the intensity of the GOP border security system. We take the view that this is an appropriately conservative perspective on the capability of the enemy. We only assume that the enemy has a longer detection range than the FGP and MGP when these defensive human resources are in their default state. Also, the objective of the infiltrators is to reach the waypoint without being killed. We exclude the case when the infiltrators attack the border security. The state of the enemy is defined as below:

- Infiltrator / default: This is the state before the infiltrator detects the border security and the behavior is defined as the ROK Army describes in the field manual (Security, FM 32-1, 2003).

- Infiltrator / contact: When the infiltrator detects the enemy, it triggers what we call the contact state and the infiltrator changes behavior. In this state, we modify specific model parameters including avoidance of certain assets and movement speed, which affects the results of the scenario.

30 homogeneous infiltrators are used to obtain near optimal behavior in Chapter 4 and then a single infiltrator is used to evaluate our GOP border security system in Chapter 5.

3.4.3 HUMAN RESOURCES

There are three types of human resources in our model, the FGP, MGP and reinforcements as explained in Chapter 2. In our scenario, each platoon takes charge of a 2 km width of the security area. There are a total of five platoons subordinate to the battalion and they each have an identical configuration. We assume that the distance between FGPs is identical regardless of terrain and they are located along the GOP line. We exclude the rotation of the FGPs and only consider MGP to make up the gaps between FGPs. Reinforcements are stationed in the platoon's CCC and dispatched to the GOP line when the platoon's CCC learns information from other assets such as FGP, MGP or the battalion's CCC. States of these human resources are defined as below:

- FGP/default: Sentinels are fixed in their post and observe the enemy with eyes in the default state;
- FGP/enemy contact: When they detect the enemy through squad or inorganic, situational awareness, the FGP uses PVS-7 night vision goggles and has longer detection range;

- MGP/default: MGP patrols along the GOP line with defined speed and detection range;
- MGP/enemy contact: When MGP have information about the enemy's location and movements, they adjust their speed;
- Reinforcement/default: Reinforce troops are stationed in the platoon CCC;
- Reinforcement/enemy contact: When other assets detect the enemy and the platoon CCC receives this information, the reinforcement troops dispatch to predefined supplement posts;
- Reinforcement/waypoint: When reinforcement troops reach their posts, they are then fixed in the post.

3.4.4 EQUIPMENT

Based on the tactical use of the TOD in our GOP border security system, TODs are located by considering height and distance from the GOP line. TODs work best when located close to the GOP line and when positioned relatively high. When there are multiple TODs, we locate them so that their total detection area is as large as possible. When a TOD detects an infiltration activity, it sends this information about the enemy to the battalion's CCC through a communication link.

3.5 Results

We formulate the GOP border security system model based on the ABMS concept with MANA software. While varying the parameters of the model, we can obtain the results indicated earlier such as the probability the enemy detected or killed, the probability that the infiltrator's mission fails and the conditional expected length of time for the enemy to reach their waypoint, conditioned on them reaching that waypoint. Since the configuration of the border security system and the environmental factors (terrain and weather etc.) are different at each battalion, it is meaningful to consider a range of such conditions when obtaining results. Also, this model can be extended to throughout the DMZ to evaluate the overall effectiveness of the border security.

When we compare the results of the human resource model of Sung (2005) with the results of our model by using parameters revealed in his paper, we obtain comparable results to his work. Compared to his model, our model captures more detail with respect to modeling the infiltrator, combines a human resource model and equipment model, which is separately implemented in his work, and takes less time to obtain the predicted detection rate and additional MOEs (measure of effectiveness). Our model can help battalion commanders adjust the configuration of border security and attain a required configuration and appropriate intensity of the security level while considering constraints including available assets and expected MOEs.

In our model, the behavior of the infiltrator is uncontrollable and difficult to predict, which strongly affects the results. When the triggered behavior of the infiltrator is considered, the detection rate is markedly difference from that when only the default state of infiltrator is used, as shown in Figure 9. In this scenario, only the FGPs are considered for border security, i.e., MGPs, TODs, and reinforcements are not included. But the parameters which we use for the FGPs and infiltrators are the same as we describe earlier in this chapter. The only difference is that the detection range of the FGP is varied as shown in Figure 9 and the 30 infiltrators have behavior (-100 in MANA input value) to avoid the FGPs.

We define a design point via the following triple: The number of FGPs (2, 4 or 6), the detection range of the FGP (50, 100, 150 or 200 m), and whether the infiltrator is in default mode or has behavior triggered to avoid a FGP once he detects that post, with a range of 150 m. For each design point we replicate the simulation model 100 times. The stochastic parameters include the initial location of the infiltrators, and the movement of the infiltrators. The initial location of the infiltrators is independent and identically distributed on the northern GOP line of the DMZ. The movement of an infiltrator is random in that when movement to a collection of neighboring cells is nearly equivalent, then infiltrator chooses among such cell in random. In this experiment, we have 24 design points and at each design point we carryout 1,000 replications for a total of 2.4×10^4.

The blue line in Figure 9 represents the average detection rate when the infiltrators have triggered behavior and the red line represents the detection rate when only the default state is considered. The x axis represents the detection range when the FGPs only use their eyes. In practice, the detection range varies based on the level of moonlight and weather during the night. Figure 9 and Table 5 suggest that it is important to consider the triggered behavior of the infiltrator. For example, when there are 6 FGPs and the FGP's detection range is 100 m the average detection rate is estimated to be about 63% when the infiltrator does not have triggered behavior but this drops to about 34% when the infiltrator has triggered behavior. This result inspired us to explore the behavior of the infiltrator in the next chapter.

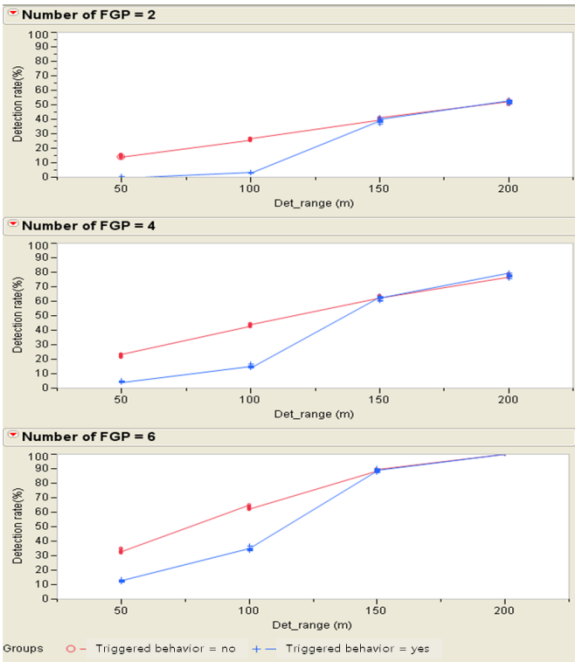


Figure 9. Comparison of detection rates

Num_FGP	Design point	Mean (%)	Std Dev	Low 95%	Upp 95%	Min (%)	Max (%)
2	Det_range[50] Triggered behavior[no]	14.34	0.62	13.89	14.79	13.33	15.37
2	Det_range[50] Triggered behavior[yes]	0.42	0.12	0.33	0.51	0.20	0.57
2	Det_range[100] Triggered behavior[no]	26.00	0.69	25.51	26.50	24.77	26.93
2	Det_range[100] Triggered behavior[yes]	2.75	0.22	2.60	2.90	2.43	3.13
2	Det_range[150] Triggered behavior[no]	39.32	1.06	38.56	40.08	38.13	41.30
2	Det_range[150] Triggered behavior[yes]	38.82	1.29	37.90	39.75	36.83	40.87
2	Det_range[200] Triggered behavior[no]	51.55	1.00	50.83	52.27	49.73	53.10
2	Det_range[200] Triggered behavior[yes]	52.05	0.90	51.40	52.70	50.77	53.40
4	Det_range[50] Triggered behavior[no]	22.37	0.76	21.82	22.91	21.33	23.53
4	Det_range[50] Triggered behavior[yes]	4.28	0.42	3.98	4.58	3.80	4.90
4	Det_range[100] Triggered behavior[no]	43.50	0.83	42.91	44.10	42.23	44.77
4	Det_range[100] Triggered behavior[yes]	14.93	0.82	14.34	15.51	14.10	16.67
4	Det_range[150] Triggered behavior[no]	62.75	0.63	62.30	63.19	61.80	63.73
4	Det_range[150] Triggered behavior[yes]	62.25	1.04	61.51	63.00	60.23	63.27
4	Det_range[200] Triggered behavior[no]	77.29	0.71	76.78	77.80	76.40	78.90
4	Det_range[200] Triggered behavior[yes]	77.32	0.98	76.63	78.02	75.70	79.30
6	Det_range[50] Triggered behavior[no]	33.11	1.02	32.38	33.84	31.87	35.10
6	Det_range[50] Triggered behavior[yes]	12.75	0.70	12.25	13.25	11.73	13.60
6	Det_range[100] Triggered behavior[no]	63.05	1.04	62.31	63.80	61.63	65.07
6	Det_range[100] Triggered behavior[yes]	34.31	0.97	33.61	35.01	33.13	36.40
6	Det_range[150] Triggered behavior[no]	88.72	0.50	88.36	89.08	88.03	89.70
6	Det_range[150] Triggered behavior[yes]	88.75	0.84	88.15	89.34	87.40	90.03
6	Det_range[200] Triggered behavior[no]	100.00	0.00	100.00	100.00	100.00	100.00
6	Det_range[200] Triggered behavior[yes]	100.00	0.00	100.00	100.00	100.00	100.00

Table 5. Confidence interval of each design point

CHAPTER 4 ANALYSIS UNDER OPTIMIZED INFILTRATOR BEHAVIOR

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

- Sun Tzu (476-221 BC)

In this chapter, we describe an optimization model that is used to determine the infiltrator's behavior, i.e., the behavior of the infiltrator forces (the red force). We use a genetic algorithm (GA) to approximately optimize this behavior. The optimization model we form aims to determine what we view as the worst case behavior for the infiltrator in overcoming the highest border security level of the ROK Army (the blue force). In terms of military operations, knowing the strategies and tactics of the enemy significantly affects the friendly forces' course of action (COA). The propensity of the infiltrator needs to be described in order to use it as input data when evaluating the GOP border security system.

GAs can be useful in military modeling for approximately solving difficult combinatorial optimization problem such as determining an adversary's COA (McIntosh & Lauren,

2006). For the blue force, we assume the COA of the red force is unknown, and we take the worst-case perspective mentioned above by allowing the red force to optimize its behavior. Currently, the ROK Army bases its assumptions about the COA of the infiltrator on previous infiltrations from North Korea and predicted infiltrator scenarios, which are described in its field manual (Security, FM 32-1, 2003).

That said, we instead pursue a model in which the enemy optimizes its behavior to understand the effect this has on our estimates of the performance of the border security system. The research questions are

- What are the optimal characteristics of the infiltrator against the maximum level of the blue forces' border security system (surveillance, control and command, and weapons systems)?
- How does the approximately optimized behavior of the infiltrator affect the performance of the border security system?
- Among the border security assets, which assets play the foremost roles in interdicting the infiltration?

4.1 The Infiltrator Optimization Problem

As we describe in the previous chapter, two scenarios are modeled based on the GOP border security system model. Given the ROK Army's maximum level of border security, the first scenario is developed based on the predicted infiltration scenario in the field manual (Security, FM 32-1, 2003) without the triggered behavior of the infiltrators. We name this default scenario as scenario 1. Scenario 2 is identical to scenario 1 up to the point at which the infiltrators contact the security guard. The objective of the infiltrator is to successfully pass through the DMZ and reach a pre-decided waypoint that is located south of the southern GOP line.

In modeling the infiltrator's behavior we use five simulation model constructs as decision variables to control that behavior, as enumerated below:

- x_1: Next waypoint $\in [5, 70]$;
- x_2: Avoid FGPs $\in [-100, 0]$;
- x_3: Avoid Reinforcements $\in [-100, 0]$;
- x_4: Avoid MGPs $\in [-100, 0]$; and,
- x_5: Speed of movement $\in [5, 70]$;

An infiltrator has access to intermediate waypoints on his way from his origin to his destination waypoint. Decision variable x_1 is a weight that indicates how aggressively the infiltrator attempts to reach the next waypoint. Decision variable x_2 ,

x_3, and x_4 concern how much weight the infiltrator places on avoiding blue forces in respective forms of FGPs, MGPs and reinforcements. A value of -100 represents maximum aversion to blue forces and 0 represents no aversion at all. Finally, x_5 controls the speed of movement of the infiltrator (1 km/h = 14 MANA unit). We consider two MOEs for the infiltrator: m_1 is the number of red casualties and m_2 is the (conditional) average time for the infiltrators to reach the final waypoint, conditioned on actually reaching that waypoint. Those two MOEs depend on $x_1, x_2, x_3, x_4,$ and x_5, and we denote this dependence via $m_1(x_1, x_2, x_3, x_4, x_5)$ and $m_2(x_1, x_2, x_3, x_4, x_5)$. We assume that the infiltrator attempts to minimize a weighted sum of m_1 and m_2. Specifically, we formulate the infiltrator's optimization problem as:

$$
\begin{aligned}
\min_x \quad & w\, m_1(x_1, x_2, x_3, x_4, x_5) + (1-w)\, m_2(x_1, x_2, x_3, x_4, x_5) \\
\text{s.t.} \quad & 5 \le x_1 \le 70 \\
& -100 \le x_2 \le 0 \\
& -100 \le x_3 \le 0 \\
& -100 \le x_4 \le 0 \\
& 5 \le x_5 \le 70,
\end{aligned}
$$

where w $(1 \le w \le 1)$ is a weight that can put all weight an minimizing casualties (w = 1), all weight on minimizing time to reach the destination (w = 0), or anything on the continuum in between.

From our experiments, we find that when w = 1, i.e., we minimize red casualties, that the red force evolves in a way to largely stay to the north of the GOP line. So, most of the infiltrators stay above the GOP line at the time the simulation run terminates. For this reason, we incorporated m_2, the time to reach the final waypoint, into the objective function to induce the red forces to advance. That said, we use a small weight on the latter MOE, as we detail below:

i. Scenario 2, MOE 1 ($w = 1.0$);

ii. Scenario 2, MOE 2 ($w = 0.95$);

iii. Scenario 2, MOE 3 ($w = 0.90$).

The decision variables in the infiltrator's optimization model are nominally continuous. However, the objective function has no structure that lends itself to optimization by typical algorithms for (continuous) nonlinear optimization. So, we discretize the feasible region for $(x_1, x_2, x_3, x_4, x_5)$ and only allow them to take on integer values in this domain. Enumerating all such feasible solutions amounts to 4.225×10^{11} points, which we term design points. Given that a simulation model must be run to estimate the objective function at a single design point, compete enumeration is not viable. So, we use a heuristic to approximately solve our model. In particular, we use a GA. Details of the GA we use are given in the next section.

4.2 GA in MANA

For this study, we use the GA tool kit in MANA based on the GOP border security model which we developed in Chapter 3. The genes in the GA correspond to the decision variables of the model specified in Section 4.1.

In one iteration of the GA, specific values for these genes are assigned, i.e., the chromosome is specified. Then, the infiltrators are placed in the corresponding scenario and the objective function is calculated for the border security system. Once the MOEs in the objective function have been estimated, the decision is made whether to keep or eliminate the chromosome in the subsequent generation. This process is repeated over generations with the goal of decreasing the specific weighted sum.

Figure 10 demonstrates how chromosomes evolve from one generation to the next based on defined parameters, including population number, number of multi-runs, mutation rate, and mutation strength (McIntosh & Lauren, 2006).

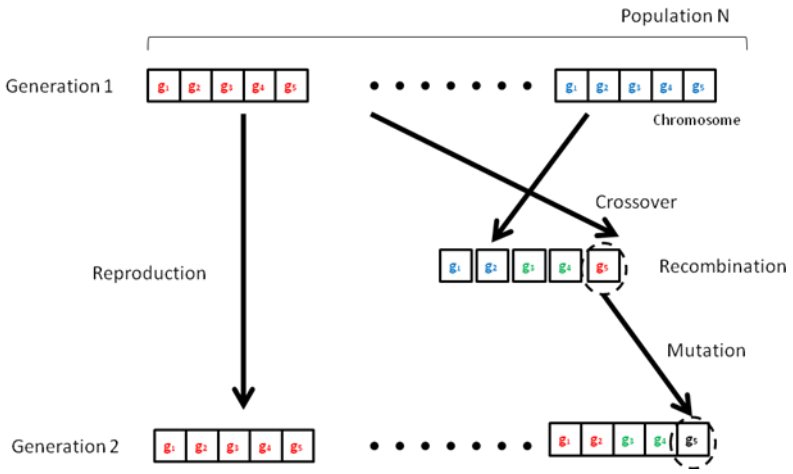


Figure 10. Schematic diagram for the GA

Before the GA scheme is executed, the size of its population, the mutation rate, the mutation strength, and number of multi-runs must be specified as shown in Figure 11. The mutation rate represents the probability that genes will mutate in one generation. The mutation strength refers to the percentage of each gene's allocated range by which the gene's value will change if a mutation does occur. We have random mutations to infiltrators' genes. Genes in our schemes have an integer value so we have a choice to change the integer value due to mutation. Mutation can be useful in attaining an improved value of the MOEs compare to that of the original genes. Both mutation rate and strength should not be too high because they can destroy good chromosomes (McIntosh et al., 2005). For this problem, we used a total 7.5×10^3 replications with a population size of 10, with 5 multi-run, 5% mutation rate, 10% of mutation strength and with 50 GA generations.

