2022-12

TRADE-OFF ANALYSIS OF LARGE-SCALE SWARM ENGAGEMENTS

Redder, Nathan C.

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/71529

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

TRADE-OFF ANALYSIS OF LARGE-SCALE SWARM ENGAGEMENTS

by

Nathan C. Redder

December 2022

Thesis Advisor: Abram H. Clark IV
Co-Advisor: Isaac I. Kaminer

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

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

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE TRADE-OFF ANALYSIS OF LARGE-SCALE SWARM ENGAGEMENTS	**5. FUNDING NUMBERS** RMK2H; R4Q04
6. AUTHOR(S) Nathan C. Redder	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Office of Naval Research/CRUSER	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

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

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

13. ABSTRACT (maximum 200 words)

This research performs trade-off analysis on attacker-defender swarm engagements to compare the relative efficiency of factors governing swarm behavior, namely targeting algorithms and individual drone parameters. In particular, we examined algorithms developed for the Service Academies Swarm Challenge (SASC), a live-fly drone swarm exercise of swarm-on-swarm engagements. We performed this analysis with dynamic swarm simulations that permitted variations in swarm composition and behavior. This allowed us to confirm the qualitative results of swarm performance from the SASC. In addition, we used scaling analysis methods to perform quantitative trade-off analysis and developed functional forms to assess defender swarm fitness. Our results provide a framework for studying more complex swarm behaviors in follow-on research.

14. SUBJECT TERMS drone, autonomy, autonomous systems, swarm	**15. NUMBER OF PAGES** 65
	16. PRICE CODE

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

NSN 7540-01-280-5500

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

THIS PAGE INTENTIONALLY LEFT BLANK

TRADE-OFF ANALYSIS OF LARGE-SCALE SWARM ENGAGEMENTS

Nathan C. Redder
Lieutenant, United States Navy
BS, University of Michigan, 2016

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN APPLIED PHYSICS

from the

NAVAL POSTGRADUATE SCHOOL
December 2022

Approved by: Abram H. Clark IV
Advisor

Isaac I. Kaminer
Co-Advisor

Frank A. Narducci
Chair, Department of Physics

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research performs trade-off analysis on attacker-defender swarm engagements to compare the relative efficiency of factors governing swarm behavior, namely targeting algorithms and individual drone parameters. In particular, we examined algorithms developed for the Service Academies Swarm Challenge (SASC), a live-fly drone swarm exercise of swarm-on-swarm engagements. We performed this analysis with dynamic swarm simulations that permitted variations in swarm composition and behavior. This allowed us to confirm the qualitative results of swarm performance from the SASC. In addition, we used scaling analysis methods to perform quantitative trade-off analysis and developed functional forms to assess defender swarm fitness. Our results provide a framework for studying more complex swarm behaviors in follow-on research.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Acronyms and Abbreviations

DARPA	Defense Advanced Research Projects Agency
HVU	High Value Unit
SASC	Service Academies Swarm Challenge

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

I would like to thank my advisers, Dr. Kaminer and Dr. Clark, for their help and support. Their assistance and guidance was invaluable.

Chloe, love you. Thank you for putting up with the late nights and early mornings.

Mom and Dad, thank you for providing me every opportunity needed to get to where I am today.

Steve and Jody, thank you for your kindness and hospitality. It helped make this process easier.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1: Introduction To Drone Swarms

Drone swarms are groups of autonomous vehicles which coordinate and communicate to achieve goals [1]. The size of a drone swarm can be scaled arbitrarily according to swarm capability and the ability of an actor to logistically support the swarm. Militarily, large swarms present high risk to a High Value Unit (HVU), such as an aircraft carrier, due to the swarm's ability to overwhelm existing HVU point defenses [2].

1.1 Risks From Drone Swarms

The ability to field a drone swarm has historically been limited by computer processing, drone-to-drone communication, and energy storage density [3]. Developments in these fields have, however, led to increased swarm development and feasibility. This has caused the risk from drone swarms to increase dramatically. Large swarms have become increasingly possible, with China testing swarms of over 1000 drones as early as 2017 [3]. The technological improvements which have made drone swarms more practical are expected to continue.

The largest drone risk to HVUs are aerial drones executing a suicide mission while utilizing an on-board explosive charge. The goal of the swarm is, through sheer numbers, to saturate HVU defenses and either destroy or disable the HVU. Current HVU defenses, such as missiles or close-in weapon systems, are insufficient and uneconomical to counter large drone swarms [2]. These defenses, designed to counter aircraft and missiles, are unequipped to deal with drones and their drastically different threat profile. A swarm's low-cost and large size risks the HVU expending the entirety of its limited defensive ordnance while only destroying a fraction of the swarm [2]. The HVU, in this case, would then be vulnerable to either the swarm remnants or attacks from other units exploiting its exhausted defenses.

The strategic utility and financial value of the HVU can also lead to an adversary benefiting from the HVU's destruction at the cost of an entire drone swarm. Capable drones can be fielded for as little as $500,000 per unit [2]. This estimate includes the cost of the drone, launcher, and logistical support. Therefore, a 600 drone swarm, capable of attriting existing HVU defenses, would cost a total of $300 million [2]. This compares favorably with the

$12 billion cost of an aircraft carrier [4]. This disparity allows swarms to be used as force multipliers to minimize the advantages the U.S. currently gains from expensive HVUs [5].

1.2 Counter Swarming Techniques

Proposed methods of countering drone swarms include laser and electromagnetic weapons and drone counter-swarming. Laser and electromagnetic weapons are technically better suited to countering a drone swarm than existing point defenses due to their ability to expend a nearly limitless number of shots. However, neither weapon system is currently widely fielded. In fact, both laser and electromagnetic weapons have faced substantial technical difficulties and would require considerable technological advancement to credibly provide counter-drone defense [6].

Drone counter-swarming consists of using a defensive drone swarm to combat the offensive, adversarial drone swarm. This swarm countermeasure has a relative dearth of research compared to offensive drone swarms. However, defensive drone swarms have the advantage, over other countermeasures, of leveraging the same technological advances that have spurred the development of offensive drone swarms. As offensive drone swarms become more capable, so too do defensive drone swarms. In fact, defensive drone swarming is likely easier to implement than offensive swarming due to defensive swarms operating among friendly forces in controlled airspace [7]. Counter-swarming also allows a defender to undermine the most significant advantage of an offensive drone swarm, its size. A defensive drone swarm can have sufficiently large size to mitigate an offensive swarm's ability to saturate defenses.

Previous work from researchers at the Naval Postgraduate School has focused on examining counter-swarming as an optimal control problem [8]–[12]. This previous work utilized potential-based models, long-range weapons, and defender herding strategies. This thesis builds on these previous works by implementing different swarm cooperation rules and applying new analysis techniques. For example, prior studies focused on long-range weapons where the attacking swarm was engaged as a whole. This thesis focuses on simulations using short-range weapons, where defenders engage individual attackers. Additionally, this thesis examines trade-off analysis instead of optimization, but the tools described here could be combined with optimization in future work.

The development of a defensive drone swarm requires answering a series of questions. First, what are the best tactics for a defending swarm to best counter the attacking swarm? Second, what platform specifications, such as speed or weapon range, would be most effective? Third, what costs or technological limitations associated with these platform specifications might affect the feasibility of fielding the optimal swarm? These three categorical questions include many other questions. For example, what is the benefit of adding more drones, given an algorithm and a set of platform specifications? Is there a point at which adding more drones is no longer beneficial? How does an improvement in platform specifications compare with adding more drones; e.g., is it more advantageous to double speed or the number of drones?

To answer these questions, mission planners and designers must perform a comprehensive trade-off analysis of drone swarm parameters to determine how to maximize swarm capabilities while minimizing swarm cost. A thorough distillation of factors such as swarm behavior, swarm size, and individual drone performance, to include its speed and weapon range, could allow a mission planner to field the drone swarm which most capably and economically counters adversarial swarms. Without this analysis, a mission planner risks making a swarm that is insufficient to defeat the offensive swarm which places the HVU at risk. Conversely, the mission planner could also create a drone swarm which soundly defeats the offensive swarm but is an inefficient allocation of resources. At present, there are few analysis tools that are suited for performing these planning tasks. The goal of this thesis is to begin to fill this knowledge gap.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2: Case Study: Service Academy Swarm Challenge

Answering the analysis and planning questions at the end of the previous chapter requires the selection of different tactics and platform specifications to compare against one another. Since there are an essentially unlimited diversity of swarm tactics that could be chosen, the literature was investigated to find simple, realizable algorithms that could demonstrate an appropriate analysis framework.

A literature review revealed the Defense Advanced Research Projects Agency (DARPA) Service Academies Swarm Challenge (SASC) as an excellent candidate. In this 2017 live-fly swarm exercise, service academy student teams were provided with existing drones and drone control programs by DARPA. These teams then fielded swarms, of up to 25 drones, against other service academy teams. They then attempted to accomplish objectives including destroying opposing drones and controlling aerial territory [13].

2.1 Swarm Targeting Behaviors

During the SASC, DARPA provided teams with several drone targeting and control algorithms of varying complexity and effectiveness. The teams also developed and implemented targeting behaviors of their own design. Together, these included Greedy Shooter (Greedy), Smart Shooter (Smart), and Reverse Shooter (Intercept). Throughout the competition, the success of swarms with varying targeting behavior was compared to determine their relative effectiveness [14].

2.1.1 Greedy

Greedy consisted of each defending drone determining the closest attacking drone and flying a direct path toward the attacking drone. This behavior was relatively simple to implement and required minimal communication or coordination among swarm members. However, this behavior also led to sub-optimal drone pairings, with multiple defending drones attacking a single attacking drone while other attacking drones were not targeted.

Greedy, therefore, tended to be the lowest performing of the DARPA-provided targeting algorithms [14].

2.1.2 Smart

Smart consisted of the swarm distributing targets so each defender targeted the closest opposing drone that was not already targeted by a defender. After selecting a target, the defending drone would fly a direct path to the attacking drone. Smart resulted in defenders being allocated to attackers more efficiently than Greedy and avoided numerous defenders attacking a single target. Therefore, Smart outperformed Greedy during the competition [14]. However, a weakness of Smart was its tendency to enter into tail-chases of opposing drones due to flying directly at its target's current position.

2.1.3 Intercept

Intercept, like Smart, consisted of each drone targeting the closest attacking drone that was not already being targeted. However, each defending drone also calculated and flew an intercept path with the attacking drone instead of flying directly toward the attacker. This allowed earlier intercept of attacking drones and avoided defending drones entering tail-chase situations. Intercept outperformed Greedy and slightly outperformed Smart [14].

2.1.4 Swarm Relative Effectiveness

The SASC determined that Greedy performed the poorest of these algorithms. In addition, the competition found that drone algorithm and swarm size were the largest factors in predicting swarm success [14]. The SASC also demonstrated the binary dynamic of swarm engagements, with one side winning an engagement and the other losing. Winning the engagement allowed one's swarm to operate unimpeded while, conversely, losing the engagement allowed the adversary unimpeded operations [14]. However, unimpeded operations were achieved regardless of the scale of the victory. Therefore, a swarm would be effective regardless of how convincingly they defeated the adversary as long as victory was achieved.