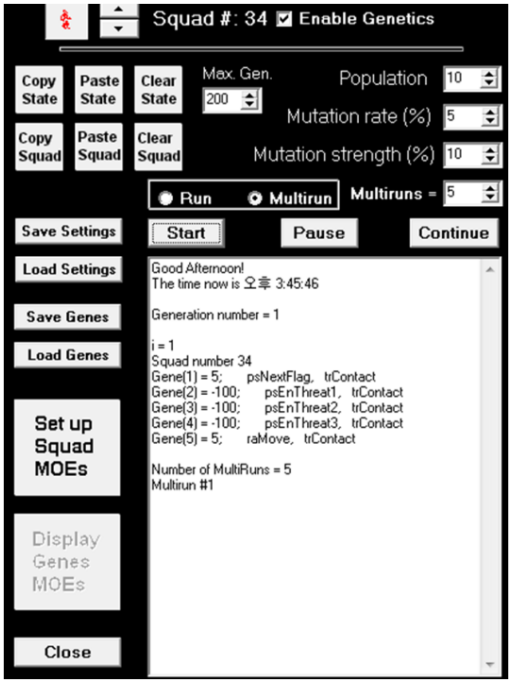


Figure 11. Screenshot of GA running in MANA

Figure 12 indicates how the user can specify the decision variables, along with the simple bounds that specify the feasible region of the infiltrator's optimization model. There is also an option to set the range over which gene values will be randomly generated to make up the initial chromosome population (McIntosh et al., 2007).

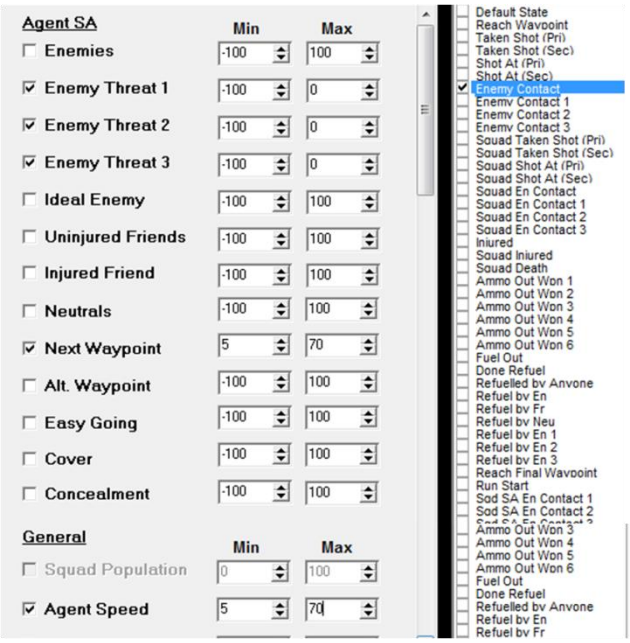


Figure 12. Selecting genes and trigger states

4.3 Further Model Description

In our simulation model, we assume that the infiltrator's default speed of movement is based on the infiltrator's activities. From analyzing of previous infiltrations by the North Korea Army, we assume that the infiltration is executed after sunset which means the input data is based on night operation and the red force has longer surveillance capacity than the blue force in the default state as shown in Table 6.

	Blue Force	Red Force
Detection Range	• FGP, Reinforcement: - Default state: 50m - Enemy contact state: 200m • MGP: 20m	150m

Table 6. Detection range of blue and red forces

We do not consider the situation in which the infiltrators attack the security guards as explained in Chapter 3. Additionally, friendly forces have an ideal condition in that there is no delay in the communication network. Communication is assumed to be 100% accurate and reliable for the blue force. The blue force includes FGPs, MGPs, reinforcements, and TODs are located along the GOP line. We do not give the exact number of security assets for the scenarios since the data are classified.

Scenario 1 consists of three steps as we describe below. First, 30 homogeneous infiltrator agents are randomly generated within the area north of the GOP line, as in Figure 13, and the blue force maintains border security level, type C as given in Table 2.

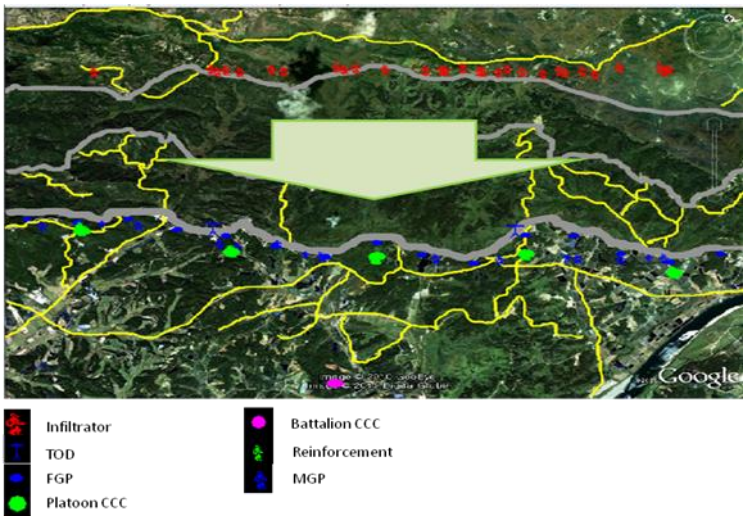


Figure 13. Scenario 1 step 1: initiation screen

Second, as Figure 14 shows, the red force is detected by the TOD. The green color of the TOD on the right side of the map shows it detected the red force and that this information is shared with the battalion and platoon CCC. As Figure 14 shows the state of the battalion and platoon CCC were changed into the detected state as the yellow color indicates. The battalion CCC directs an upgrade to the border security level from type C to type A and the reinforcements that are stationed at the platoon CCC move to occupy predetermined complementary posts along the GOP line.

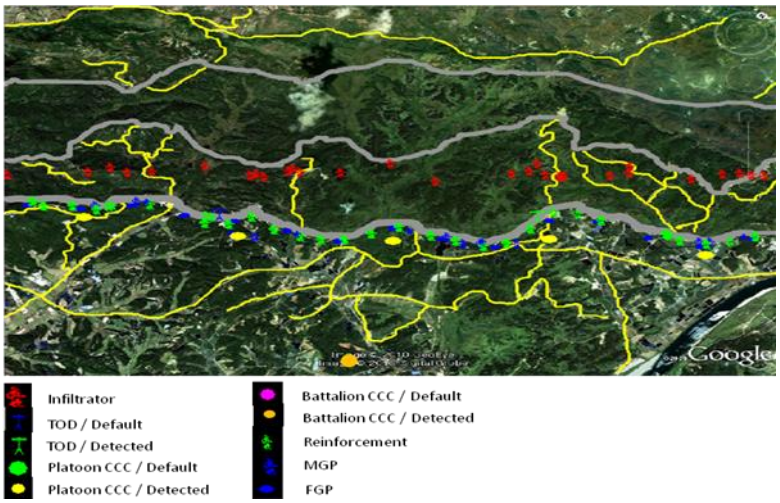


Figure 14. Scenario 1 step 2: blue force detects the infiltrator

Figure 15 shows that part of the red force has passed between blue assets and advanced toward their waypoints south of the GOP line in the map.

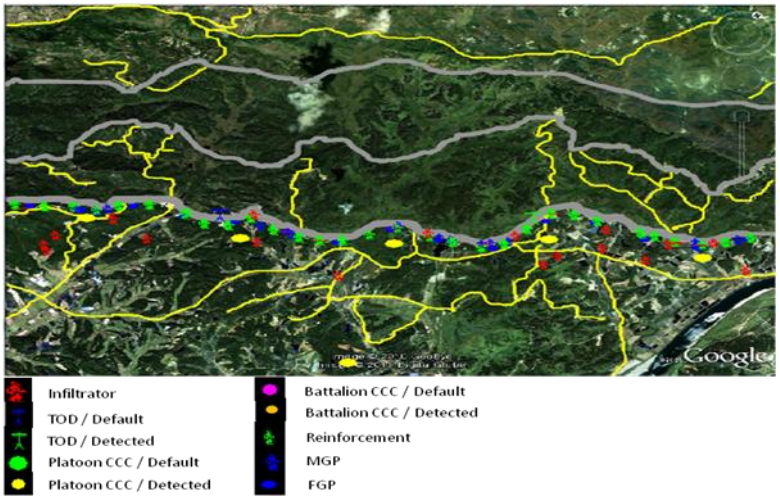


Figure 15. Red force overcomes the GOP line

By running 500 replication of scenario 1, the important phase of the infiltration was identified as to when the triggered state was endowed to the red forces. Based on the triggered behavior of the red force, a second scenario (named scenario 2) was developed and analyzed using three different weights, (w = 1.0, 0.95, 0.9) as explained in Section 4.1 The Infiltrator Optimization Problem. From the analysis of the default scenario, we understand that the decisive phase of the scenario is between time step 450 and 850, as this is when the infiltrators may be detected by the security guards.

4.4 Simulation Analysis

The expected number of infiltrators killed is used as the primary MOE to analyze and compare the results of the GA. The number of infiltrators killed is a single simulation run is a random variable and so we use 500 replications to form an estimator of this MOE. The same number of replications are also used when running the GA to approximately solve the optimization model of Section 4.1. Fractal dimension governing the spread of infiltrating forces is another MOE that is sometimes advocated to provide insight into the dynamics of conflicts (Sprague & Dobias, 2008). We assessed fractal dimension in our experiments but found that it added little insight over the number of casualties in the red force.

From the analysis of scenario 1, the average number of red force detected and the red force alive as a function of time are obtained as shown in Figure 16. As Figure 16 indicates, the time step from 450 to 850 is decisive for the red infiltration and the involved triggered behavior when the infiltrator detects the border security assets.

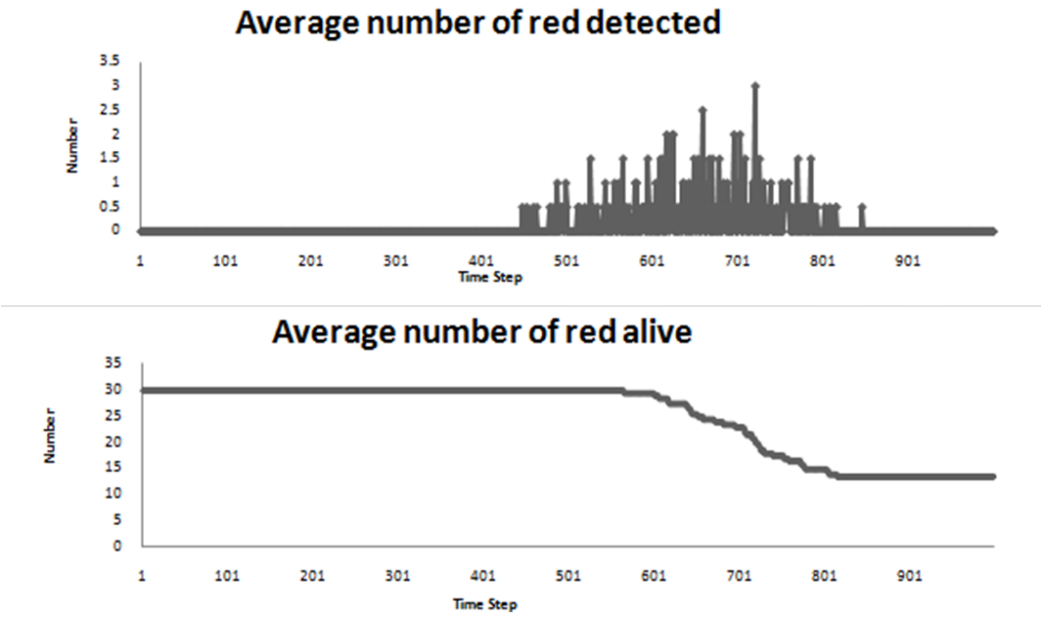


Figure 16. Results of scenario 1 over time steps 0 to 1000

The results of scenario 2 based on the GA are as shown in Figure 17, Figure 18, and Figure 19. The best chromosomes were obtained within 30 GA generations for each MOE.

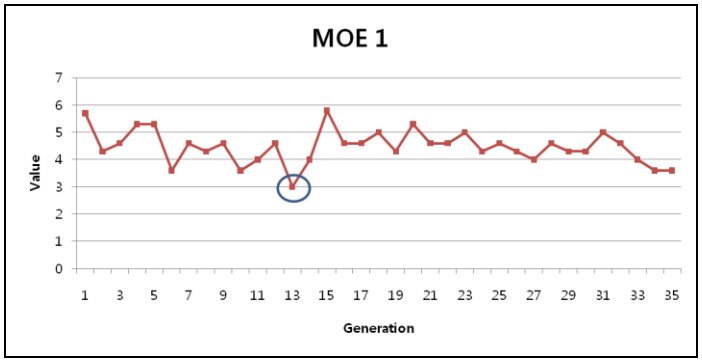


Figure 17. MANA run results of scenario 2, MOE 1 $(\mathbf{w = 1.0})$

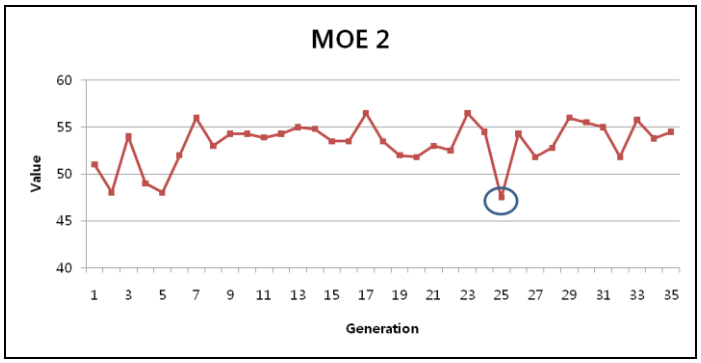


Figure 18. MANA run results of scenario 2, MOE 2 $(\mathbf{w = 0.95})$

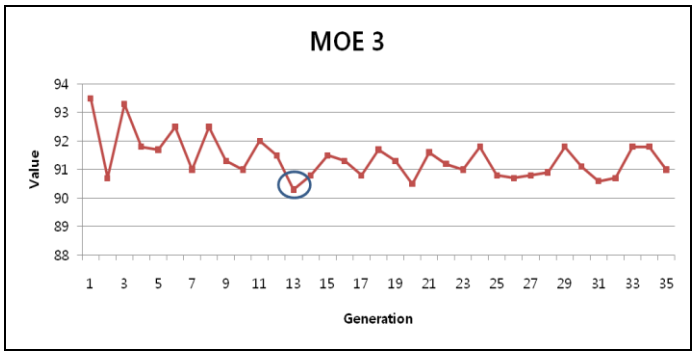


Figure 19. MANA run results of scenario 2, MOE 3 $(w = 0.90)$

Based on the GA results, Table 7 is obtained from 500 simulation runs. Table 7 shows near optimal behavior of the infiltrator. As the weighting of MOE m_2 increases, we can predict the speed of movement increases but it is not always true, as Table 7 demonstrates. The speed of movement from the MOE 2 to MOE 3 decreases since the behavior of the infiltrator involves five characteristics, and there are interactions when these variables interact.

Also, from the results of x_2, x_3, and x_4, we can estimate how the infiltrator recognizes the relative threat from each border security resource. The infiltrator has the best characteristic when seeking to avoid the FGP the most, i.e., when the absolute value of x_2 exceeds that of x_3 and x_4.

	Scenario 1 (Default)	Scenario2 (MOE 1)	Scenario2 (MOE 2)	Scenario2 (MOE 3)
Next Waypoint (x_1)	30	5	28	45
FGP (x_2)	0	-100	-43	-21
Reinforcement (x_3)	0	-90	-34	-11
MGP (x_4)	0	-80	-24	-11
Moving Speed (x_5)	56	20	56	44

Table 7. The results of GA for values of three weights in the objective function

Table 8 explicitly shows how the approximately optimized behavior affects the results of the infiltration in terms of red casualties. The second column, the MOE, represents the best value of each case as w varies. The number of red casualties decreases dramatically when we move from scenario 1 to scenario 2 with w = 1. In this case, as we mention above, the infiltrators largely stay north of the GOP line. A similar result appears to hold when we decrease w to w = 0.95, i.e., for scenario 2 (MOE 2). However, these results are different in that in scenario 2 (MOE 2) most of the infiltrators do reach their waypoint. When we further decrease w to w = 0.90, the performance of the infiltrators has almost reverted to that of scenario 1. Based on these results, we select scenario 2 (MOE 2) for the near optimal behavior of the infiltrators for evaluating the border security system in Chapter 5.