2.2 Algorithm Comparison and Trade-Off Analysis

Due to the binary nature of winning versus losing an engagement, trade-offs of swarm capabilities and performance must focus on the crossover point of swarm performance. That is, the point at which a swarm transitions from being insufficient to counter an adversary to the point at which it is sufficient. By quantitatively determining this point, drone parameter performance and swarm performance can be identified. By determining the most important swarm parameters, a mission planner can invest in those capabilities while limiting investment in less important parameters. Therefore, identification of swarm performance criteria coupled with trade-off analysis can improve swarm fitness.

While the SASC provided a benchmark for assessing and predicting swarm performance, the results were largely qualitative. Therefore, it has limited quantitative or predictive capability. While a quantitative model is required for proper mission planner use, the SASC was valuable in providing a live-fly exercise which can be compared to future quantitative trade-off work.

The algorithms in the SASC also provided a good test case to compare qualitative differences in algorithm choice as well as changes to platform specifications. The computer simulations discussed in the following chapters will allow a comprehensive comparison and trade-off analysis of all algorithms and platform specifications.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3: Swarm Modeling Methodology

Determining drone swarm trade-off analysis requires modeling an engagement between an offensive and defensive drone swarm. The ultimate objective of this analysis is to develop and demonstrate an analysis framework that can be used to determine which swarm tactics and platform specification parameters most efficiently contribute to overall swarm fitness. Simulations are run with varying drone defensive behaviors and parameters, such as acceleration, velocity, weapon range, and swarm size. Across the range of parameters, the time for the defending swarm to completely destroy the attacking swarm is measured.

3.1 Modeling Dynamic Behavior

An offensive and defensive swarm are initially generated a fixed distance from each other. The attacking drone swarm is modeled to spread and evade the defenders at the start of each simulation and is assumed to consist of drones designed to strike HVUs and unable to attack defender drones. The defender goal is to destroy attackers. The standard initial conditions for a simulation is shown in Figure 3.1 with defenders in blue, attackers in red, and the HVU in green. For actual simulations, the defenders and attackers are plotted while the HVU is not explicitly plotted and is instead assumed to be behind the defender initial positions.

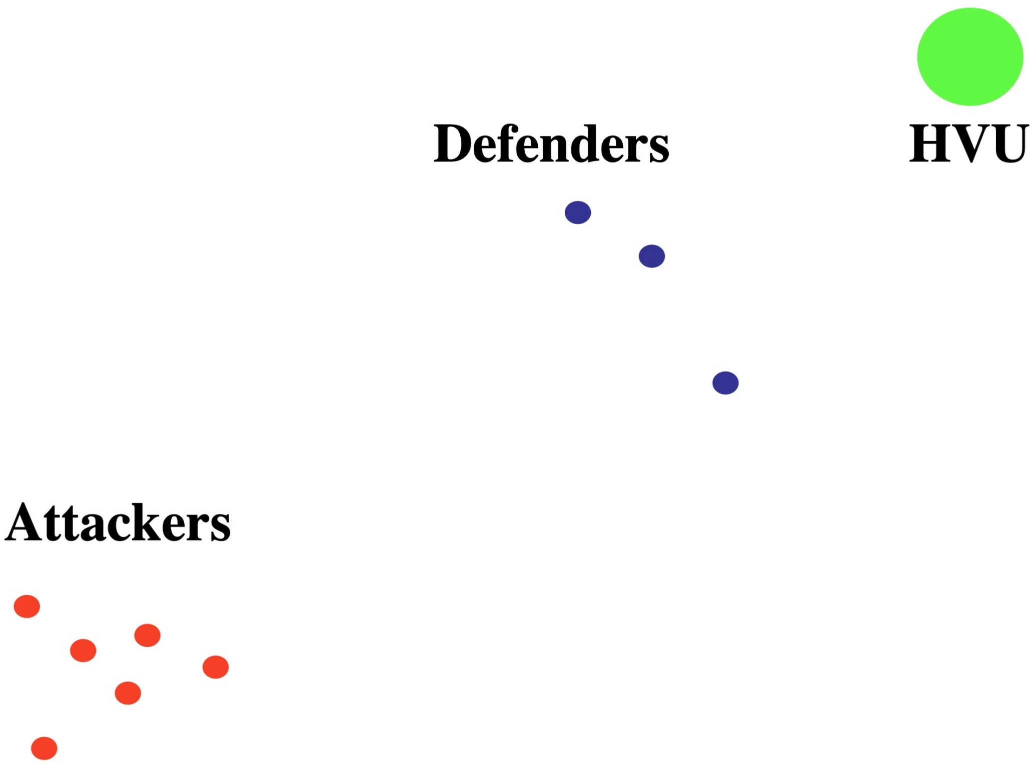

Figure 3.1. Standard Simulation. The initial positions of a standard swarm engagement simulation.

Individual drone dynamics are modeled using an Euler-based dynamic agent model where each defender drone's acceleration is determined by

$$m_i \ddot{\mathbf{r}}_i = K \frac{\mathbf{R}_i^{\text{targ}} - \mathbf{r}_i}{|\mathbf{R}_i^{\text{targ}} - \mathbf{r}_i|} - B\dot{\mathbf{r}}_i \tag{3.1}$$

where the individual defender drone acceleration $\ddot{\mathbf{r}}_i$ is a function of the drone mass m_i, an acceleration coefficient K, the effective target position $\mathbf{R}_i^{\text{targ}}$, the current defender position $\mathbf{r}_i$, the defender drag coefficient B, and the current defender velocity $\dot{\mathbf{r}}_i$. Therefore, the defender accelerates in the direction of the effective target position, which varies based on the specific targeting algorithm.

The terms of Equation (3.1) can be expressed as

$$v = K/B \tag{3.2}$$

$$t_a = m/B \tag{3.3}$$

where a defender maximum velocity v is function of the acceleration coefficient K and the defender drag coefficient B. The defender acceleration time constant t_a is a function of the defender mass m and the defender drag coefficient B. The defender maximum velocity and the acceleration time constant will be varied for the analysis in follow-on chapters.

3.2 Targeting Methods

The behavior of the defender drones is determined by the Greedy, Smart, and Intercept algorithms. These algorithms are simply different ways to set $\mathbf{R}_i^{\text{targ}}$, as described below.

3.2.1 Greedy

The Greedy algorithmic process is shown in Figure 3.2 which is consistent with Equation (3.1). Since drones using Greedy accelerate directly toward the attacking drone, the effective target position is located at the current target position. Therefore, drones using Greedy tend to place themselves in tail-chases of the attacking drone.

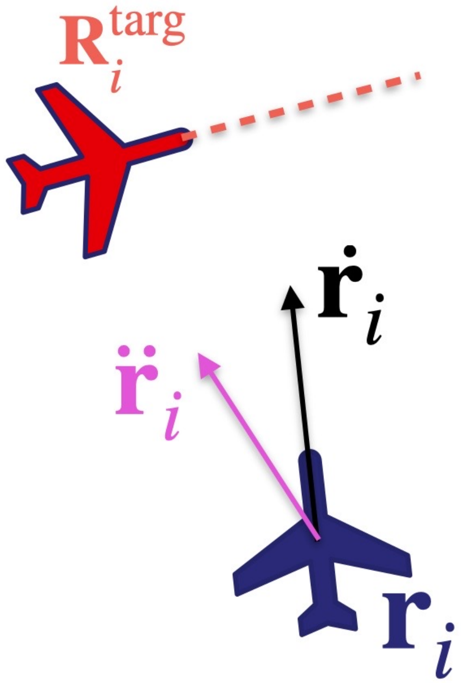

Figure 3.2. Greedy Diagram. Greedy causes defenders to accelerate directly toward the target drone.

Greedy targeting is also shown in Figure 3.3. Each defender targets the closest attacker, shown with a blue line. Attacker velocities, shown with a red line, are also plotted. Due to each defender attacking the closest attacker, multiple defenders can target the same attacker.

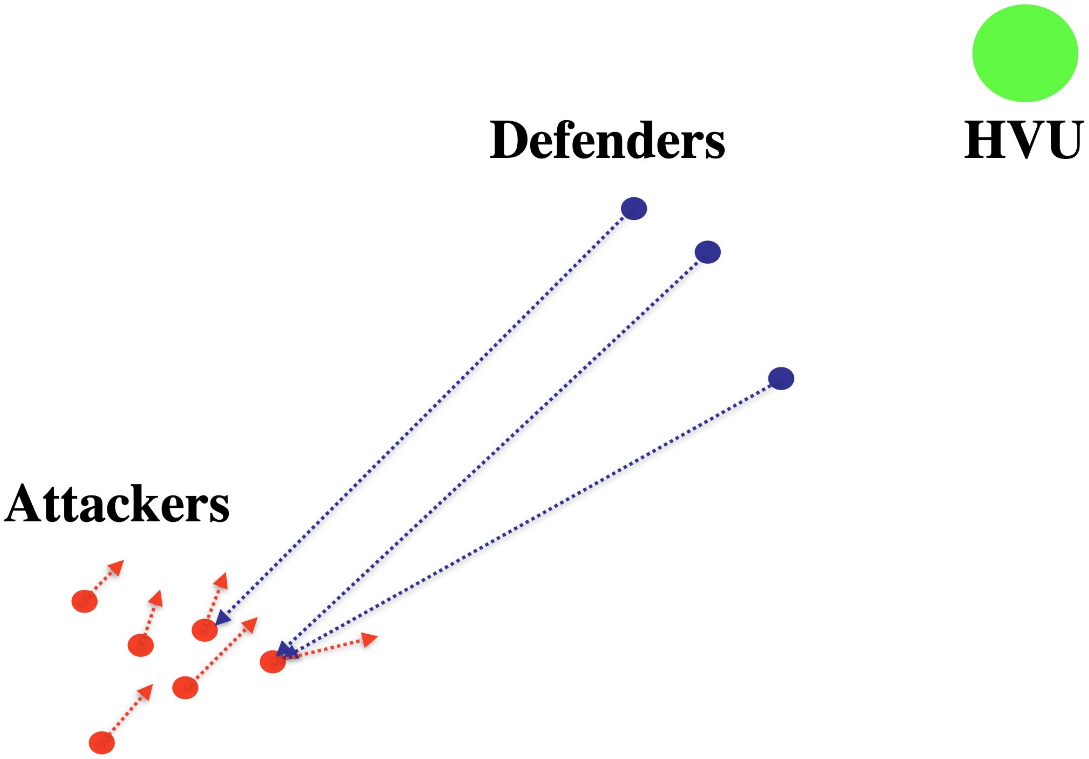

Figure 3.3. Greedy Targeting. Defenders target the closest attacker and accelerate directly toward the current attacker position.

3.2.2 Smart

The Smart algorithmic process is similar to Greedy except drones allocate targets so that targets are distributed among defender drones. Every simulation time step, the distance between each defender and attacker is assessed. The shortest defender-attacker combination is then assigned to the respective defender and both that attacker and defender are removed from the targeting queue. This is performed iteratively until every defender is assigned an attacker. For cases with more defenders than attackers, this process is performed until every attacker has an assigned defender. At this point, every remaining defender is assigned to the closest attacker. Upon selecting a target, Smart performs mechanically identically to Greedy. Therefore, Smart drones also tend to be in tail-chases with attacking drones.

Smart targeting is shown in Figure 3.4. By distributing defenders, each defender targets a different attacker. Therefore, Smart, unlike Greedy, does not cause defenders to congregate on a single attacker. The defenders, however, accelerate directly toward the current position of their respective attacker every time step.

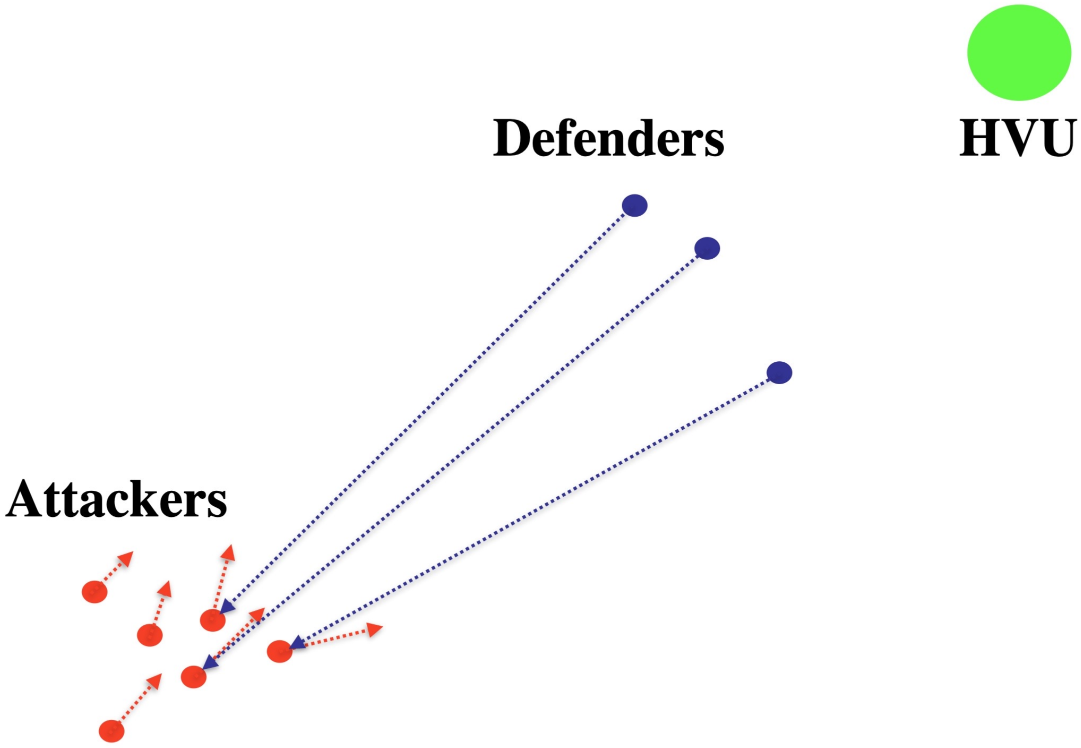

Figure 3.4. Smart Targeting. Defenders queue and distribute targets then accelerate directly toward the current attacker position.

3.2.3 Intercept

The Intercept algorithmic process is shown in Figure 3.2. The effective target position is the calculated intercept point. Every time step, defender-attacker pairs are allocated based on current distances between drones, similar to Smart. The intercept point is then calculated for each pair. The intercept point is calculated every time step by solving a second-order dynamics equation where the attacker and defender current positions and velocities are known and the final positions are unknown. Defenders then accelerate toward the calculated intercept point. Intercept drones efficiently fly to attacking drones and do not place themselves into tail-chases.

A version of Intercept where the intercept point for every defender-attacker pair is calculated and the closest intercept points is assigned to each defender was also evaluated. This process was, however, computationally intensive and yielded similar results to the final Intercept algorithm.

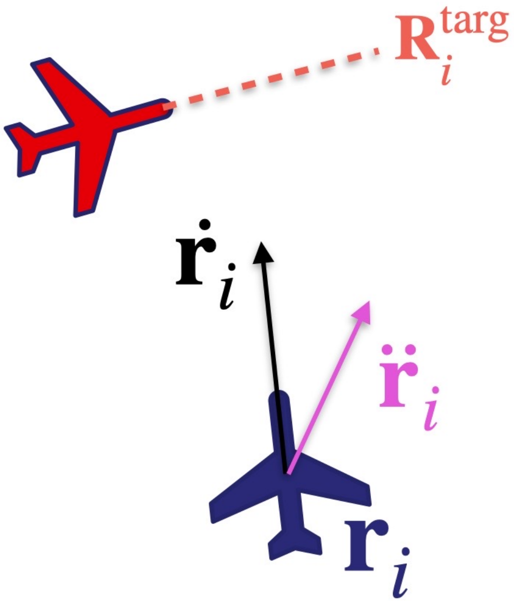

Figure 3.5. Intercept Diagram. Intercept causes defenders to accelerate toward a calculated intercept point with the target drone.

Intercept targeting is shown in Figure 3.6. Intercept distributes defenders similarly to Smart, however Intercept also calculates and accelerates toward an intercept point with each respective attacker.

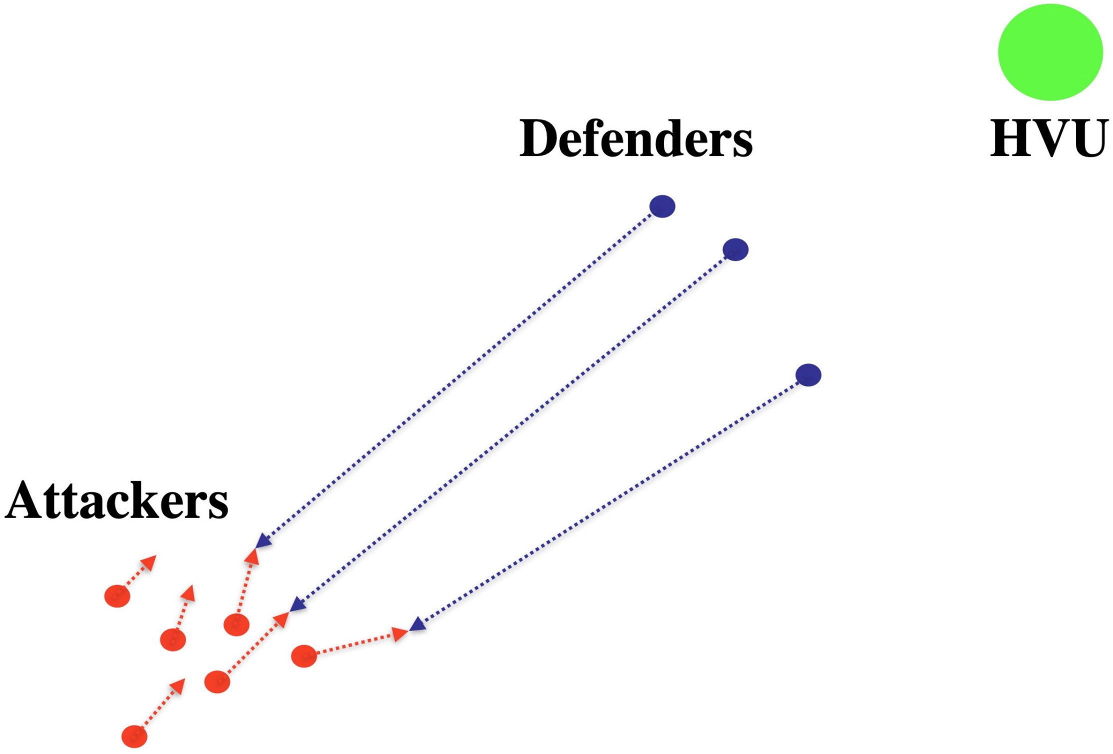

Figure 3.6. Intercept Targeting. Defenders queue and distribute targets then calculate and fly to intercept points.

3.3 Parameter Variation

In each simulation the two swarms are generated with preset parameters. The attacking drones are given a specified swarm size and maximum velocity, which dictates the distance they can move per time step. The defending drones are given a specific swarm size, weapon range, maximum velocity, and characteristic acceleration time. For each simulation, these parameters are varied across a range of values and each set of parameters is run a total of 120 times. In each of these 120 simulations, a random seed is used to vary the initial positions of the attackers and defenders. This allows slightly different variations of each parameter set to be simulated.

Attackers are marked as destroyed if their distance from a defender is within the defender weapon range. Destruction of the attacker causes the respective attacker drone to be removed from the simulation. Attackers are not able to destroy defenders and defenders do not experience attrition.

3.4 Recorded Data

The number of time increments to destroy all attackers is recorded for each individual run and averaged across the 120 cases per simulation. The amount of time to destroy each attacker is then compared to the variation in each respective parameter. The relative weight and effect of each parameter change then allows the development of a swarm effectiveness function and a quantified expression for determining whether the defender swarm would succeed or fail.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4:
Results: Swarm Modeling

Determining drone swarm trade-off analysis requires modeling an engagement between an offensive and defensive drone swarm. The ultimate objective of this analysis is to determine which swarm parameters most efficiently contribute to overall swarm fitness.

4.1 Algorithm Performance

4.1.1 Greedy

The performance of Greedy is evaluated in four successive snapshots in Figure 4.1. The initial positions of the defenders, in blue, and the attackers, in red, are shown in Figure 4.1.(a). At this point, each defender determines the closest attacker and flies a direct course toward that attacker.

By Figure 4.1.(b), the defenders have reached the attacking swarm. Due to multiple defenders targeting the same attacker, the defenders are closely spaced and in poor position for follow-on pursuit of the remaining attackers. In Figure 4.1.(c), the defenders continue pursuit however they have already been bypassed by some of the attackers. In Figure 4.1.(d), the defenders are in a tail-chase pursuit of the attackers, which have completely bypassed the defenders and now threaten the HVU.