	Red Casualties	Std. Dev	Red Casualty (%)	Lower 95%	Upper 95%
Scenario 1 (Default)	13.38	2.76	44.6	13.13	13.62
Scenario2 (MOE 1)	0.006	0.08	0.02	0	0.01
Scenario2 (MOE 2)	0.436	0.68	1.45	0.37	0.50
Scenario2 (MOE 3)	12.408	2.77	41.36	12.16	12.65

Table 8. The results of 500 simulation runs with the best solution for scenario 2 and comparison between scenario 1 and 2

The quantile box plot in Figure 20 shows the difference in number of casualties in each case. As the plot represents, the average number of casualties between the default scenario and MOE 1 scenarios are significantly different, while the default scenario and MOE 3 scenario look very similar.

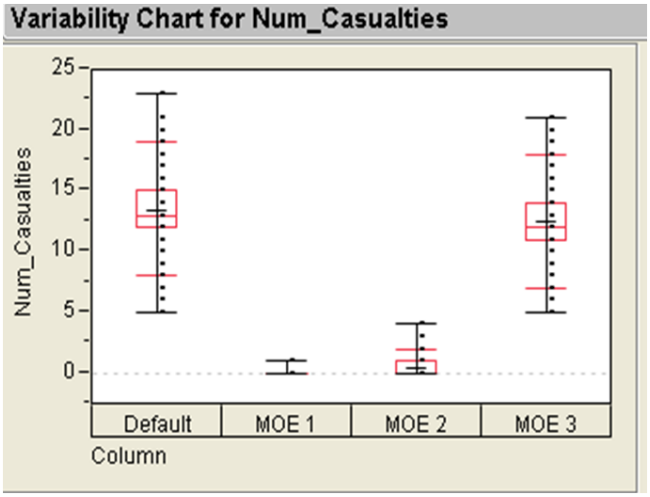


Figure 20. Comparison of each scenario by using quantile box plot

4.5 Conclusion

In this chapter, we formulated an optimization model and approximately solved it using a GA in order to capture near optimal behavior of an infiltrating force. In our experiments the GA obtains its best solution within 30 iterations. We found several weaknesses of the GA tool such as reliance of randomness when generating the initial population and redundant excursions to certain chromosomes. One reason for this behavior of the algorithm is that a memory structure is not used to avoid revisiting the same solution. For

this reason, improvements to generate the initial solution intelligently or an adaptive search procedure that uses a memory structure could improve our results. The results presented in this chapter give two significant insights for our border security system.

First, optimizing the infiltrator's behavior can make a significant difference. Previous studies mostly do not consider the optimized behavior of the infiltrator in their scenarios and model the enemy similar to our scenario 1. But, the casualties of the infiltrators show the MOE between scenario 1 and scenario 2 can be significantly different.

Second, the quantitative results regarding the infiltrator's avoidance of each asset in our security system can be viewed as capturing their relative importance to our border security system. A previous study of Sung (2005) suggests that the role of the MGP is minor compare to other assets because the range of the surveillance is short. But, the results of our simulation reveal the MGPs plays an important role to interdict the infiltrator since the MGP is capable of detecting and killing infiltrators who try to pass through gaps between the FGP and the reinforcements. Specifically in Table 7, the values of x_4 are not minor compared to that of x_2 and x_3.

In this chapter, we have sought to address research questions related to optimized behavior of infiltrators, and we have sought to identify the importance of each asset by interpreting degree of avoidance. Part of the results of the infiltrator's behavior is used in Chapter 5 to further evaluate the border security system.

CHAPTER 5 ANALYSIS OF THE GOP BORDER SECURITY SYSTEM

Based on the approximately optimized behavior of the infiltrator which we obtained in Chapter 4, we evaluate the GOP border security system in this chapter. We use four MOEs to evaluate the security system's performance, and we use a NOLH design to deal with the large number of factors of interest important in our model of that system.

5.1 Measure of Effectiveness

In the context of the overall security system, it is useful to choose representative MOEs to evaluate and compare the results of different configurations and the values of numerous factors including number of assets, detection range, shooting distance, etc. Although multiple MOEs can result in more sophisticated measures, limitations of the capabilities of MANA must also be considered. Based on these considerations, four MOEs are identified:

- Probability enemy is detected (MOE 1);
- Probability enemy is killed (MOE 2);
- Average time to reach enemy waypoint (MOE 3); and,

- Probability enemy mission fails (MOE 4).

Each experiment starts with a single infiltrator whose initial location is uniformly distributed along the 2 km segment of interest on the northern GOP line, as we described in Section 3.4. The infiltrator then proceeds south, towards his final waypoint. One of four events then occurs: He is first detected by a TOD, he is first detected by FGP, he is first detected by a MGP, or he reaches the final waypoint undetected. We let TODD, FGPD, and MGPD denote the first three of these events. Then, we can represent MOE 1 as:

$$\text{MOE 1} = \text{P(TODD)} + \text{P(FGPD)} + \text{P(MGPD)},$$

where P(·) is the probability associated with the corresponding event. If the enemy is first denoted by a TOD and subsequently detected by an FGP or MGP then event TODD occurs but events FGPD and MGPD do not occur, i.e., detection of the enemy is only counted once. Similarly defining FGPK, MGPK, and ReinK as the event that the infiltrator is killed by a FGP, MGP, and Reinforcement, respectively. In our scenario, Reinforcements are deployed conditioned on the border security level is upgraded from level C to level A when detection is occurred by FGP, MGP, or TOD. We can define MOE 2 as:

$$\text{MOE 2} = \text{P(FGPK)} + \text{P(MGPK)} + \text{P(ReinK} \mid \text{Security level upgraded)},$$

where P(·) is again the probability of the corresponding event. MOE 3 represents the average time the infiltrator takes to reach their waypoint, given that they reach it within 1500 time steps. Finally, MOE 4 is the sum of the probability that the enemy is killed and the probability he is not killed but still fails to reach the final waypoint within 1500 time steps.

5.2 Design of Experiment

5.2.1 Overview

Our simulation model has many factors that are input for the model but can be varied across a range of reasonable values. When this is the case we must select a means for considering the enormous number of combinations that are possible.

5.2.2 Important Factors and Range

Among the numerous factors which comprise our border security model, twenty significant factors are identified in Table 9. The table groups these factors as to whether they are specific to human resources, equipment (TOD) or the CCCs. And, the table further indicates whether those human resources are FGPs, MGPs, or reinforcements, and

whether it involves the platoon CCC or the battalion CCC. We further note that the factors numbered from 8 to 12 affect both the FGPs and the reinforcements.

Classification	Factor number	Assets	Name	Low level (Real World)	High level (Real World)
Human Resources	1	FGP	Number of FGPs per platoon	0	6
	2		Turret height	2m	10m
	3	MGP	Number of MGPs per platoon	0	4
	4		Speed of movement	1km/h	2km/h
	5		Detection range	20m	50m
	6	Reinforcement	Number of reinforcements per platoon	5	10
	7		Speed of movement	4km/h	7km/h
	8	Common for FGP and Reinforcement	Detection range/ Default state	50m	200m
	9		Detection range/ Contact state	200m	300m
	10		Shooting range/contact	50m	150m
	11		Communication latency	25sec	60sec
	12		Communication reliability	80%	100%
Equipment	13	TOD	Number of TODs per battalion	0	3
	14		Turret height	40m	60m
	15		Communication latency	25sec	60sec
	16		Communication reliability	25sec	60sec
Command and Control Center	17	Platoon CCC	Latency	25sec	60sec
	18		Reliability	80%	100%
	19	Battalion CCC	Latency	25sec	60sec
	20		Reliability	80%	100%

Table 9. Important factors and range of the GOP border security system

5.2.3 Nearly Orthogonal Latin Hypercube (NOLH) Design

Latin Hypercube (LH) designs provide a flexible way to construct efficient designs for quantitative factors (Sanchez, 2007). In this thesis, the NOLH design helps reduce the computational requirements of some classic designs by many orders of magnitude, which still making it possible to develop a better understanding of a complex simulation model.

Let k denote the number of factors and let N $\geq$ k denote the number of design points. If each factor has 2 or 5 levels we could employ a 2^k or 5^k factorial design but the number of design points increases exponentially with k and quickly becomes impractical.

To avoid the danger associated with high pairwise correlations associated with random LH designs, we employ the ideas of Cioppa and Lucas (2005), who develop NOLH designs with good space-filling and orthogonality properties. Table 10 lists the number of design points up to k = 29. As can be seen from Table 10, the number of required design points is dramatically reduced from that of a full factorial 5^k design. Such design points are easily generated through the NOLH.xml file, which can be downloaded at the Seed center website (SEED Center for Data Farming, 2010).

No. of factors	No. of Design points
2-7	17
8-11	33
12-16	65
17-22	129
23-29	257

Table 10. Requirement for NOLH design (Sanchez, 2007)

We use our 20 factors from Table 9 with a variable number of levels for each factor. A full factorial design would require 1.85×10^{19} design points whereas only 129 design points are used in our NOLH design, as indicated in Table 10. Based on the factors and

ranges of the GOP border security system from Table 9, a NOLH design is generated with an excerpt of that design shown in the Table 11.

low level	0	2	0	14	2	5	56	5	20	5	80	0	40	5	80	5	80	5	80	5
high level	6	10	4	27	5	10	98	20	30	12	100	3	60	12	100	12	100	12	100	15
decimals	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
factor name	Num_ FGP	FGP_ Hei	Num_ MGP	MGP_ Spd	MGP_ Det	Rein_ Num	Rein_ Spd	Det_D ef	Det_C ont	Com m_Lat	Com m_Rel	Num_ TOD	TOD_ Hei	TOD_ Lat	TOD_ Reli	Pln_L at	Plt_R eli	Bat_L at	Bat_R ei	Sht_R ange
1	1	6	2	20	3	8	80	16	26	12	95	2	52	12	99	9	97	9	98	15
2	5	4	2	20	2	7	74	8	25	8	98	2	52	12	95	11	98	9	92	12
3	3	8	0	18	3	6	88	15	26	9	89	0	50	11	100	9	91	6	97	12
										. . .										
126	4	7	0	19	3	6	83	18	25	10	94	3	58	6	85	7	90	11	84	7
127	3	9	2	20	3	8	64	10	24	9	98	2	56	7	80	5	86	10	89	7
128	4	5	1	15	3	8	84	17	29	11	86	0	49	5	82	8	88	8	83	9
129	1	6	1	16	2	7	64	11	21	7	83	1	44	7	88	8	89	8	86	5

Table 11. NOLH design with 20 factors and 129 runs

Figure 21 shows the pairwise plots for each pair of design points. These show that, at least pairwise, the design points are spread out fairly evenly. The pairwise correlations from Figure 21 range from -0.097 and 0.105, suggesting pairwise correlations are relatively low.

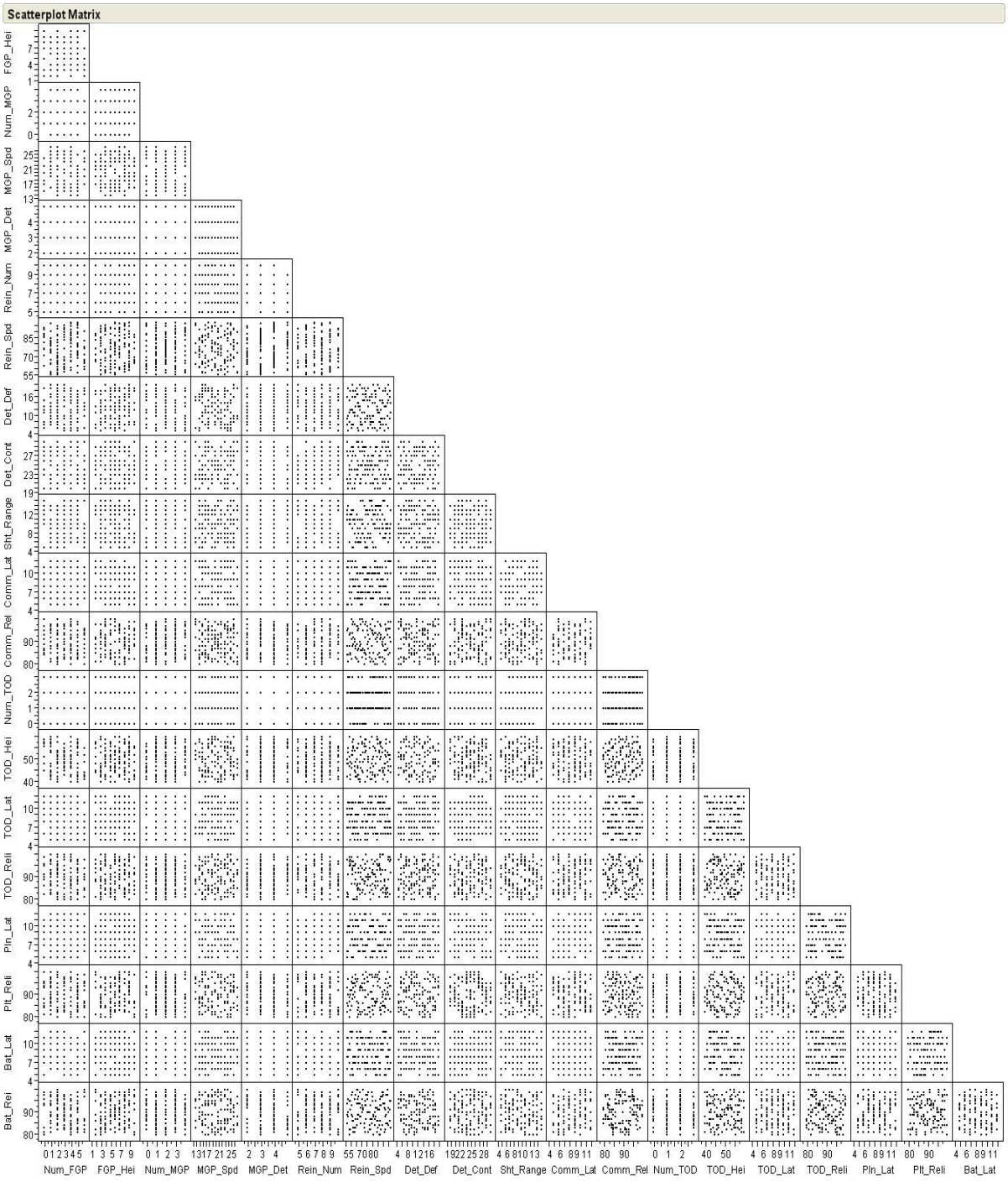


Figure 21. Pairwise scatter plots for NOLH design with 20 factors in 129 runs

5.3 Model Run

5.3.1 OVERVIEW

After generating 129 design points based on a NOLH design, numerous replications of the simulation model are formed. As described in Chapter 3, the stochastic elements of the simulation model include start point and movement of infiltrator. In these simulation runs a single infiltrator is randomly generated instead of multiple infiltrators above the DMZ area. From a single run of the simulation model the enemy is either detected or not, the enemy is either killed or not, and the enemy's mission either fails or succeeds. We encode these with a '0' or '1' as to whether, e.g., event TODD occurred (1) or not (0). We use 1000 replications of the simulation to form estimators for MOE 1, MOE 2, MOE 3, and MOE 4.

5.3.2 ANALYSIS TOOLS

We use XStudy and OldMcData (Upton, 2006), which the SEED Center developed (SEED Center for Data Farming, 2010) to facilitate iterating through each of the 129 design points and to process output data from MANA. XStudy uses information specified within a MANA scenario file to identify the factors that are to be varied. Given a scenario file and the NOLH design file it generates a file called study.xml, which contains the

study information about scenario, the number of replications, specification of the algorithm for generating the factor variations, and factors to be used for that variation.

By using the study.xml file from XStudy, OldMcData generates excursions which are modified from the original scenario file with the factors detailed in the study.xml file. For our GOP border security system model, 129 excursion files are generated and OldMcData conducts experiments using Condor (University of Wisconsin-Madison, 2010). Condor is a workload management system which was developed at the University of Wisconsin-Madison for computationally intensive jobs. After the simulation run terminates, OldMcData carries out post-processing in which it collects all output data into one file. The overall data process flow is described in Figure 22.