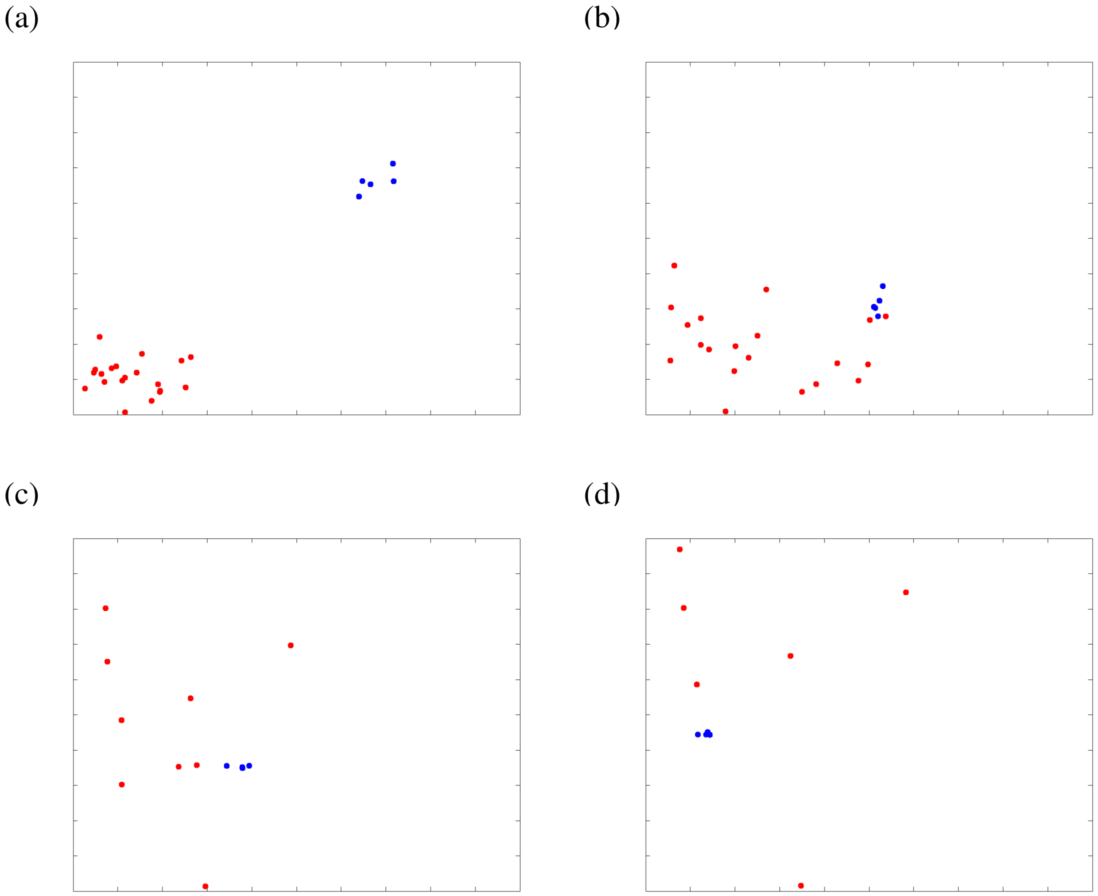

Figure 4.1. Greedy Demonstration. Attackers bypass defenders due to defender bunching.

The performance of Greedy demonstrates its inherent weaknesses as a targeting algorithm. By directly pursuing the closest attacker, the defender swarm is ineffective in efficiently destroying the attacking swarm. Instead, the defenders bunch together and allow a sufficiently distributed attacking swarm to bypass the congregated defender swarm. Therefore, targeting behavior which distributes and coordinates group behaviors is needed.

4.1.2 Global Targeting

Global Targeting, which includes the Smart and Intercept algorithms, can distribute targeting between swarm members as shown in Figure 4.2. Each defender targets the closest attacking drone that is not already targeted by another defender. This, therefore, avoids the defender bunching caused by Greedy.

In Figure 4.2.(a), the attackers and defenders are generated and each defender determines its target based on proximity to each attacker. In Figure 4.2.(b), the two swarms first encounter each other. By Figure 4.2.(c), the defenders have largely surrounded the attackers and destroyed most of the swarm. In Figure 4.2.(d), the attacker swarm is nearly completely destroyed with only a few remaining attackers that pose minimal risk to the HVU. This highlights the advantages of Global Targeting. The defensive drone swarm is more efficient at targeting the attacking swarm and avoids the defenders bunching.

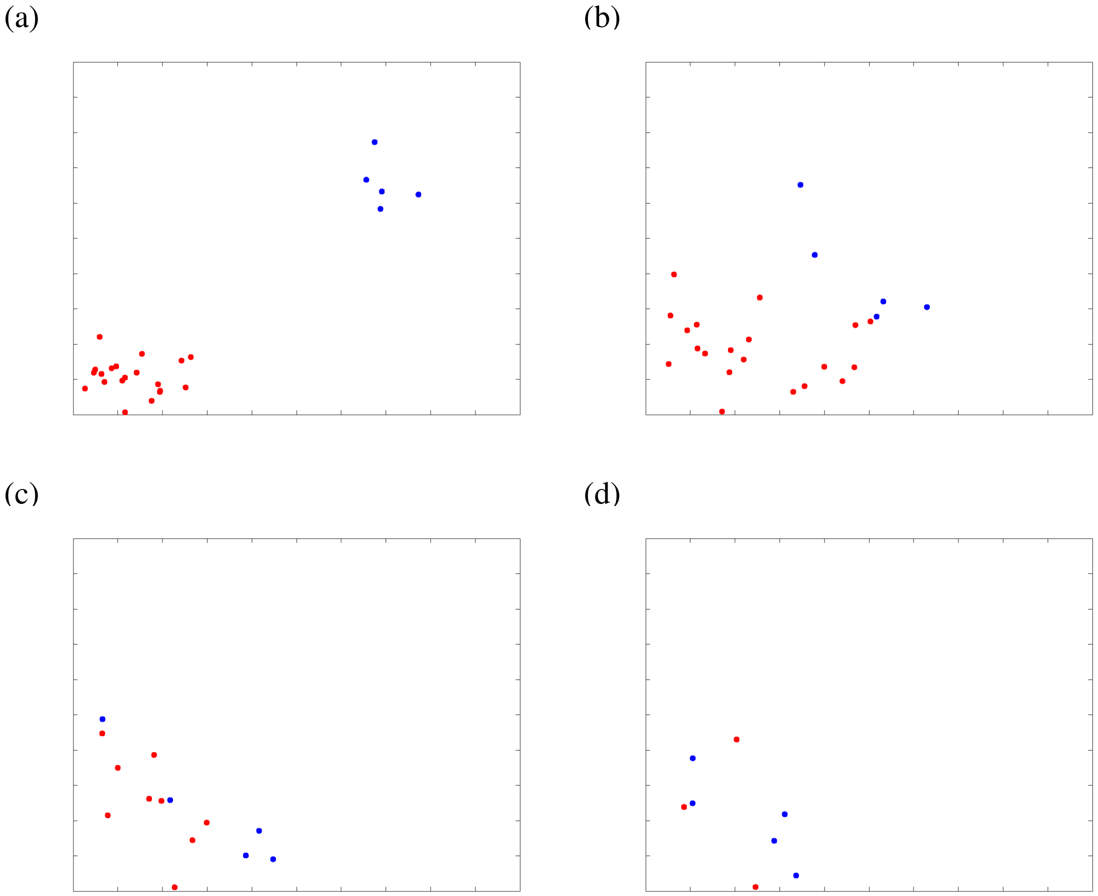

Figure 4.2. Global Targeting Demonstration. Defenders distribute targets, which allows for more efficient targeting.

4.2 Swarm Performance

Swarm performance can be determined by the ability of the defensive swarm to expeditiously destroy the attacking swarm. Quickly destroying the attacking swarm minimizes the possibility of attackers evading defenders, closing distance with the HVU, and ultimately placing the HVU at risk. Swarm performance can be characterized as a strong defender win, weak defender win, and an attacker win. Due to the aforementioned success of Global Targeting algorithms, this analysis is performed with the Intercept algorithm.

4.2.1 Strong Defender Win

The strong defender win case is shown in Figure 4.3. First, the attackers and defenders are generated and defenders determine their targets, as shown in Figure 4.3.(a). By Figure 4.3.(b), the swarms first encounter each other. By Figure 4.3.(c), the defenders have destroyed much of the attacking swarm. The defender swarm is sufficiently large and capable to avoid being overwhelmed by attackers. In Figure 4.3.(d), the defenders have nearly completely destroyed the attackers, which are unable to evade the defenders or place the HVU at risk.

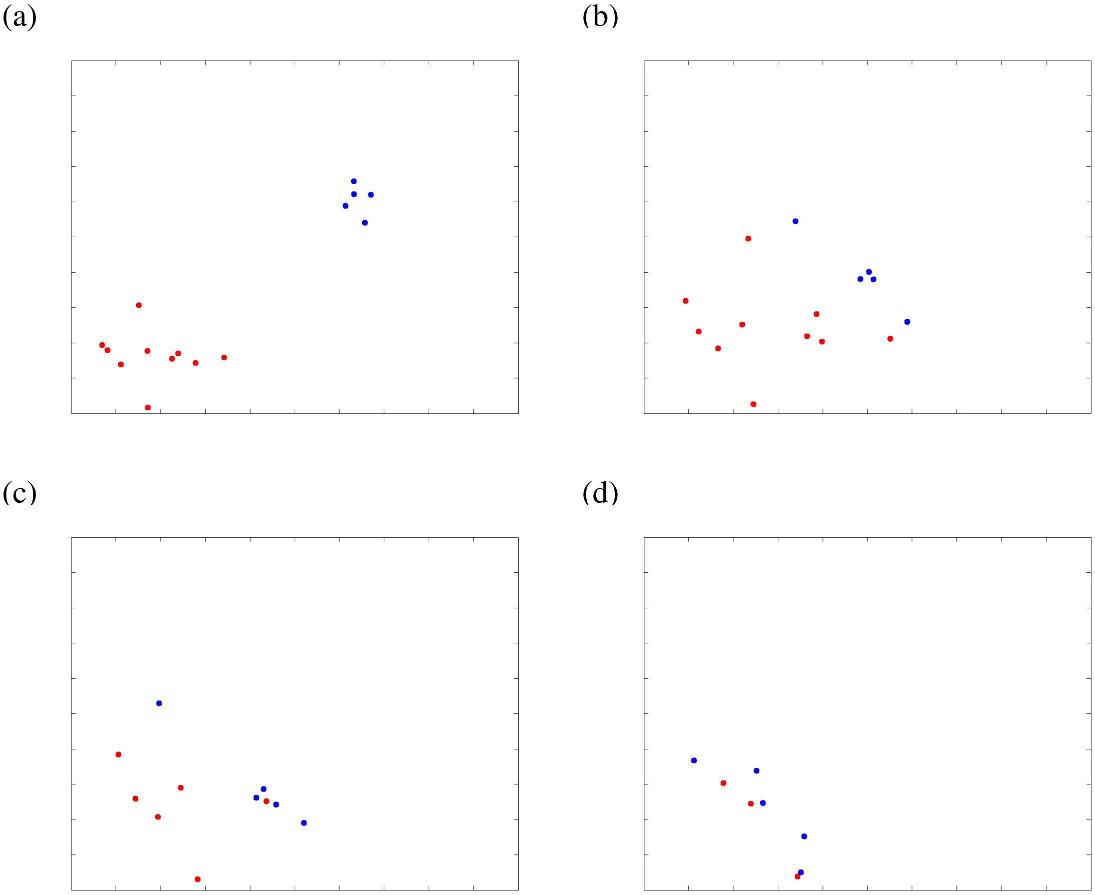

Figure 4.3. Strong Defender Win. Defenders overwhelm and easily destroy attackers before attackers are able to sufficiently close range to HVU.

In this case, the defender swarm is quickly able to destroy the incoming attacker swarm. Therefore, the attackers are unable to bypass the defenders and the HVU incurs minimal risk. The likelihood of an engagement ending in a strong defender win is a combination of the relative sizes of the swarms and the individual capabilities of each swarm member. Large defender swarms, small attacker swarms, and highly effective individual defenders combine to increase the probability of a strong defender win.

4.2.2 Weak Defender Win

The weak defender win case is shown in Figure 4.4. After being generated in Figure 4.4.(a), the swarms start the engagement in Figure 4.4.(b). By Figure 4.4.(c), the attackers have started to bypass a portion of the defending swarm. However, by Figure 4.4.(d) the defenders have recovered and successfully contain the attackers, minimizing the risk to the HVU.

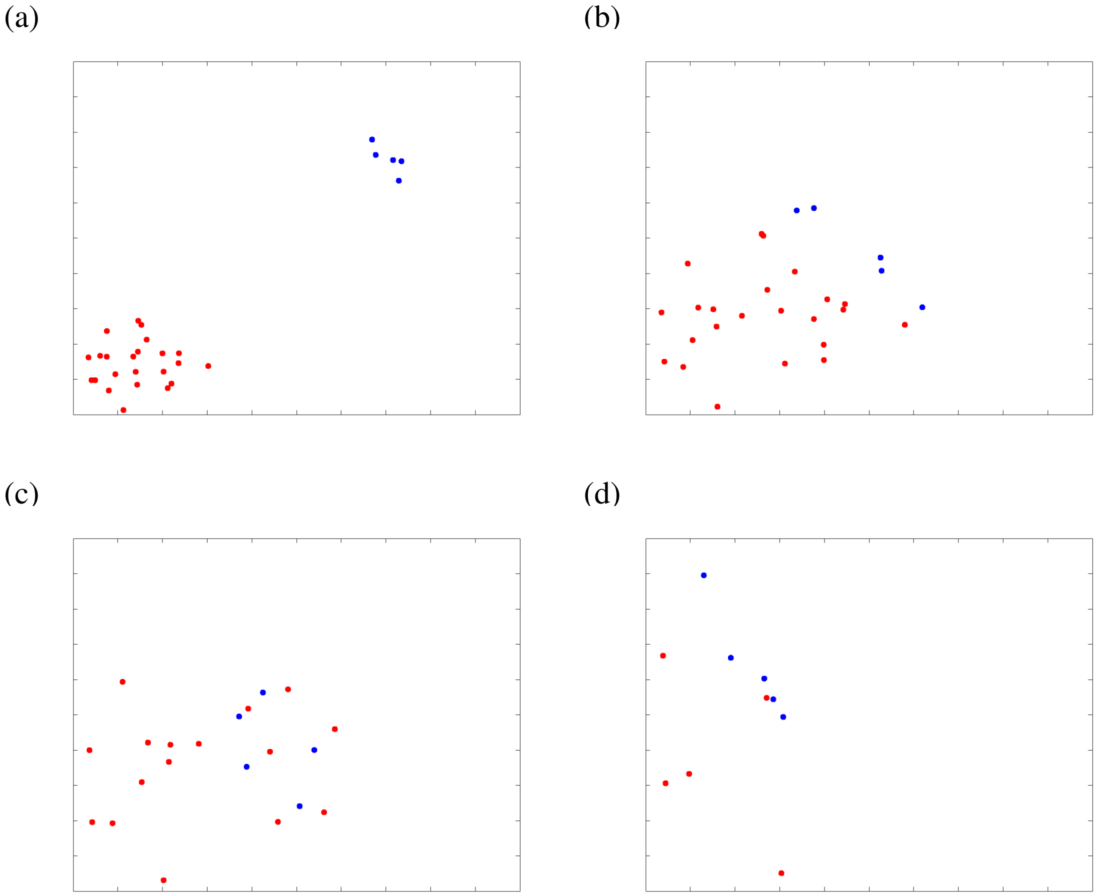

Figure 4.4. Weak Defender Win. Defenders destroy attackers and some attackers temporarily bypass the defenders. The defenders ultimately prevail despite the HVU being in some risk.

In this case, the attackers are able to place the HVU in more risk than in the strong defender win. However, the defenders are ultimately able to contain and destroy the attackers. This win case features a defending swarm which is large and capable enough to ultimately provide sufficient defense but neither large nor capable enough to completely overwhelm the attackers.

4.2.3 Attacker Win

The attacker win case is shown in Figure 4.5. After being generated in Figure 4.5.(a), the swarms start the engagement in Figure 4.5.(b). Despite being spread out, the defenders are overwhelmed by Figure 4.5.(c). At this time, attackers advance through the significant gaps in the defense. By Figure 4.5.(d), the attackers have pushed the defenders back to the depth of their starting position.

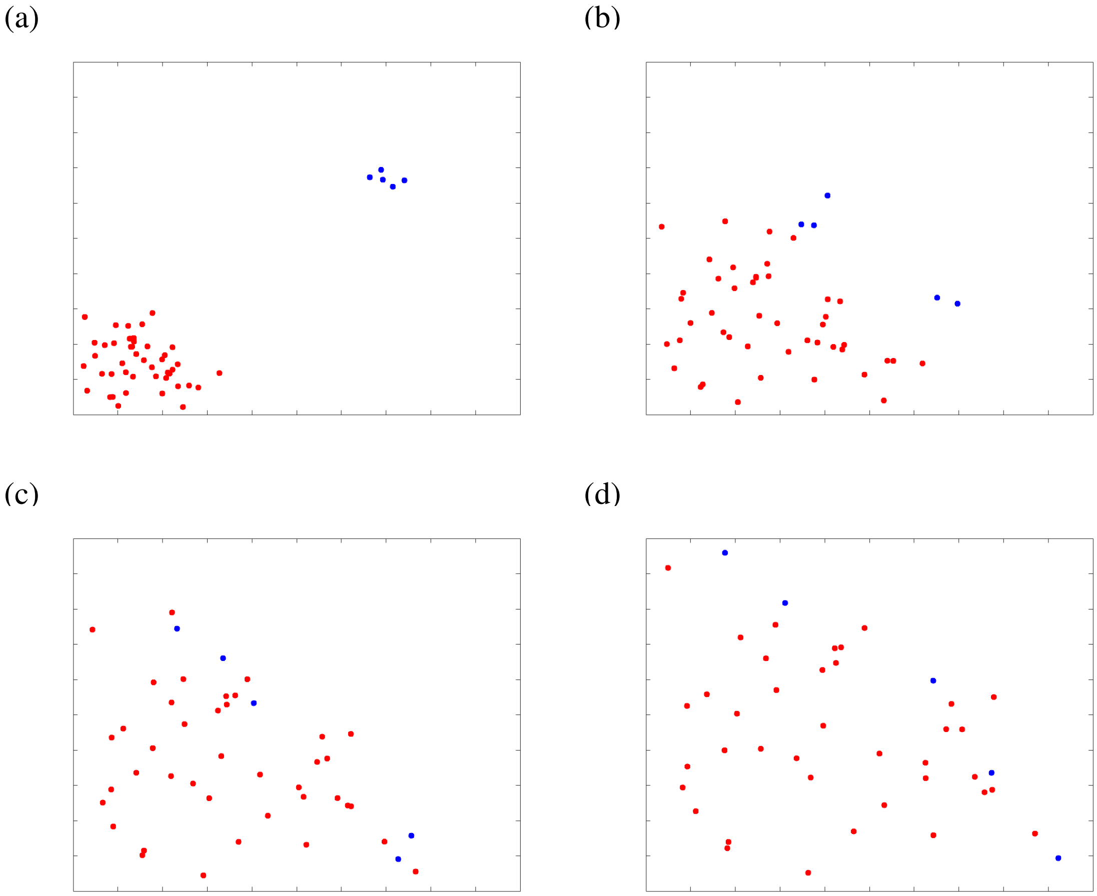

Figure 4.5. Attacker Win. Attackers overwhelm and bypass defenders and place the HVU at significant risk.

The attackers are able to quickly overwhelm and bypass the defender swarm. Though the defender swarm is able to somewhat attrit the attacker swarm, the majority of the attackers are able to advance despite the defenders. The defenders are ultimately pushed back to their initial location and the HVU is at significant risk. This condition occurs due to the relative size disparity between the attacking and defending swarm as well as defenders not being individually capable enough to offset this size difference.

4.2.4 Algorithm Comparison

The time for each targeting algorithm to destroy the attacking swarm as a function of number of attackers is shown in Figure 4.6 for the Greedy, Smart, and Intercept cases. For Intercept, this data is plotted for defender drones having both a high and low turn rate. This confirms the analysis from SASC, notably that Greedy is the lowest performing of the algorithms with a significant performance increase for Smart and Intercept, which both feature Global Targeting. For this reason, the Intercept algorithm is selected as the defender algorithm for all future analysis and results. The performance differences between high and low turn rate defenders also demonstrates that defender parameters have an influence on defender swarm performance.