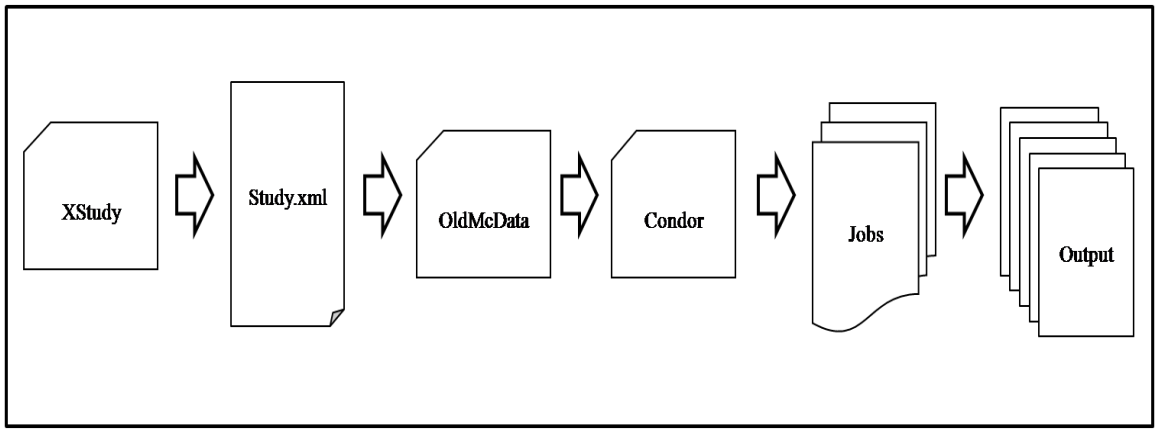


Figure 22. Data process flow

To run the 129 excursions with 1000 replications for each excursion, the HPC (High Performance Computer) resources at the Naval Postgraduate School were used; run time

was approximately 6.5 hours, which corresponds to approximately 240 hours on a typical personal laptop (2.4GHz, 4.0 GB RAM).

5.4 Results Analysis with Statistical Tools

After running the simulation model for 129 design points and 1000 replications for each design point, a total of 1.29×10^5 data points are analyzed for each MOE. To perform a statistical analysis of the obtained data points and provide an appropriate visual tool for decision makers, JMP is primarily used in this study because its features are dynamic, interactive, visual, and easy to use. For this study, several statistical techniques are used, which are listed below (Proust, 2008):

- Variable importance plot: PLS (Partial Least Square) regression in JMP and the variable importance score in TreeNet are used to identify important factors among 20 factors in our model. Variable importance in the projection (VIP) is obtained by using PLS regression and the VIP summarizes the contribution a variable makes to the model, i.e., its correlation to the response (MOE). This enables us to choose the number of extracted factors by fitting the model to part of the factors and minimizing the prediction error. If a factor has a small VIP, then it means that the factor does not influence much on response. VIP score below one (We use 0.8 instead of 1 (Wold, 1994)) can be considered a small VIP

since the average of squared VIP score is one. TreeNet (Salford Systems, 2005) is a regression modeling platform. The variable importance score is based on the improvements when we obtain the optimal RSquare value among 200 splits associated with given factors. The scores are rescaled so that the most important factor always gets a score 100.

- Contour plot: This is a graphical representation of the relationships among three numeric variables in two dimensions. Two important factors are identified from the VIPs, and each MOE provides a third variable to from contour levels. The contour levels are plotted as curves; the area between curves can be color coded to indicate interpolated values.

- Bivariate scatter plot and fitting: This explores how the distribution of one continuous factor is related to another continuous factor. The analysis begins with scatter plot of points, to which we can interactively add other types of fits, such as simple linear regression and polynomial regression of selected degree.

- Box plot: This shows additional quantiles on the response axis. If the distribution is symmetric the quantiles shown in a box plot are approximately equidistant from each other, so this plot suggests whether a distribution may be symmetric or skewed.

- Regression tree: A regression tree provides a method for exploring which factors are most significant in predicting a dependent response. It finds a series of cuts and groupings of factors that best predict the dependent variable. It does this by exhaustively searching all possible cuts or groupings. These splits are done recursively forming a tree of decision rules until the desired fit is reached. This is a powerful platform, since it examines a very large number of possible splits.

5.5 Results

5.5.1 CORRELATION ANALYSIS

The correlation coefficient (γ) between random variables for estimator of MOEs ($\widehat{MOEs}$) can give good insights into linear relationship between MOEs. In our model, the enemy detected (X), killed (Y), and mission failed (Z) are the random variables which have binary number '0' or '1', e.g. detected (1) and not detected (0), to estimate $\widehat{MOE}_1$, $\widehat{MOE}_2$, and $\widehat{MOE}_4$ as shown in Section 5.1. Instead of time length variable, the infiltrator remained (F) variable added for better understanding of $\widehat{MOE}_4$. This result shows how the mission failure of infiltrator caused by either killed or remained above the GOP line. The multivariate platform of JMP is used to explore the relationship and dependency between random variables. Suppose we compute the sample γ between two

random variables, enemy detection (X) and enemy killed (Y), to explore the correlation between $\widehat{MOE}_1$ and $\widehat{MOE}_2$. We have n = 1.29×10^4 with iid pair of X and Y, written as x_i and y_i where i = 1,2,…., n, then we can estimate the γ between X and Y by computing:

$$\gamma_{xy} = \frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{(n-1)s_x s_y},$$

where $\bar{x}$ and $\bar{y}$ are the sample mean, s_x and s_y are sample standard deviation of X and Y respectively. The matrix in Table 12 summarizes the strength of the linear relationship between each pair of random variables.

Variable	Variable	Correlation	Lower 95%	Upper 95%
Detection (X)	Casualty (Y)	0.1326	0.1271	0.1379
Mission (Z)	Detection (X)	0.4182	0.4137	0.4227
Mission (Z)	Casualty (Y)	0.4012	0.3966	0.4058
Remain (F)	Detection (X)	0.3621	0.3573	0.3668
Remain (F)	Casualty (Y)	-0.2065	-0.2117	-0.2013
Remain (F)	Mission (Z)	0.8130	0.8112	0.8149

Table 12. Pair-wise correlations between $\widehat{MOEs}$

The dependency between X and Y is only 0.1326 which is lower than one might anticipate. The reason is that most detection of infiltrators was by the TOD. The enemy can have difficulty avoiding detection by the TOD because of its longer detection range

when compared to the FGP, MGP, and reinforcement troops. But TOD does not have an ability to attack directly from a long distance. From this result, we see the necessity of enforcing the connection between surveillance systems and weapon systems.

From the result of the correlation between F and Z which is 0.8130, and we can estimate the mission failure of the infiltrator is mostly caused by remaining above the GOP line within 1500 time steps.

Considering only one MOE can be relatively simple without results analyzing process, but the results above show that it can be insufficient and have limitations in evaluating the overall system. In particular, the correlation between Z and the other random variables help to find which system affect the most or least the overall success of the border security system. Generally, the detection rate and the number of captured (killed) enemies are used as performance measures for the border security system on the US-Mexico (Berner, 2004) (Yildiz, 2009) and US-Canada borders (Patrascu, 2007). In these theses, the MOE 3 and MOE 4 are introduced and MOE 4 shows that it may give better insight when assessing the border security system. The following sections show the statistical results for each MOE.

5.5.2 PROBABILITY OF ENEMY DETECTED (MOE 1)

Simulation results are analyzed through JMP and TreeNet as can be seen in Figure 23. The VIP plot in the left side in Figure 23 shows VIP score corresponding to the 20 factors. The factors which have VIP score greater than 0.8, denoted by the blue vertical line in the figure left, represent important factors among twenty factors. The graph in the right side in Figure 23 reflects contribution of each factor in predicting the MOE 1 by regression in TreeNet. We identify the number of TOD and detection range (default state) as the important factors with VIP score 3.94 and 1.96, and variable importance score 100% and 60% respectively from the results of both methods as shown in Figure 23. When the triggered behavior of the infiltrator is not applied, the other factors such as number of FGP and MGP identified significant along with number of TOD and detection range (default state). We can see that the security guards including FGP and MGP does not much contribute to the enemy detection according to the results Figure 23. Detection range varies according to the weather and moonlight from 50m to 200m with eye sight. For this reason, Figure 23 also supports the idea that the configuration of GOP border security system has to be adjusted based on the line of sight (LOS).

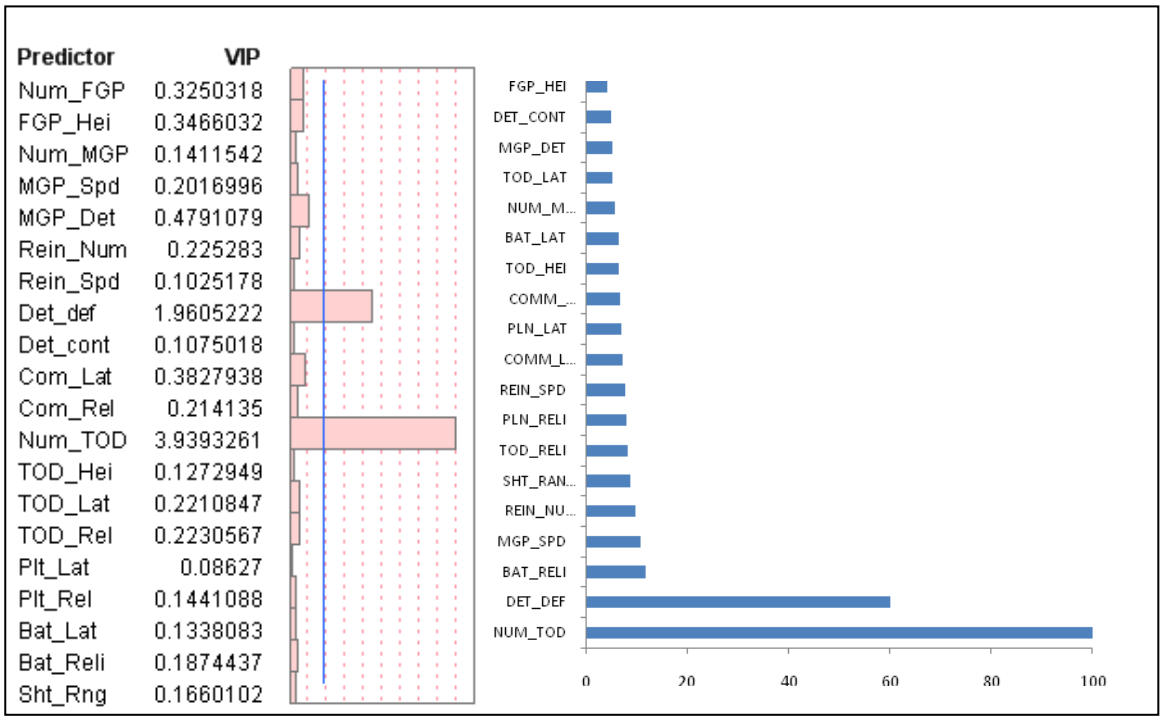


Figure 23. VIP score (left) and variable importance score (right) for MOE 1

As Figure 24 shows, the contour plot for MOE 1 corresponding to the number of TOD and detection range (default state) is identified in Figure 23. In general, as the number of TOD and the detection range increases, MOE 1 tends to increase. Since the infiltrator is assumed to have a detection range of 150 m, MOE 1 abruptly increases when the detection range becomes 150 m (15 MANA distance units). The detection rate has a relatively spread, from 0 to 0.8 when none of the TOD are used in the operational area, whereas it ranges from 0.6 to 0.9 when two TOD are used. When the number of TOD is

greater than equal to 2 then the MOE 1 is always greater than 0.6. Later, we explore this using regression.

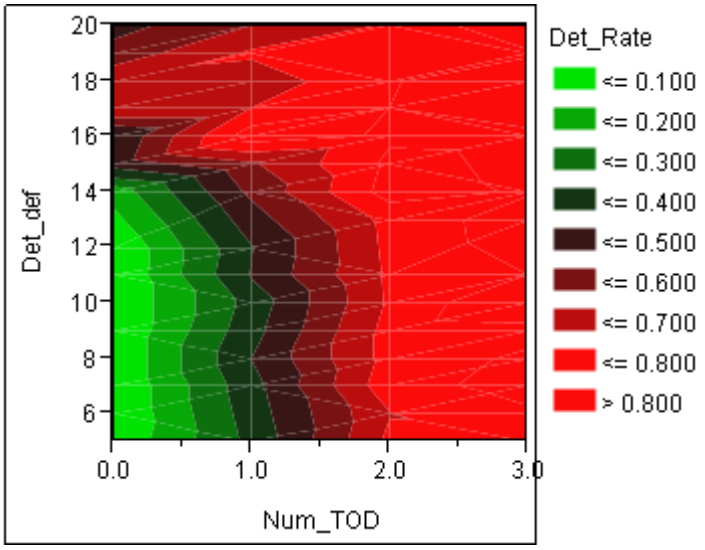


Figure 24. Contour plot for MOE 1 correspond to the detection range and the number of TOD

Since the number of TODs seems to be the most important factor of the surveillance system, i.e., MOE 1 is most sensitive to changes in the number of TODs, this sensitivity is further examined in Figure 25. A variability chart and a box plot are used for this analysis. In the variability chart, the polynomial fit of degree two has 0.59 RSquare value. The variability chart shows that when the number of TODs is more than one, it shows stable value of MOE 1, whereas it has a huge variability when the number of TOD is less than two. The variation of MOE 1 represents that the effectiveness of TOD decreases as the number of TODs increase as estimator of MOE 1 varies from 0.25, 0.48, 0.76, and

0.82 at each number of TOD. If the objective is maximization of MOE 1 with budget constraint, the results of Figure 25 can be useful reference. But, a cost analysis is not included in this study.

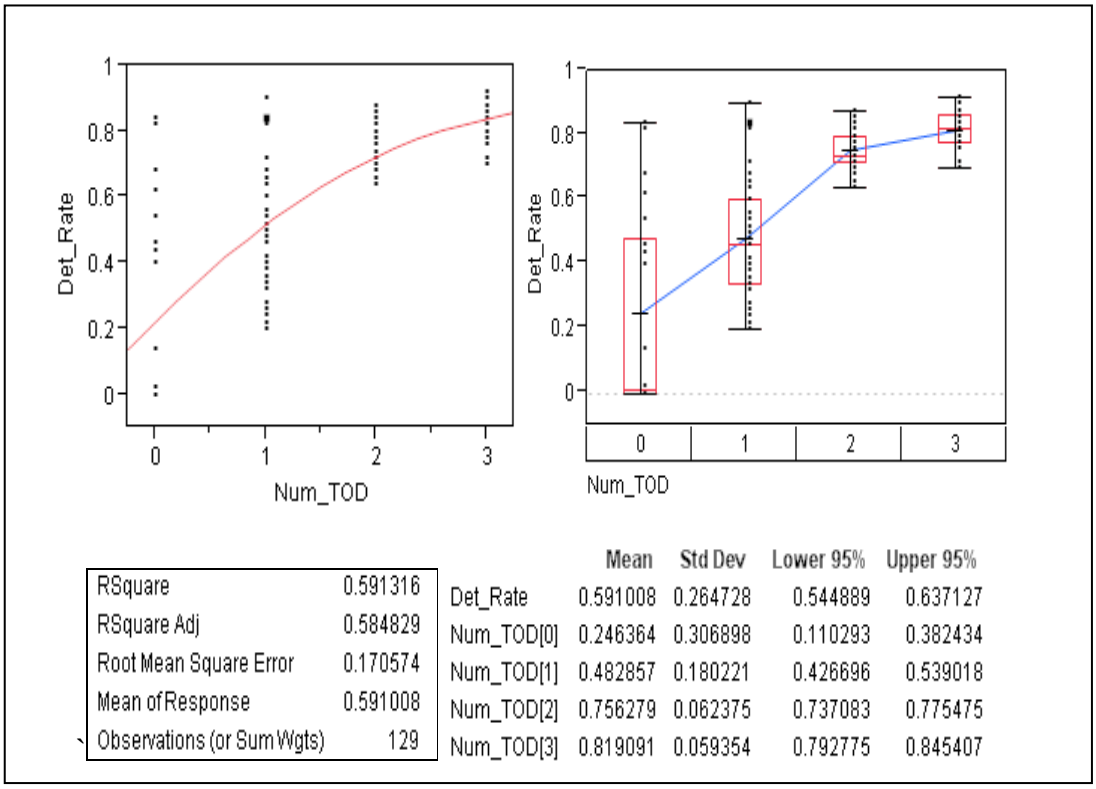


Figure 25. Variability chart and box plot chart for each number of TOD

Figure 26 shows a bivariate plot between the detection range and MOE 1 as the number of TODs increases. In Figure 26, a polynomial fit of degree two is used within the detection range (default state) of FGPs and Reinforcements ranges from 50 m to 200 m. When the system has no TODs, MOE 1 is very low within the detection range (default

state) of FGPs and Reinforcements, whereas MOE 1 abruptly increases when the detection range is 150 m. It is clear that the MOE 1 is affected by the detection range (default state) when the number of TOD is less than two. The RSqure fit is very close to zero when the number of TOD is greater than one and it indicates the fit is no better than the simple mean model as the mean square error is 0.06 in both cases. When the number of TOD is designated, the decision maker can estimate the MOE 1 from Figure 26.