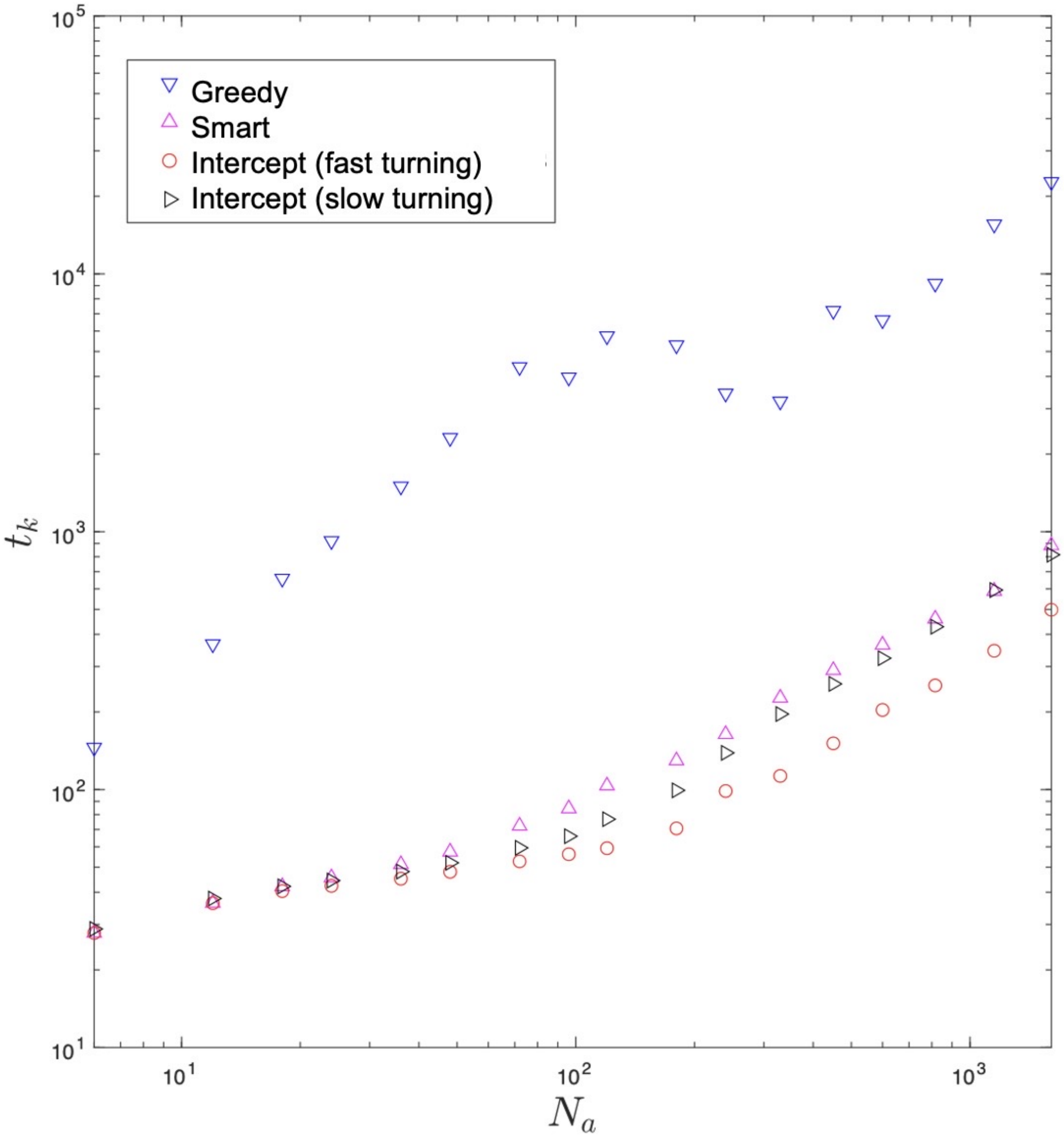

Figure 4.6. Algorithm Performance Comparison. Global targeting algorithms significantly outperform Greedy however Intercept slightly outperforms Smart. Intercept with fast turning also slightly outperforms Intercept with slow turning.

4.3 Effect of Varying Parameters

The time to destroy the attacking swarm as a function of number of attackers is shown in Figure 4.7 for defending swarms with varying parameters. The defender parameters that can be varied are the number of defenders N_d, the weapon range R, the characteristic acceleration time t_a, and the velocity v. In this case, all parameters except the characteristic acceleration time are varied.

As the parameters of the defenders change, the time to destroy the attackers also changes. Despite these changes, the overall shape of the curves stays largely the same. This suggests that the overall behavior of the swarm remains constant despite changes in defender or attacker performance. While the time to destroy an attacking swarm changes with parameters, these parameters do not affect the overall swarm behavior. Therefore, the time to destroy the attackers can be determined as a function of the selected defender parameters.

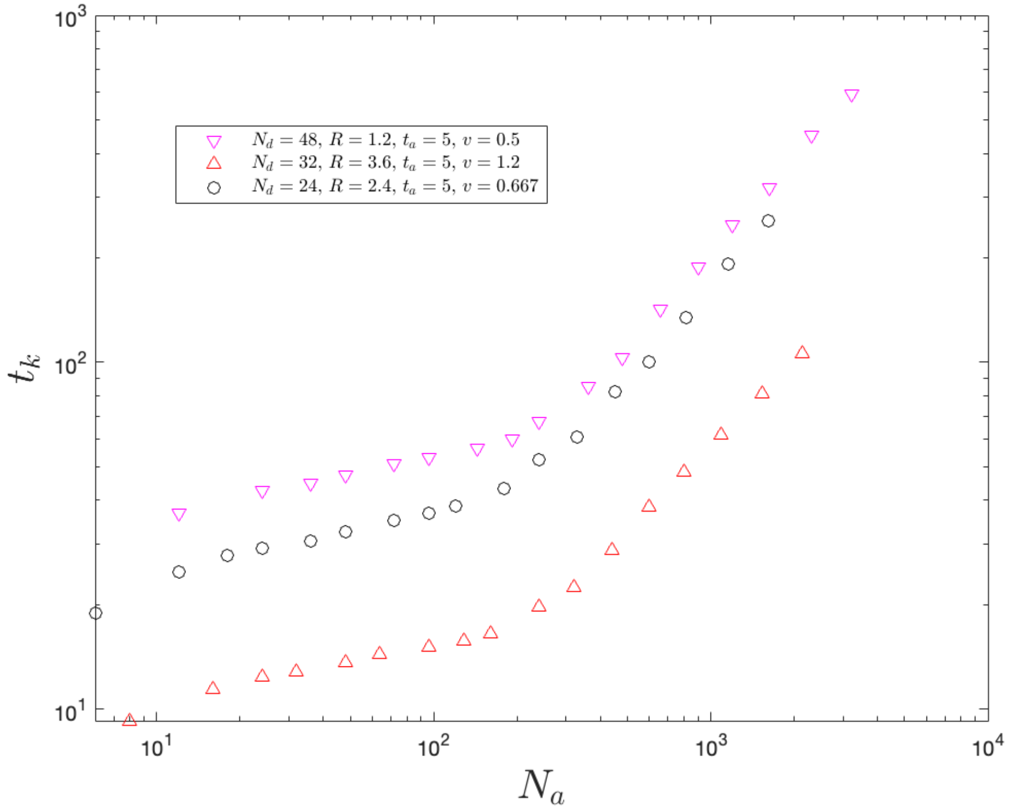

Figure 4.7. Behavior Consistency. The overall swarm behavior does not change despite differences in swarm composition and parameter choice.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5:
Results: Scaling Analysis

Due to the similarities in swarm behavior across varying swarm composition, the effectiveness of the swarm can be scaled to predict performance given a specific swarm make-up. This analysis, however, requires creating dimensionless swarm parameters.

5.1 Buckingham π

The Buckingham π theorem states that any physical system can be fully characterized by p dimensionless parameters π_i (where i runs from 1 to p), where

$$p = n - k. \tag{5.1}$$

here, n is the number of system variables, and k the number of dimensions (usually three: mass, length, and time). There then exists a constraint function that determines any π_i in terms of all the others. For example,

$$\pi_1 = f(\pi_2, \pi_3, ..., \pi_p). \tag{5.2}$$

5.1.1 Reynolds Number

An example of practical use of Buckingham π is in the dependence of the drag force on Reynolds Number (Re) in fluid mechanics [15]. If a sphere is moving through a viscous fluid at a specific velocity, there are $n = 5$ system variables: the diameter D, a velocity v, fluid density ρ, fluid viscosity ν, and a drag force F_D. These variables include mass, length, and time dimensions, so $k = 3$. Therefore, Equation (5.1) states that the system can be described by two dimensionless parameters,

$$\pi_1 = \frac{F_D}{\rho v^2 D^2} \tag{5.3}$$

$$\pi_2 = \frac{\rho v D}{\nu} = \text{Re} \tag{5.4}$$

thus, the drag force can be expressed as $F_D = \rho v^2 D^2 f(Re)$. This function f is equal to the drag coefficient (up to a geometrical prefactor), which only depends on Re.

5.1.2 Drone Swarm

The parameters in the drone swarm simulation include the time to destroy the attackers t_k, number of attackers N_a, number of defenders N_d, attacker velocity v_a, defender velocity v_d, defender characteristic acceleration time t_a, defender weapon range R, and the characteristic system length d for a total of $n = 8$. The system dimensions include length and time which can be described by

$$L^* = d, \tag{5.5}$$

$$T^* = \frac{d}{v}, \tag{5.6}$$

where the length dimension L^* and the time dimension T^* can be expressed using the characteristic system length d (the typical spacing between attackers) and the defender velocity v.

From Equation 5.1, the drone swarm system can be described using six dimensionless forms

$$\pi_1 = N_a \tag{5.7}$$

$$\pi_2 = N_d \tag{5.8}$$

$$\pi_3 = \frac{t_k v_d}{d} \tag{5.9}$$

$$\pi_4 = \frac{v_a}{v_d} \tag{5.10}$$

$$\pi_5 = \frac{t_d v_d}{d} \tag{5.11}$$

$$\pi_6 = \frac{R}{d} \tag{5.12}$$

These non-dimensional forms demonstrate the parameter combinations that can be used to determine a final functional form.

5.2 Swarm Effectiveness Functional Form

To begin the development of a functional form, and the interpretation of the swarm data, the results of Figure 4.7 are taken and the time to destroy the attacking swarm normalized by the number of attackers with this result is plotted in Figure 5.1.

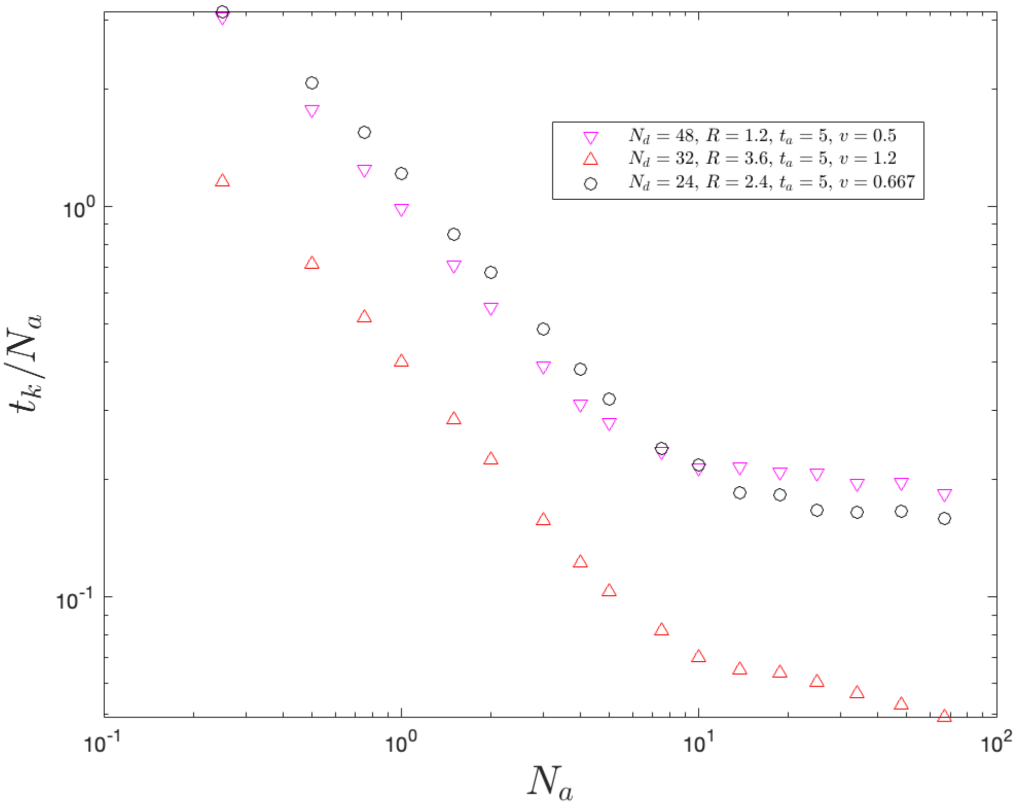

Figure 5.1. Attacker Normalized Data. Defender performance can be broken into two regimes, one with an algorithmic data and one without.