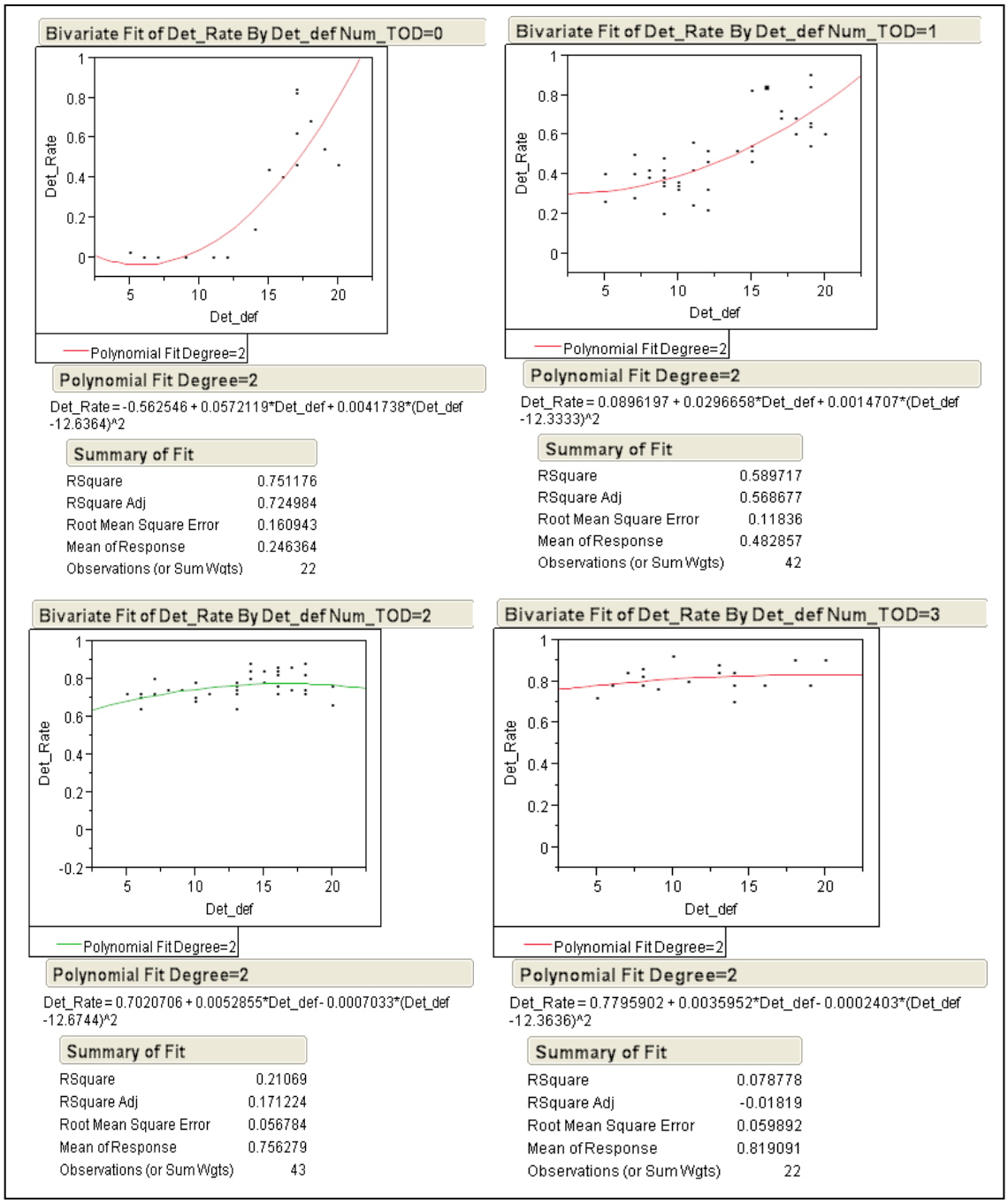


Figure 26. MOE 1 corresponding to the detection distance and the number of TOD

Figure 27 shows a regression tree with a partition feature as generated by JMP. By partitioning into regions (e.g., the number of TODs $\leq$ 2 and number of TODs $\geq$ 2) until achieving the desired fit, this regression tree is able to show the significance of factors. They are very useful for exploring relationships when the analyst does not have a good prior model. They handle large problems easily, and the results are very interpretable.

The regression starts with one group containing the non-missing dependent response (MOE 1) values. On the first partition, the platform calculates a splitting value for the factor that "best" splits the group into two groups. In this way, the split continues with each step, choosing the best split at each level. In this case > and < are used to point in the best direction for each variable. Among 10 splits, the first split indicates that when the number of TOD is greater than equal to two, there are 65 cases among 129 total cases in this condition, and the MOE 1 is higher than the overall average. On the other hand, when the number of TOD is less than two, there are 64 cases in this condition and the mean value tends to be lower than the overall average. In this manner, total 10 splits are implemented and the RSquare value is 0.941.

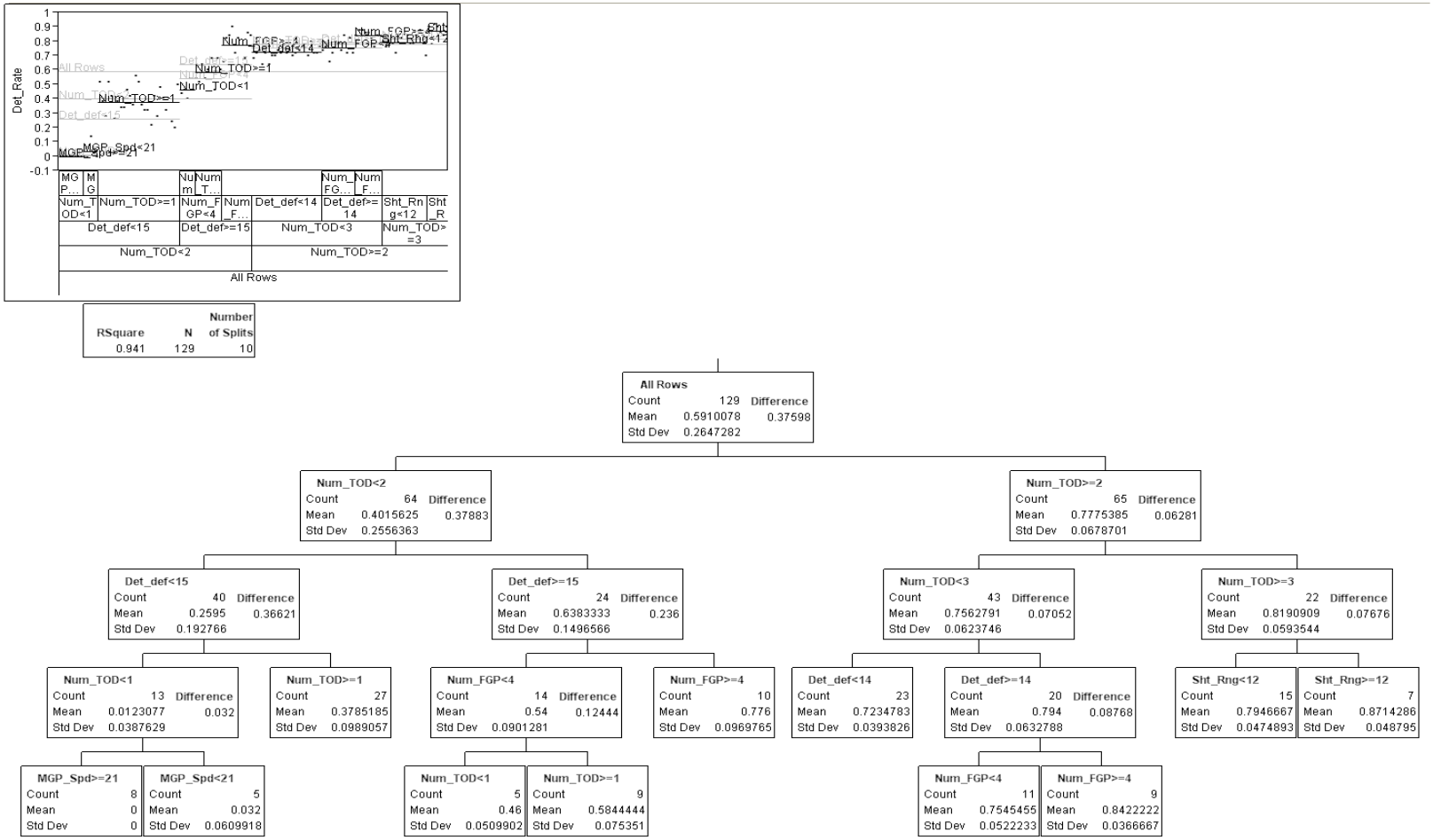


Figure 27. Regression tree output for MOE 1 (RSquare = 0.941)

5.5.3 PROBABILITY OF ENEMY KILLED (MOE 2)

In this scenario, the infiltrator is only killed by the FGP, MGP or reinforcement troops. The analysis for MOE 2 follows the similar steps with statistical results as MOE 1 in Section 5.5.1. In Figure 28, the shooting range of human resources, the detection range (default state), and the detection range of MGP are significant factors which affect the MOE 2 associate with VIP score. But, the variable important score shows that the detection range of MGP does not much contribute to the MOE 2. Although the MGP shows as important only in VIP score, it is meaningful in that the detection range of MGP ranges from 20 m to 50 m which is shorter FGP and reinforcement troop.

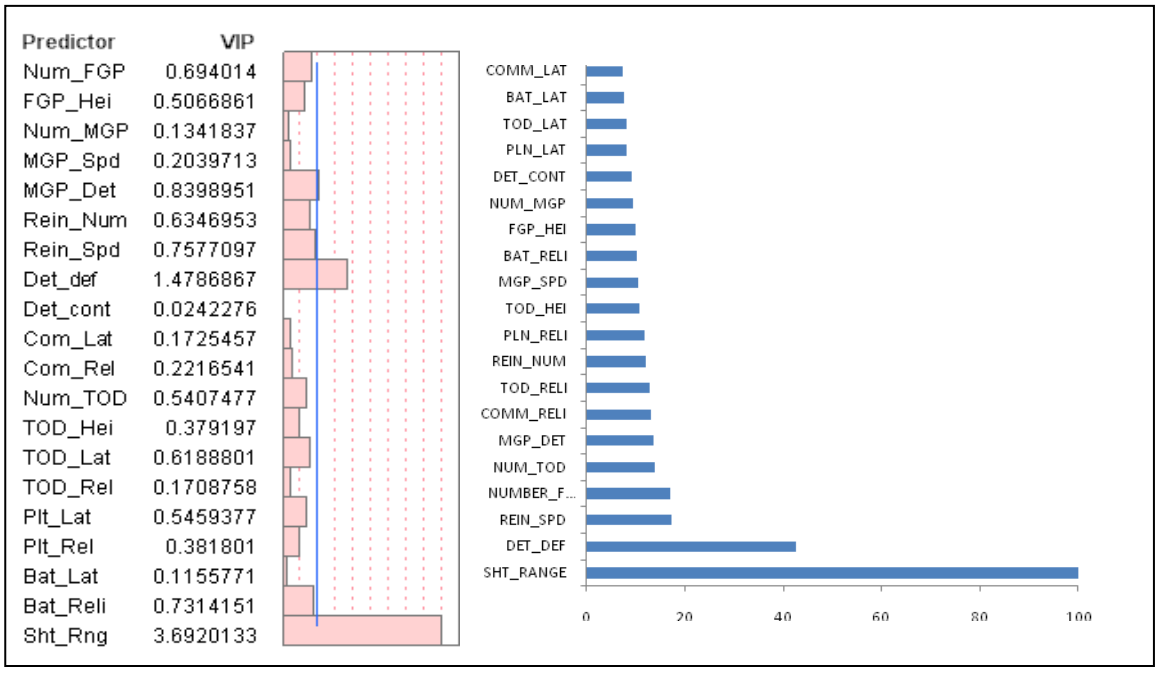


Figure 28. Variable importance for MOE 2

Because of the short shooting distance in the night situation and triggered behaviors of the enemy which observe the enemy earlier than the friendly force, MOE 2 is very low with current weapon system. For this scenario, the attack method such as howitzer gun and artillery are excluded but still the results of MOE 2 shows the night operation is vulnerable. As the contour plot represents in Figure 29, MOE 2 is almost always less than 0.4 regardless of shooting and detection range. In fact, without direct / indirect detection of the enemy, the human resources cannot shoot the enemy in our model. But, when comparing to the MOE 1, the results of MOE 2 is very low although the information of the situational awareness (SA) is shared thought the C2 network.

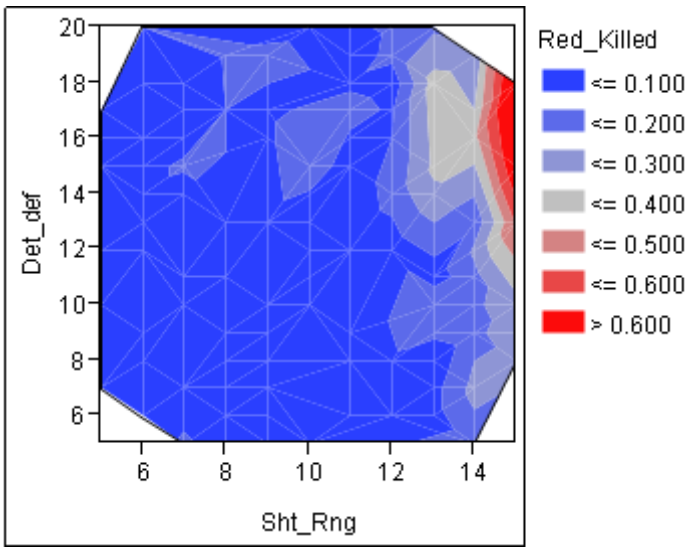


Figure 29. Contour plot for MOE 2 corresponding to the shooting range and the detection range (default)

As Figure 30 shows, MOE 2 is abruptly increased when the shooting range is 150 m, which is threshold distance in this scenario. The average MOE 2 is twice as large when the shooting distance is 150 m than 140 m which is huge jump compared to the increasing the range between 50 m and 140 m. When comparing the results of MOE 1 with Figure 30, there are many cases exist where the friendly forces miss the infiltrator although TOD detected the enemy.

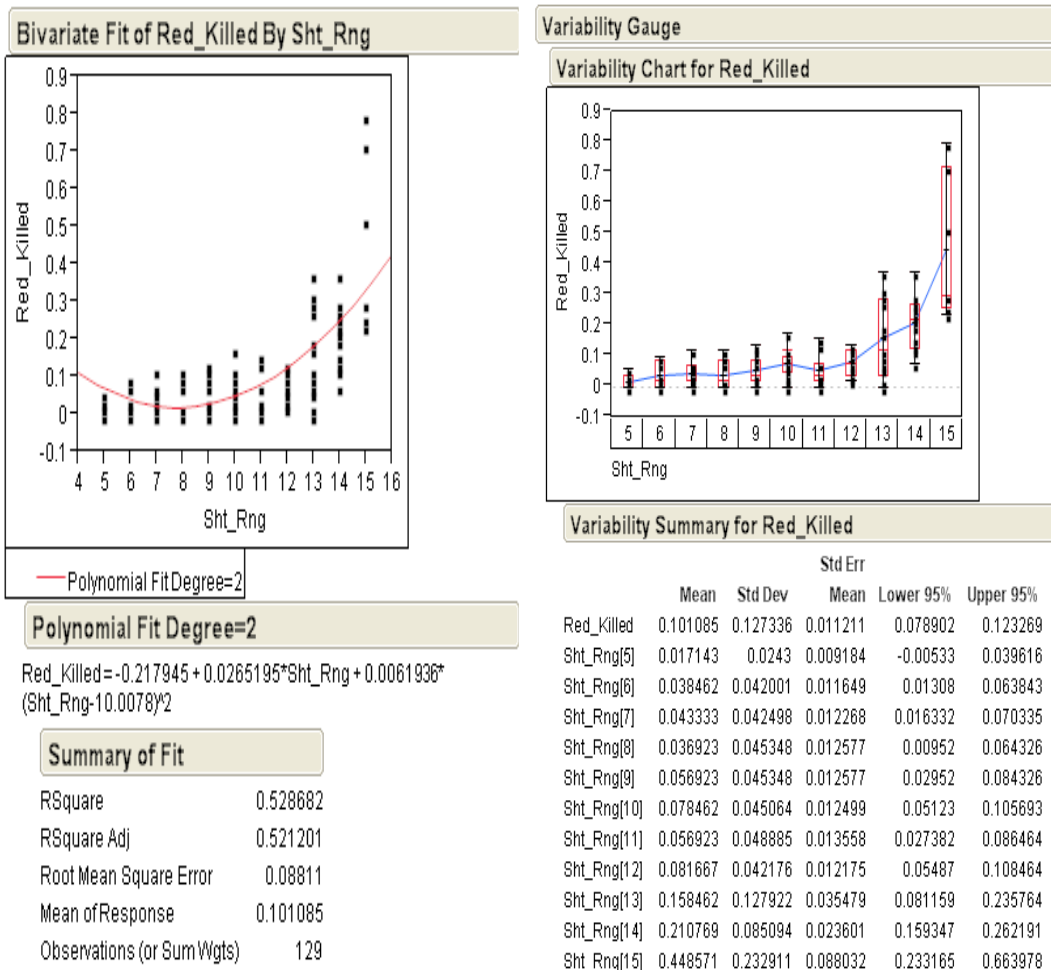


Figure 30. Variability chart and box plot chart for shooting range

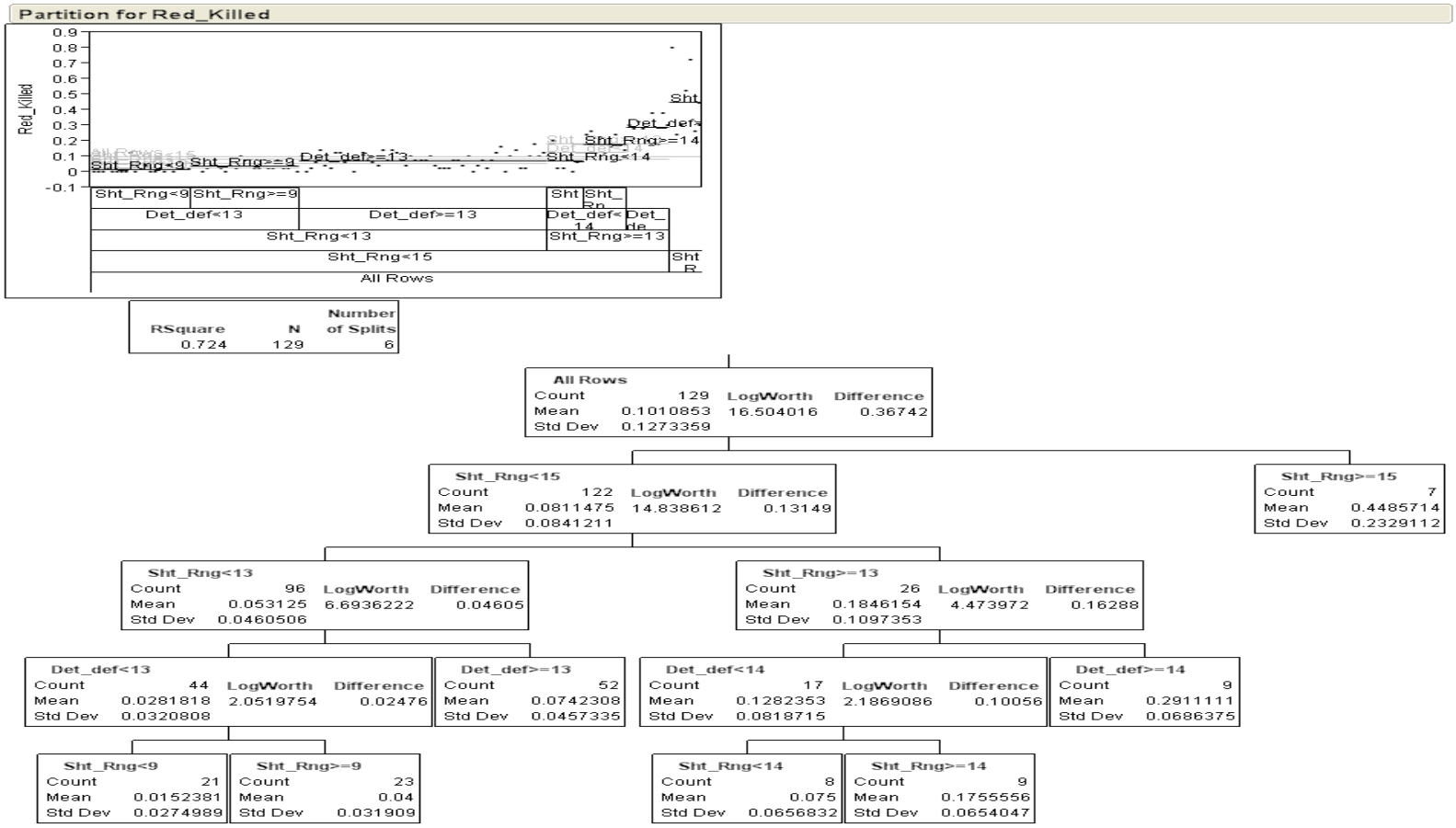


Figure 31. Regression tree output for MOE 2 (RSquare = 0.72)

5.5.4 AVERAGE TIME LENGTH TO THE WAYPOINT (MOE 3)

Four factors including number of TOD, shooting range, number of FGP, and detection range of MGP are identified significant for MOE 3 as can be seen VIP score in Figure 32. Number of TOD contributes to MOE 3 which can be interpreted as early detection makes the enemy have difficulties in overcoming the DMZ.

One more finding is that the number of MGP is one of the significant factors for MOE 3 with VIP value 0.91 although the infiltrator has behavior to avoid MGP with -24 from the results of GA. The previous study (Sung, 2005) draws the conclusion that the MGP does not contribute to the border security system, but the result from Figure 32 shows the MGP plays a role to delay the enemy near the GOP line.

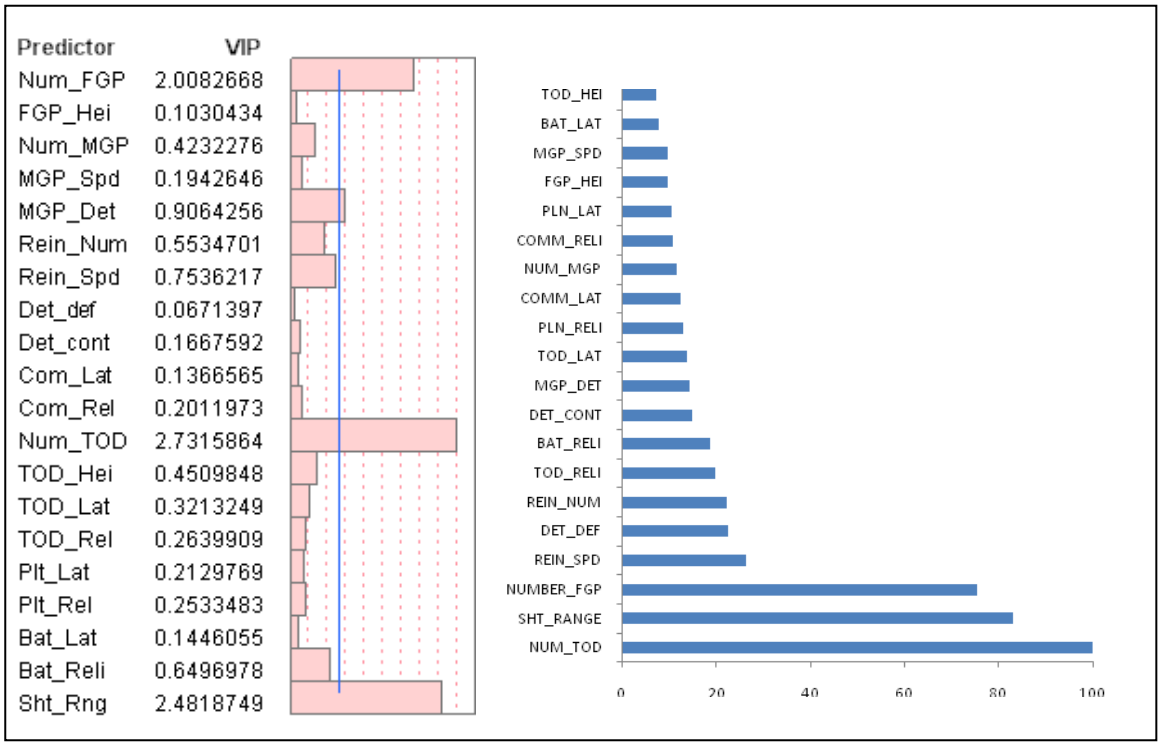


Figure 32. Variable importance for MOE 3

Based on the identified significant factors shown in Figure 32, Figure 33 helps understanding the relationship between the number of FGP and shooting range as the number of TOD is increasing. We omit the further explanation for the following figures for MOE 3.

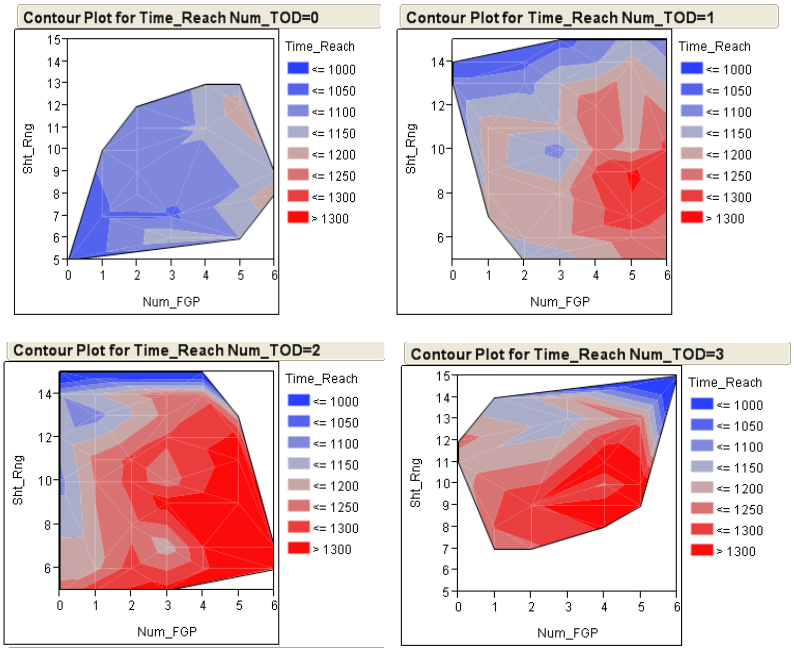
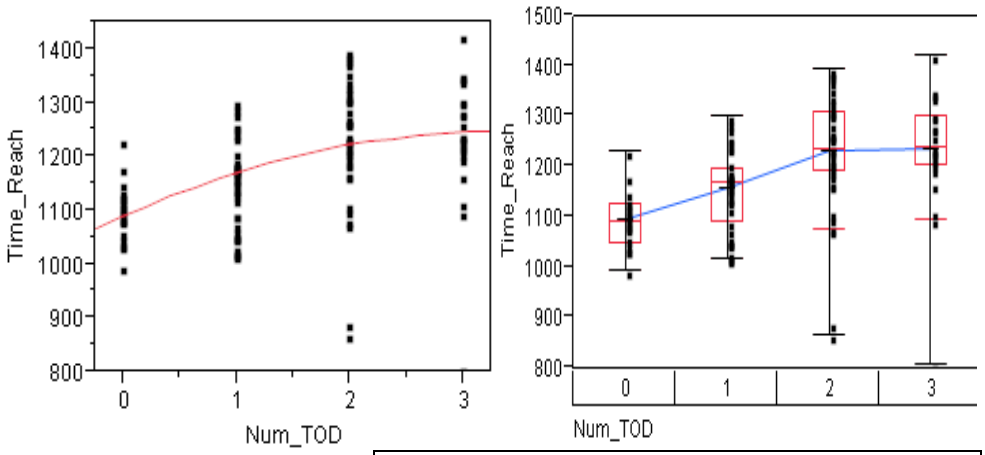


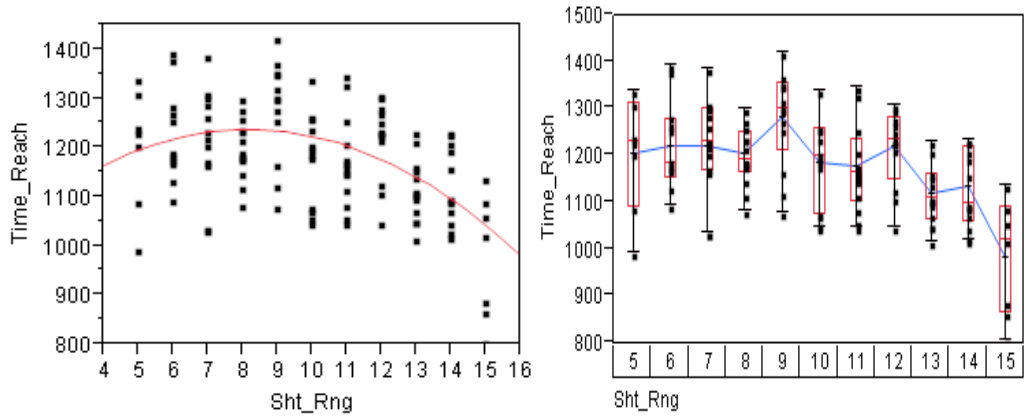
Figure 33. Contour plot for MOE 3 corresponding to the number of FGP and shooting range as the number of TOD increases



RSquare	0.225202
RSquare Adj	0.212903
Root Mean Square Error	97.27061
Mean of Response	1187.611
Observations (or Sum Wgts)	129

	Mean	Std Dev	Mean	Lower 95%	Upper 95%	Minimum	Maximum	Observations
Time_Reach	1187.611	109.6396	9.653233	1168.511	1206.712	811.48	1427.56	129
Num_TOD[0]	1097.709	53.05058	11.31042	1074.188	1121.23	999.38	1233.72	22
Num_TOD[1]	1160.434	78.95028	12.18229	1135.832	1185.037	1020.46	1306.4	42
Num_TOD[2]	1234	114.3089	17.43195	1198.821	1269.179	871.8	1398.92	43
Num_TOD[3]	1238.728	122.7393	26.1681	1184.309	1293.148	811.48	1427.56	22

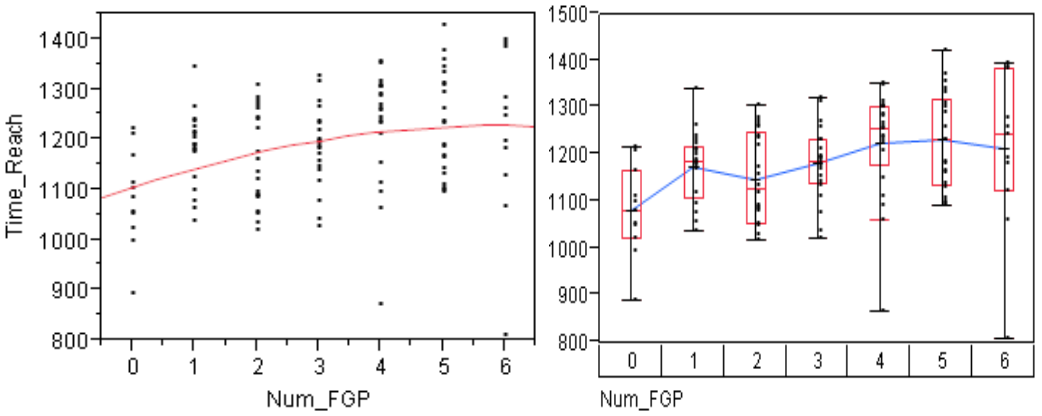
Figure 34. Variability chart and box plot chart for number of TOD



RSquare	0.2649
RSquare Adj	0.253231
Root Mean Square Error	94.74595
Mean of Response	1187.611
Observations (or Sum Wgts)	129

	Mean	Std Dev	Mean	Lower 95%	Upper 95%
Time_Reach	1187.611	109.6396	9.653233	1168.511	1206.712
Sht_Rng[5]	1207.874	121.7264	46.00824	1095.296	1320.452
Sht_Rng[6]	1224.845	92.67006	25.70205	1168.845	1280.845
Sht_Rng[7]	1224.765	106.0098	30.6024	1157.41	1292.12
Sht_Rng[8]	1206.962	62.6248	17.369	1169.118	1244.805
Sht_Rng[9]	1284.451	100.0512	27.74921	1223.99	1344.911
Sht_Rng[10]	1188.992	92.51001	25.65766	1133.089	1244.896
Sht_Rng[11]	1179.202	93.42015	25.91009	1122.748	1235.655
Sht_Rng[12]	1223.198	81.62388	23.56278	1171.337	1275.06
Sht_Rng[13]	1122.345	63.27901	17.55044	1084.105	1160.584
Sht_Rng[14]	1136.577	80.86145	22.42693	1087.713	1185.441
Sht_Rng[15]	986.7629	126.9409	47.97915	869.3621	1104.164