These results show that swarm success consists of two separate behavioral regimes. In the first, the time to destroy each attacker normalized by the number of attackers drops. In the second, this quantity plateaus. The first regime represents the cases where algorithmic advantages are present. In the second, performance increases diminish and the algorithmic advantage is significantly reduced. These two regimes fundamentally represent the cases in which the defending swarm succeeds and fails, respectively. This crossover point depends on defender and attacker swarm parameters, though every defender swarm eventually reaches this point of diminishing returns. By determining the crossover point, one can determine the effectiveness of a swarm based on given swarm parameters. A key question that mission planners should answer for this particular algorithm is how to stay in the first regime, where the defending force has an advantage.

5.2.1 Examining Swarm Data

The swarm parameters of the number of defenders, the weapon range, the characteristic acceleration time, and the velocity were varied to create over 1 million defender swarm simulations. The normalized time to destroy the attacking swarm is plotted as a function of number of attackers in Figure 5.2. These results again show that while the exact behavior of the defender swarm varies based on parameters, the overall curve shape stays relatively the same between different cases.

This justifies the previous assumption that changes in parameter values improve swarm fitness in the same way as increasing numbers of agents, but with different sensitivities. This motivates the definition of an effective number of defenders, $N_{d,\text{eff}}$, where a defender swarm is effective when $N_{d,\text{eff}} > N_a$ and ineffective when $N_{d,\text{eff}} < N_a$.

Plotting the data in this way should cause all curves to have crossovers from downward sloping to flat at the same value on the horizontal axis. Similarly, another scaled variable could be defined for the kill time per attacker, with a physical interpretation to be determined. Note that Buckingham π demands that there be a constraint function among all six dimensionless parameters. The similarity of the scaling functions suggests that a very simple form may be possible, where the behavior does not depend on each parameter independently but on a fixed combination which could collapse the data shown in Figure 5.2 into a single curve.

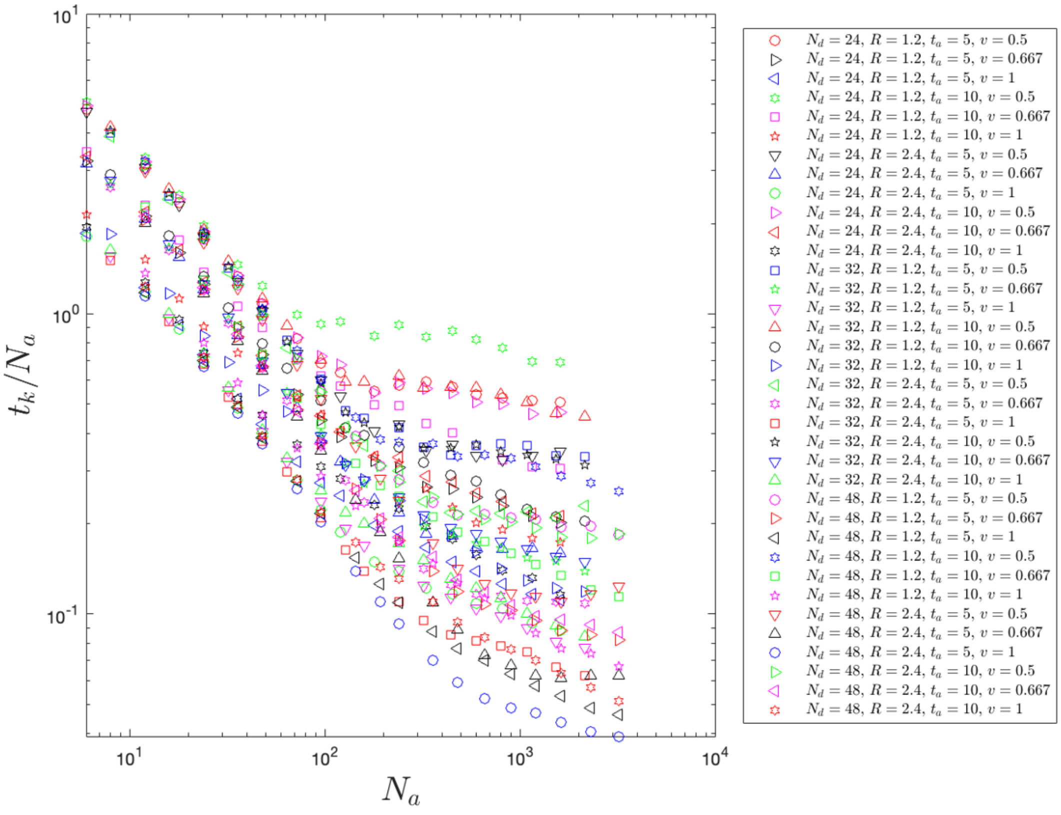

Figure 5.2. Swarm Parameter Variation. Defender swarm parameters are varied and the overall curve shape remains the same over the range of cases.

To determine whether the curve shapes would properly collapse, the position of the transition from the first to second regime was determined from each specific line shape by performing linear fits to the two branches in MATLAB and finding the intersection between the two lines. Using these calculated points, each individual curve is normalized and plotted in Figure 5.3. These results demonstrate that the swarm data can collapse on one curve. However, manually calculating the transition point yields no quantitative understanding of the data and merely serves to demonstrate the consistent line shape.

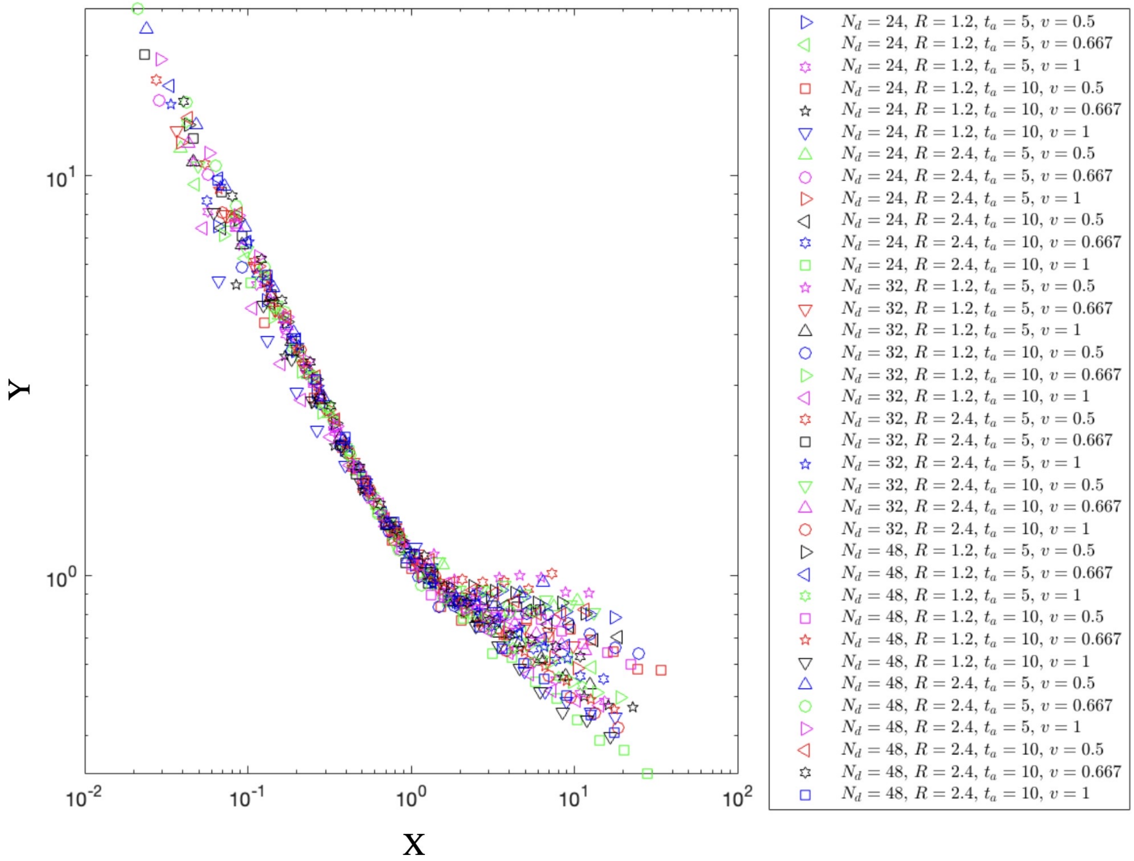

Figure 5.3. Manually Collapsed Curves. Curve points are manually calculated and each curve individually adjusted to allow collapse. This confirms the consistent curve shape over the range of cases.

5.2.2 Deriving the Functional Form

To determine functional forms, parameters were varied one at a time to determine the overall effect each parameter had on the overall swarm fitness. By iteratively changing each variable, scaling was used to satisfactorily collapse the data. This yields the functions

$$Y = \frac{d}{v} \tag{5.13}$$

$$X = \frac{N_a f(v, t_a)}{R {N_d}^{\frac{3}{2}}} \tag{5.14}$$

where Y is the scaled kill time and X is the scaled number of attackers N_a. The dependence on velocity and characteristic acceleration time can be approximately captured by

$$X = \frac{N_a e^{\frac{-4v}{5}} e^{\frac{t_a}{8}}}{R {N_d}^{\frac{3}{2}}} \tag{5.15}$$

The swarm is in regime one if $X < 1$ and the second regime when $X > 1$.

X can also be expressed as

$$X = \frac{N_a}{N_{d,\text{eff}}} \tag{5.16}$$

which is the ratio of the attackers to the effective number of defenders $N_{d,\text{eff}} = R {N_d}^{\frac{3}{2}} e^{\frac{4v}{5}} e^{\frac{-t_a}{8}}$. This result means that the defender swarm is effective when the number of defenders, scaled with defender parameters, exceeds the number of attackers.

The defender swarm effectiveness decreases linearly with the number of attackers, increases linearly with weapon range, increases non-linearly with number of defenders, and increases exponentially with higher acceleration and velocity. This relatively simple yet unintuitive result, containing different weighting factors and functional forms of each parameter, demonstrates the value of this method. Specifically, this form for $N_{d,\text{eff}}$ gives an explicit way to evaluate how improvements to the drone parameters correspond to changes in N_d (e.g., doubling N_d is better than doubling R, since N_d is raised to the power of 3/2).

These functional forms are then used to scale the results of Figure 5.2 as shown on Figure 5.4. This indicates a clear collapse of swarm behavior despite variation of drone parameters. Therefore, this result can be used to assess swarm success based on swarm composition and drone parameters.