Figure 35. Variability chart and box plot chart for shooting range



RSquare	0.122601
RSquare Adj	0.108674
Root Mean Square Error	103.5109
Mean of Response	1187.611
Observations (or Sum Wgts)	129

	Mean	Std Dev	Mean	Lower 95%	Upper 95%
Time_Reach	1187.611	109.6396	9.653233	1168.511	1206.712
Num_FGP[0]	1084.056	96.33781	29.04694	1019.336	1148.777
Num_FGP[1]	1177.91	74.71948	16.30513	1143.899	1211.922
Num_FGP[2]	1151.605	95.39627	20.33855	1109.309	1193.902
Num_FGP[3]	1184.351	79.36163	17.31813	1148.226	1220.476
Num_FGP[4]	1227.634	114.1468	24.90887	1175.675	1279.593
Num_FGP[5]	1236.204	101.8928	21.72362	1191.027	1281.38
Num_FGP[6]	1214.329	172.1603	51.90828	1098.67	1329.988

Figure 36. Variability chart and box plot chart for number of FGP

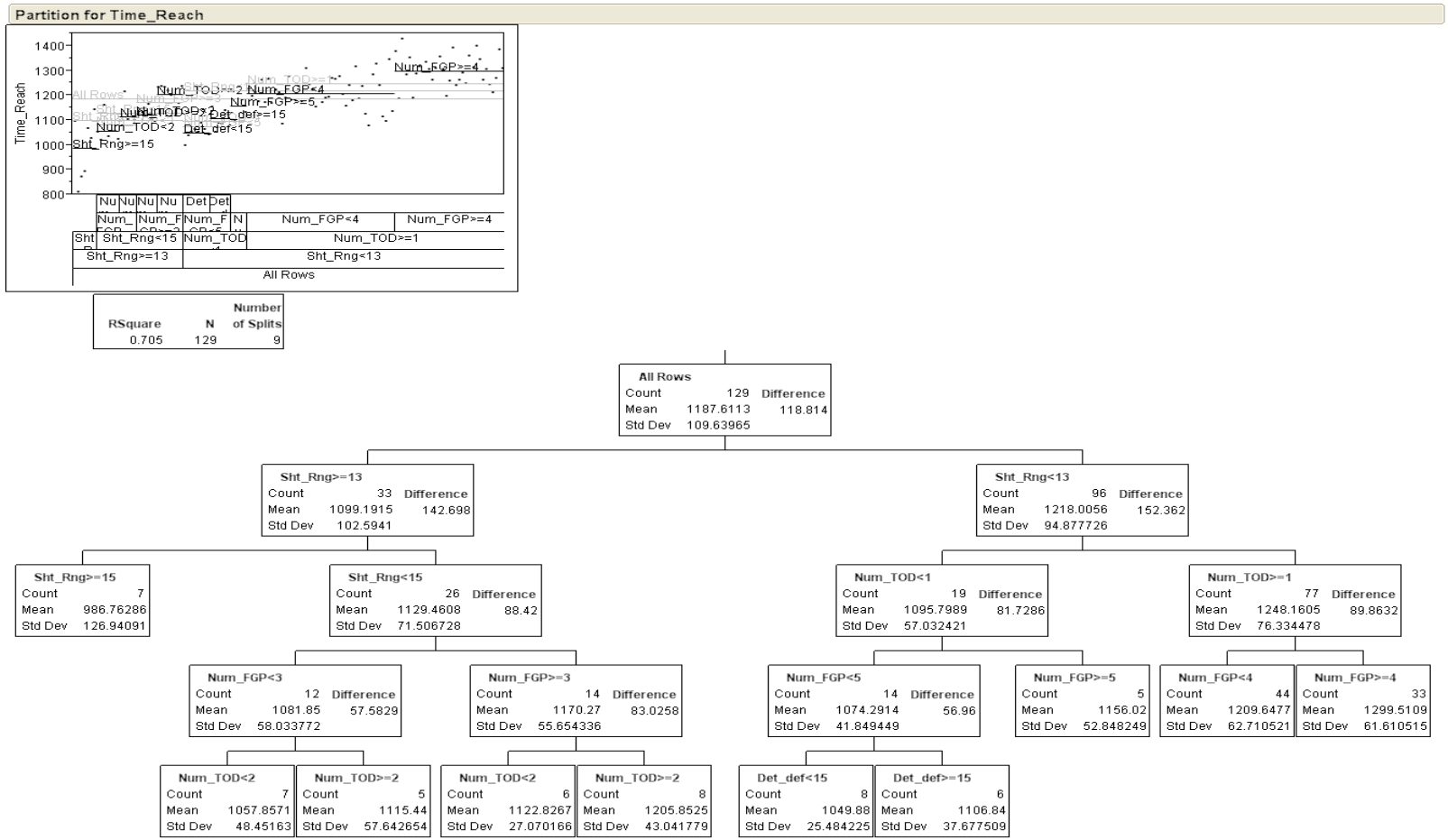


Figure 37. Regression tree output for MOE 3 (RSquare = 0.705)

5.5.5 PROBABILITY OF RED MISSION FAILED (MOE 4)

Five factors are identified as important variable in both results as shown in Figure 38. MOE 4 has characteristics which encompass the results from MOE 1 to MOE 3 as the correlation coefficient matrix shows. The number of TOD and FGP are comparable factors which affect the MOE 4. Compare to the variable importance for MOE 1 which score ratio of 100:60, Figure 38 shows unexpected importance of number of FGP similar to number of TOD. Also, number of reinforcement troops is newly identified as an important factor for MOE 4 which did not appear in the other MOEs.

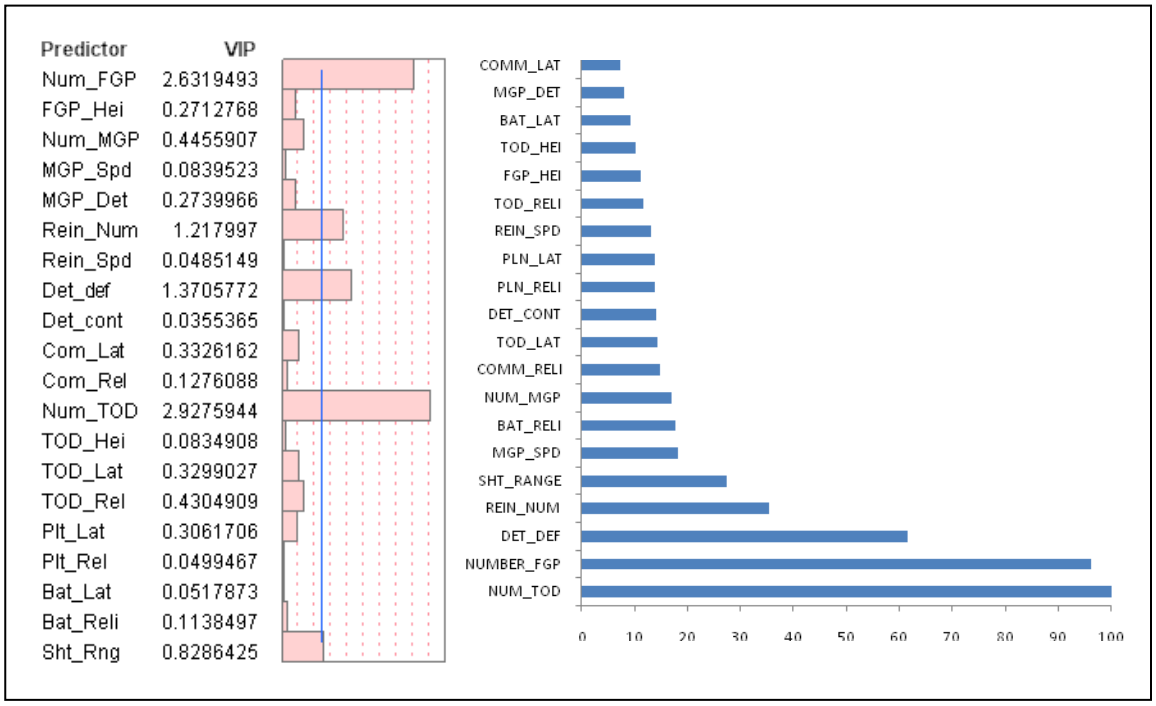


Figure 38. Variable importance plot for MOE 4

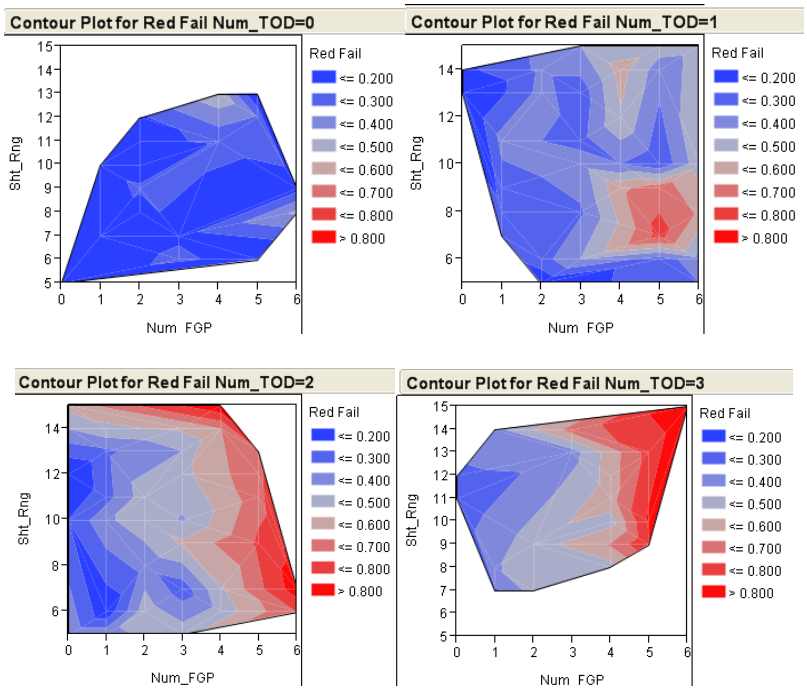
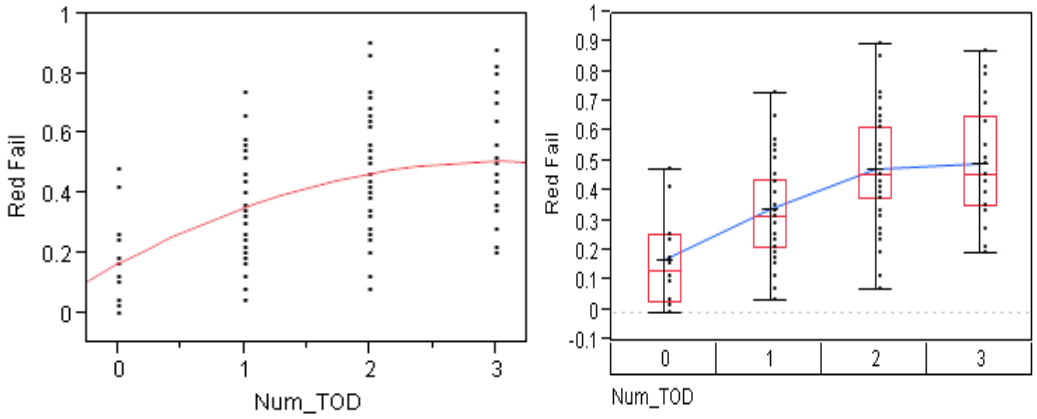


Figure 39. Contour plot for MOE 4 corresponding to the number of FGP and shooting range as the number of TOD increases



RSquare	0.312898
RSquare Adj	0.301992
Root Mean Square Error	0.173323
Mean of Response	0.387442
Observations (or Sum Wgts)	129

	Mean	Std Dev	Mean	Lower 95%	Upper 95%
Red Fail	0.387442	0.207456	0.018265	0.351301	0.423583
Num_TOD[0]	0.174545	0.157744	0.033631	0.104606	0.244485
Num_TOD[1]	0.34381	0.158852	0.024511	0.294308	0.393311
Num_TOD[2]	0.480465	0.184623	0.028155	0.423647	0.537284
Num_TOD[3]	0.501818	0.193111	0.041171	0.416198	0.587439

Figure 40. Bivariate Fit and Variability chart for number of TOD and MOE 4

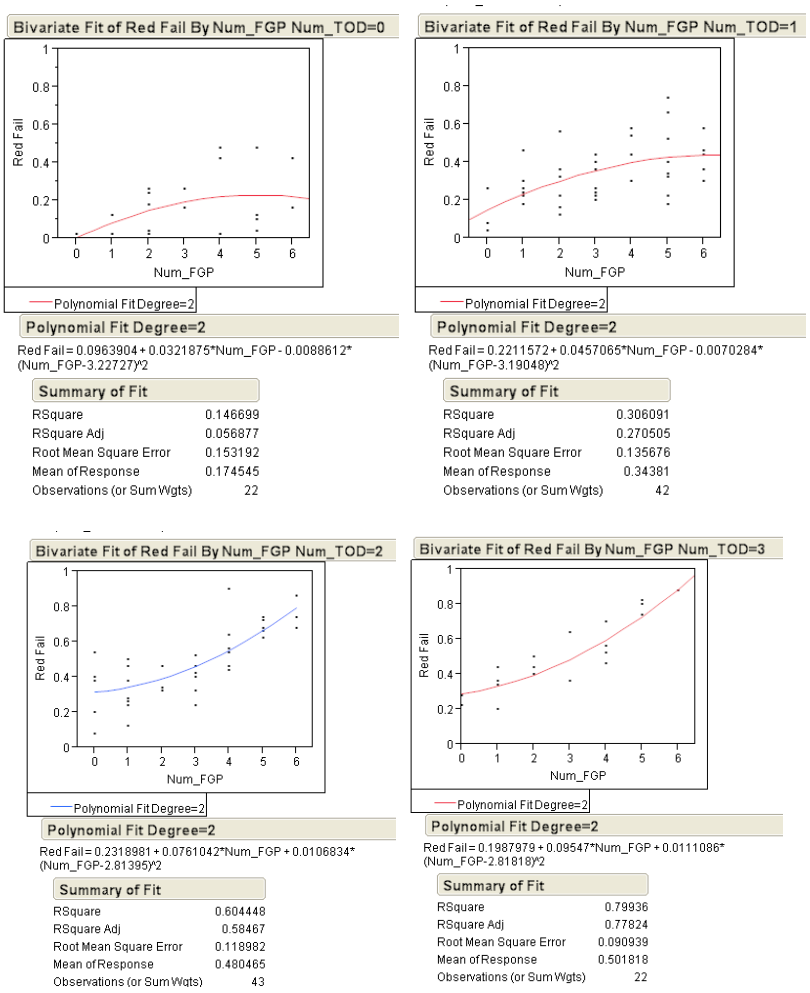


Figure 41. Bivariate fit of MOE 4 for the number of FGP as the number of TOD increases

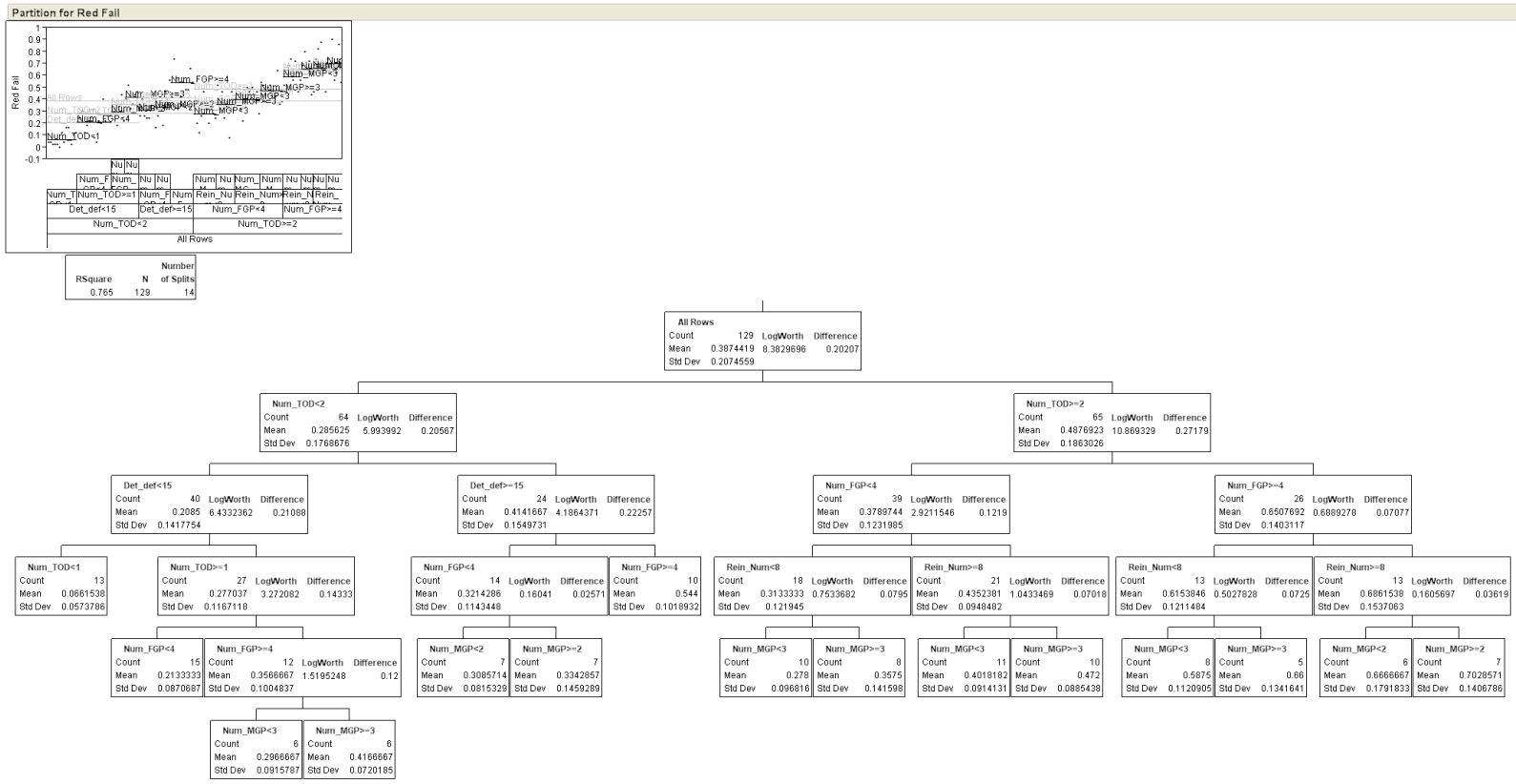


Figure 42. Regression tree output for MOE 4 (RSquare = 0.765)

CHAPTER 6 CONCLUSION

In this thesis, the border security problem of the ROK Army is examined by applying ABMS concept and its platform, MANA. There are previous studies exist which solve the border security problem thought the optimization technique, but few studies by simulation. Based on the stream of the border security problem by using ABMS, this study contributes to the military operations for the following aspects.

First, different from the previous work, this study suggests the way to evaluate the border security system in terms of three main systems, which are surveillance, communication, and weapon system through the four MOEs. This study provides two more measures that are time to reach the waypoint (MOE 3) and probability of enemy mission failed (MOE 4) in addition to the probability of enemy detection and enemy killed (captured). The coefficient correlation matrix of estimator for MOEs demonstrates the dependency of the pair of MOEs and it is expected to help analyzing the system with variety of aspects.

Second, the intelligent infiltrators who have the triggered behaviors are considered in the scenario. The previous analysis of the GOP border security system is not based on the enemy but the probability of the predicted enemy routes is used. But, this information purely relies on the prediction from the friendly force and the evaluation of the border security system must have a limitation. Also, studies for evaluating the effectiveness of UAV in the border security system of U.S use the randomly generated infiltrator without

having any triggered behaviors. In this study, the near optimal behavior of the infiltrator given the highest level of the border security system is obtained by using GA and used these characteristics to evaluate the border security system. We proved that the existence of the triggered behavior brings significantly different results. From the GA process, the decision maker can obtain an insight about the tactics of the infiltrator while observing the reiterative simulation in a short time. In the border security operation, the friendly force assumes the worst scenarios based on the maximized behavior of the infiltrator and prepares for the combat readiness. For this reason, this study can gives more reasonable evaluation which contains real situation.

Third, varieties of factors which consist of border security system were considered to identify the importance factors and obtain the interaction between the factors. Different from the previous works, the numbers of assets (TOD, FGP, MGP, and reinforcement troop) are considered for some of the factors of design points. Also, primarily detection range, communication condition (intra and inorganic), shooting range, turret heights, and moving speed are considered among 20 factors. From the results of the enormous number of simulation run, we could find the qualitative importance of each factor and obtain the graphical results for the decision maker.

The results of this study can provide good output for deciding the configuration of the assets, border security system structure, and number of soldiers assigned either post or platoon. Also, by considering detection range which affect by the weather and terrain

factors, the qualitative and quantitative system can be adjusted to attain the certain level of the effectiveness during the peacetime. Although, this study does not contain all the weapon system to detect and destroy the infiltrator, we identify that the probability of the enemy killed is relatively much lower than the probability of enemy detection. The connection between surveillance and weapon system need to be enforced to attain the effective border security system with current assets based on the scenario we used.

Based on this study, the ROK Army can evaluate ongoing project, GOP unmanned border security system which substitute human resources to the cameras and sensors. The ROK Army also has plans to increase the number of TOD to improve the border security system. As we identified in the result of Chapter 5, the effectiveness of TOD is not linearly increased so that the method in this study can be used to obtain the optimal number of assets by considering the limited budget. Given the number of equipment, the ROK Army would reduce the human resources along with the GOP line or operate the reinforcement troop instead of the stationed security guards.

APPENDIX A. INPUT PARAMETERS FOR THE GOP BORDER SECURITY SYSTEM MODEL

1. Human Resources

1.1 FGP

Number/platoon	This varies according to the border security level.		
Number of agent/post			2
Range	Allegiance		1
	Movement speed		0 (fixed)
	Threat number		1
	No. Hits to kill		1
	Slew rate		180 degree/step
Sensors	Eye (default)	Class/detect range	5 (50 m)
		Probability	1 (100%)
	PVS-7 (enemy contact)	Class/detect range	20 (200 m)
		Probability	1 (100%)
Weapon	K-2	Shooting range	5 (50 m)
		Hit rate	1 (100%)
Communication	Squad	delay	0 sec
		Persistence	30 (150 sec)
	Inorganic	latency	0 sec
		Reliability	100 %
		Accuracy	100 %
		Persistence	30 (150 sec)
	Enemy contact	Communication links with Platoon CCC	

1.2 MGP

Number/platoon	This varies according to the border security level.	
Number of agent/post		2
Range	Allegiance	1

	Movement speed		17 (1.2 km/h)
	Threat number		3
	No. Hits to kill		1
	Slew rate		90 degree/step
	Next Waypoint		100
sensor	eye	Classify/detect range	2 (20 m)
		Probability	1 (100%)
Weapon	K-2	Shooting range	5 (50 m)
Communication	Squad	delay	0 sec
		Persistence	30 (150 sec)
	Inorganic	latency	0 sec
		Reliability	100 %
		Accuracy	100 %
		Persistence	30 (150sec)
	Enemy contact	Communication links with Platoon CCC	

1.3 Reinforcement

Number/platoon	This varies according to the number of FGP and MGP		
number of soldier/post			2
Range	Allegiance		1
	Movement speed/default		0 (fixed)
	Movement speed/Inorganic SA enemy contact		50 (3.5 km/h)
	threat number		3
	No. Hits to kill		1
	Slew rate		180 degree/step
	Next Waypoint(enemy contact)		100
sensor	Eye (default)	Classify/detect range	5 (50 m)
		Probability	1 (100%)
	PVS-7 (enemy contact)	Classify/detect range	20 (200 m)
		Probability	1 (100%)
Weapon	K-2	Shooting range	5 (50 m)
Communications	Squad	Delay	0 sec

		Persistence	30 (150 sec)
	Inorganic	Latency	0 sec
		Reliability	100 %
		Accuracy	100 %
		Persistence	30 (150 sec)
Triggered Behavior	Enemy contact	Move to supplement post	
	Reach final waypoint	Play a role same as FGP	

2. TOD

number/baterion	This varies according to the border security level.		
Range	Allegiance		1
	threat number		3
	No. Hits to kill		1
	Slew rate		180 degree/step
Sensor	TOD	Classify/Detect range	200 (2000 m)
		Probability	1 (100 %)
Communication	Squad	Delay	0 sec
		Persistence	30 (150 sec)
	Inorganic	latency	0 sec
		Reliability	100 %
		Accuracy	100 %
		Persistence	30 (150 sec)
Triggered Behavior	Enemy contact	Report to Battalion CCC	

3. Command and Control Center

3.1 Platoon CCC

Range	Allegiance		1
	Threat		3
Communication	squad	Delay	0 sec
		Persistence	30 (150 sec)
	Inorganic	Persistence	30 (150 sec)
		Range	1000 (10000m)

		Latency	0 sec
		Reliability	100 %
		Accuracy	100 %
Triggered Behavior	Enemy contact	Send signal to reinforcement	

3.2 Battalion CCC

Range	Allegiance		1
	Threat		3
Communication	squad	Delay	0 sec
		Persistence	30 (150 sec)
	Inorganic	Persistence	30 (150 sec)
		Range	1000 (10000m)
		Latency	0 sec
		Reliability	100 %
		Accuracy	100 %
	Communication links between battalion CCC and each platoon CCC and TOD		

4. Infiltrator

Range	Allegiance		2
	Movement speed		56 (4 km/h)
	Threat number		1
	No. Hits to kill		1
	Slew rate		180 degree/step
Sensors	Eye (default)	Class/detect range	15 (150 m)
		Probability	1 (100%)
Communication	Squad	delay	0 sec
		Persistence	30 (150 sec)
	Inorganic	latency	0 sec
		Reliability	100 %
		Accuracy	100 %
		Persistence	30 (150 sec)
	Enemy contact	Communication links with Platoon CCC	

BIBLIOGRAPHY

Antony, J. (2003). *Design of Experiments for Engineers and scientists.* Burlington, MA.

Army, Republic of Korea. (2009). Retrieved June 2010, from http://www.army.mil.kr/mukihome/mugi/mg11.htm

Berner, A. R. (2004). The Effective Use of Multiple Unmanned Aerial Vehicle in Surface Search and Control. *M. S. Thesis.* Department of Operational Reasearch. Naval Postgrauate School, Monterey, CA.

Cioppa, T. M. (2005). *Efficient nearly orthogonal and space-filling Latin hypercubes.* Monterey, California: Operations Research Department, Naval Postgraduate School.

CNA Analysis & Solutions. (2010). Retrieved 06 2010, from http://www.cna.org/

Davis, L. (1991). *Handbook of Genetic Algorithms.* New York: Van Nostrand Reinold.

Defence Technology Agency-Project MANA. (n.d.). Retrieved June 2010, from https://teams.nzdf.mil.nz/sites/mana/default.aspx

Dick, K. N. (2008). *Chronology of Provocations, 1950-2003.* Report for Congress.

Ferber, J. (1999). *Multi-Agent System: An Introduction to Distributed Artificial Intelligence.* Boston, Massachusetts: Addson-Wesley.

Galligan, D. P., Anderson, M. A., & Lauren, M. K. (2005). *MANA (Map Aware Non-Uniform Automata) Version 3 User Manual.* DTA Technical note.

Galligan, D. P., Anderson, M. A., Lauren, M. K., & McIntosh, C. G. (2007). *MANA version 4 user manual.* DTA.

Goldberg, D. E. *Genetic Algorithms in Search, Optimization , and Machine Learing.* 1989.

Haupt, R., & Haupt, S. (1998). *Practical Genetic Algorithms.* John Wiley&Sons, Inc.

Ilachinski, A. (2004). *Artificial War: Multiagent-Based Simulation of Combat.* World Scientific Publishing Co.

Ilachinski, A. (1997). *Irreducible Semi-Autonomous Adaptive Combat (ISAAC): An Artificial Approach to Land Warfare* (Vols. CRM 97-61). Alexandria, Virginia: Center for Naval Analysis.

Ilachinski, A. (1999). *Towards a Science of Experimental Complexity: An Artificial-Life Approach to Modeling Warfare.*

Lanchester, F. W. (1916). *Aircraft in Warfare, the Dawn of the Fourth Arm.* London.

Lauren, K. M. (2005). *A Metamodel for Describing the Outcomes of the MANA Cellular Automaton Combat Model Based on Lauren's Attrition Equation.* DTA Report 205.

McIntosh, C. G. Genetic Algorithms Applied to Course-Of-Action Develpement Using the MANA Agent-Basd Model. *Journal of Battlefield Technology , 9* (3).

McIntosh, C. G. (2009). *MANA-V (Map Aware Non-Uniform Automata-Vector) Supplementary Manual.* DTA.

McIntosh, C. G., & Lauren, K. M. (2006). Genetic Algorithms Approach to Course-Of-Action Development Using the MANA Agent-Based Model. *Journal of Battlefiled Technology , 19* (3).

McIntosh, C. G., Galligan, D. P., Anderson, M. A., & Lauren, M. K. (May 2007). *MANA (Map Aware Non-Uniform Automata) Version 4 User Manual.*

Munro, R. A. (2007). *The Certified Six Sigma Green Belt Handbook.* American Society for Qualit.

Patrascu, A. (2007). Optimizing Distributed Sensor Placement For Border Patrol Interdiction Using Microsoft Excel. *M.S. Thesis.* Ohio: Department of the Air Force.

Proust, M. (2008). *JMP Statistics and graphics guide, release 8.* SAS Institute Inc.

Pulat, H. (2005). A Two-sided Optimization of Border Patrol Interdiction. *M. S. Thesis.* Monterey, CA: Department of Operational Research, Naval Postgraduate School.

Reynolds, W. C. (1987). Flocks, Herds, and Schools: A Distributed Behavioral Model. *Computer Graphics* , 21(4): 25-34.

ROK Army Headquarter. (n.d.). Retrieved 04 07, 2010, from http://www.army.mil.kr/gbbs/mukihome/index.html

Salford Systems. (2005). TreeNet Version 2.0. San diego, California, U.S.

Salon Wanderlust. (2000). Retrieved 04 10, 2010, from Korea's No-Man's-Land: http://www.salon.com/wlust/feature/1999/02/03feature2.html

Sanchez, S. M. (2005). *NOLH Designs Spreadsheet*. Retrieved 02 16, 2010, from SEED Center: http://diana.cs.nps.navy.mil/SeedLab

Sanchez, S. M. (2007). Work Smarter, Not Harder: Guidlines For Designing Simulation Experiments. *Winter Simulation Conference* .

Security, FM 32-1 (Vols. FM 2-11). (2003). ROK Army Headquarter.

SEED Center for Data Farming. (n.d.). Retrieved 04 03, 2010, from http://harvest.nps.edu

Sprague, B. K., & Dobias, P. (2008). Modeling the Complexity of Combat in the Context of C2. *The International C2 Journal , 2* (2).

Straver, M. C., Vincent, E., & Fournier, P. (2006). *Experiences with the MANA simulation tool.* Defence Research and Development Canada.

Sung, C. (2005). *Exploration of Matehmatical Modeling of the Border Security.* Korea Advanced Institute of Technology (KAIST).

The ROK Army Defense Reform 2020. (n.d.). (M. o. Defense, Producer) Retrieved 04 12, 2010, from http://www.globalsecurity.org/military/world/rok/doctrine.htm

University of Wisconsin-Madison. (n.d.). *Condor.* Retrieved 04 10, 2010, from http://www.cs.wisc.edu/condor/

Upton, S. C. (2006). *User' Guide, OldMcData-The Data Farmer, version 1.0 beta.*

Weiss, G. (1999). *Multi-Agent System: A Modern Approach to Distributed Artificial Intelligence.* Cambridge, Massachusetts: The MIT Press.

Weiss, G. (1999). *Multi-Agent Systems: A Modern Approach to Distibuted Artificial Intelligence.* Cambridge, Massachusetts: The MIT Press.

Wold, S. (1994). PLS for Multivariate Linear Modeling. QSAR: Chemometric Methods in Molecular Design. Methods and Principles in Medicinal Chemistry.

Yildiz, B. (2009). Exploration of the Use of Unmanned Aerial Vehicles Along with Other Assets to Enhance Border Protection. *M. S. Thesis.* Department of Operational Reasearch. Naval Postgrauate School, Monterey, CA.

VITA

Kyungtack Oh was born in Kyunggi province, Republic of Korea on September 24th, 1982, the son of Jinseok Oh and Hyunjoo Lim. He graduated from Guangsin High School in Seoul, Republic of Korea in 2001. In 2005, he earned his Bachelor of Science Degree in Applied Chemistry and military art and science from the Korea Military Academy in Seoul, Republic of Korea.

After he received a B.S. degree, he was commissioned as an Infantry platoon leader and an Aid de camp as part of the 5th Infantry division until 2007. In the meantime, Kyungtack Oh was selected as a student to be sent abroad on government support in 2008 and he entered the University of Texas at Austin in August 2008 in pursuit of a Master's degree in Operations Research and Industrial Engineering. His research interests include modeling and simulation, metaheuristics and application of military OR.

Email : kt6461@gmail.com

This thesis was typed by the author.