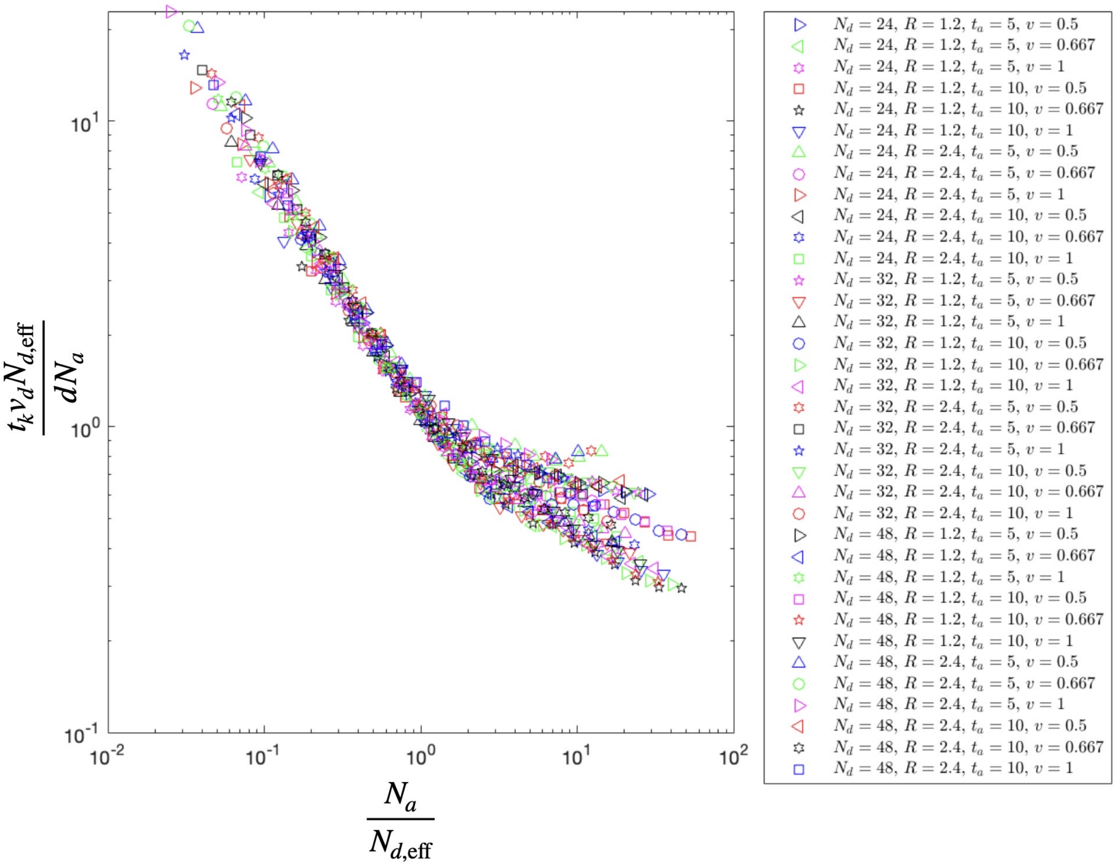

Figure 5.4. Functional Form Curve Collapse. The curve is collapsed using the generated functional forms.

5.3 Functional Form Evaluation

The creation of functional forms allows an assessment of swarm behavior given certain swarm characteristics and drone parameters.

5.3.1 Strong Defender Win Assessment

Swarm parameters are selected so $X < 1$, therefore it is expected this would fall in regime one and would result in a defender win. The results are shown on Figure 5.5. After being generated in Figure 5.5.(a), and the swarms colliding in Figure 5.5.(b), the defenders begin to overwhelm the attackers in Figure 5.5.(c). By Figure 5.5.(d) the defenders have completely overwhelmed and nearly destroyed the attacking swarm. Therefore, this predicted case matches the expectation of a strong defender win and supports the function validity in strong defender win cases.

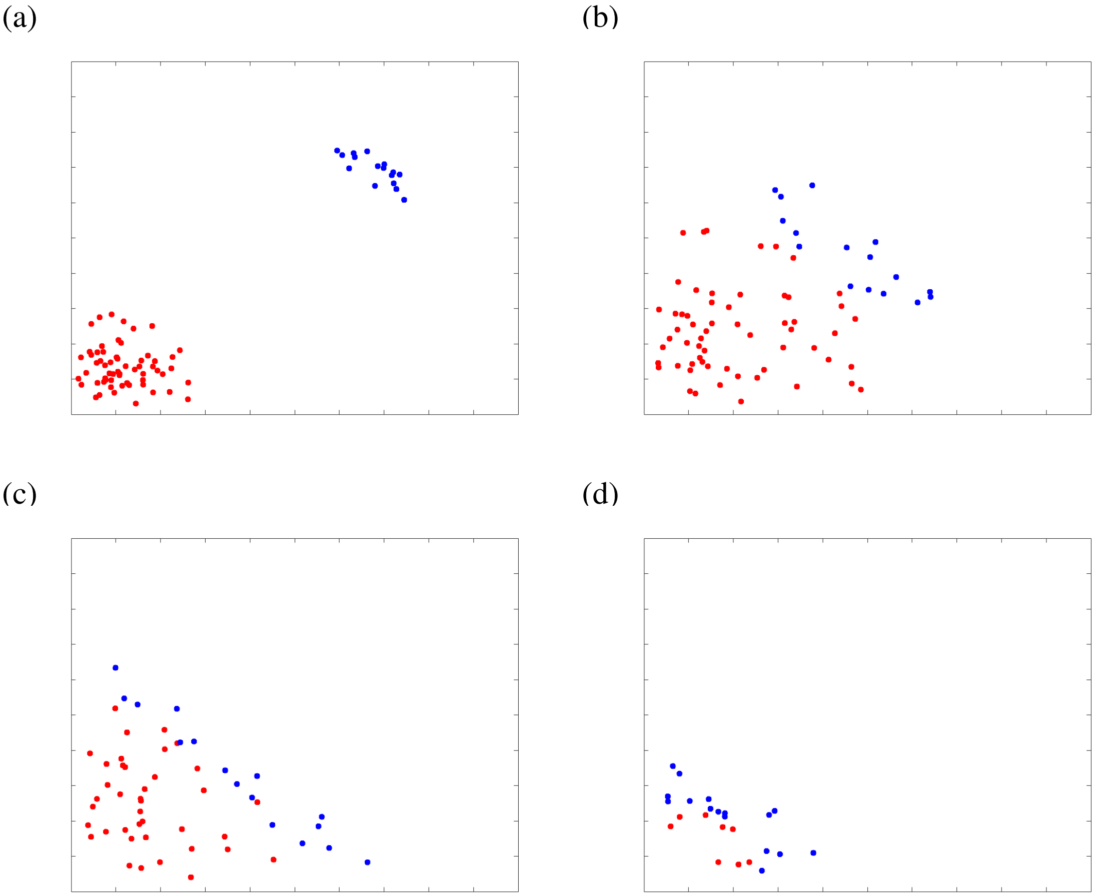

Figure 5.5. Predicted Strong Defender Win. Defenders overwhelm attackers and the HVU is not at risk.

5.3.2 Weak Defender Win Assessment

Swarm parameters are selected so $X = 1$ and results are shown on Figure 5.6. It is expected this would result in a weak defender win. After being generated in Figure 5.6.(a), and the swarms colliding in Figure 5.6.(b), the attackers have limited success evading the defenders in Figure 5.5.(c) with some attackers temporarily slipping past defenders. By Figure 5.5.(d), the defenders have surrounded and destroyed most of the attacking swarm. Despite the temporary setbacks, the defender swarm is ultimately successful and the HVU faces minimal risk. This result is consistent with the expectation of a weak defender win.

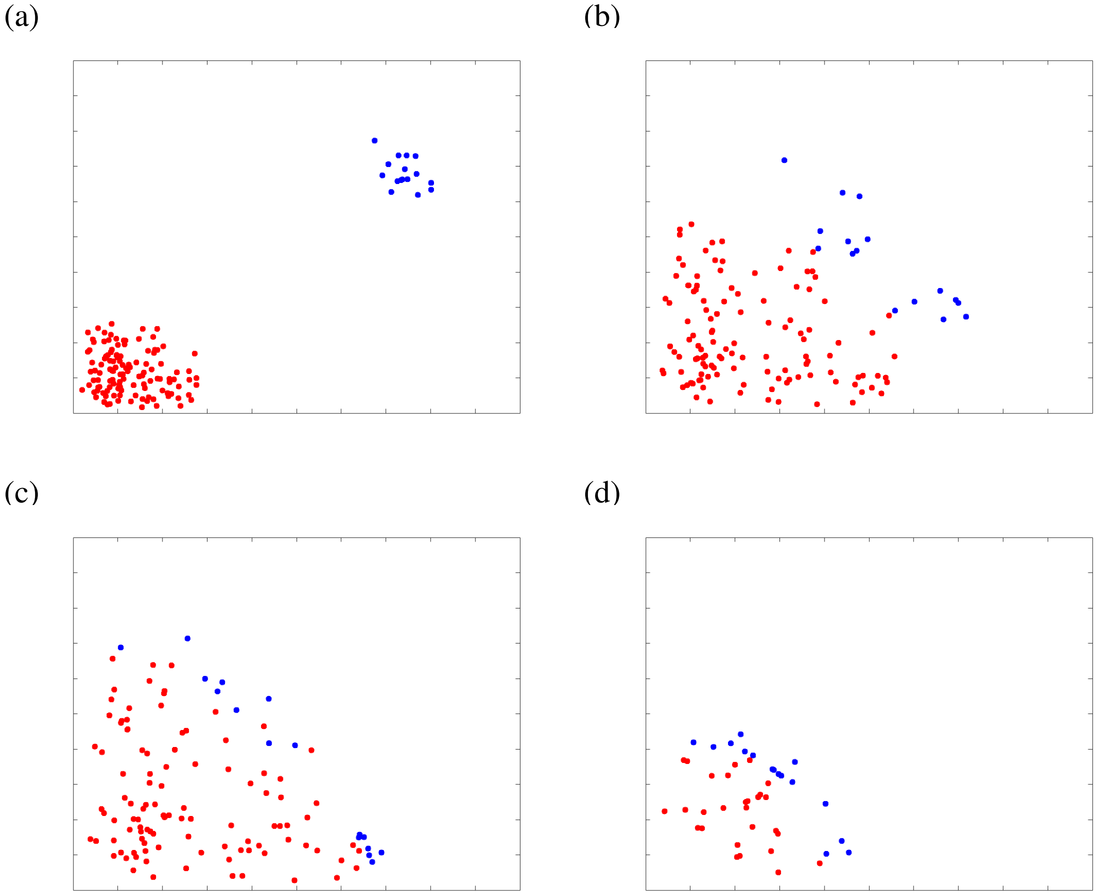

Figure 5.6. Predicted Weak Defender Win. Defenders ultimately destroy attackers with some attackers temporarily evading defenses. The HVU faces some risk.

5.3.3 Attacker Win Assessment

Swarm parameters are selected so $X > 1$ with results shown on Figure 5.5. It is expected this would result in a regime two attacker win. After being generated in Figure 5.5.(a), and the swarms colliding in Figure 5.5.(b), the attackers begin to overwhelm the defenders in

Figure 5.5.(c). Attackers quickly bypass defenders en-route to the HVU. By Figure 5.5.(d), the defenders have completely overwhelmed defenders and the HVU is at significant risk.

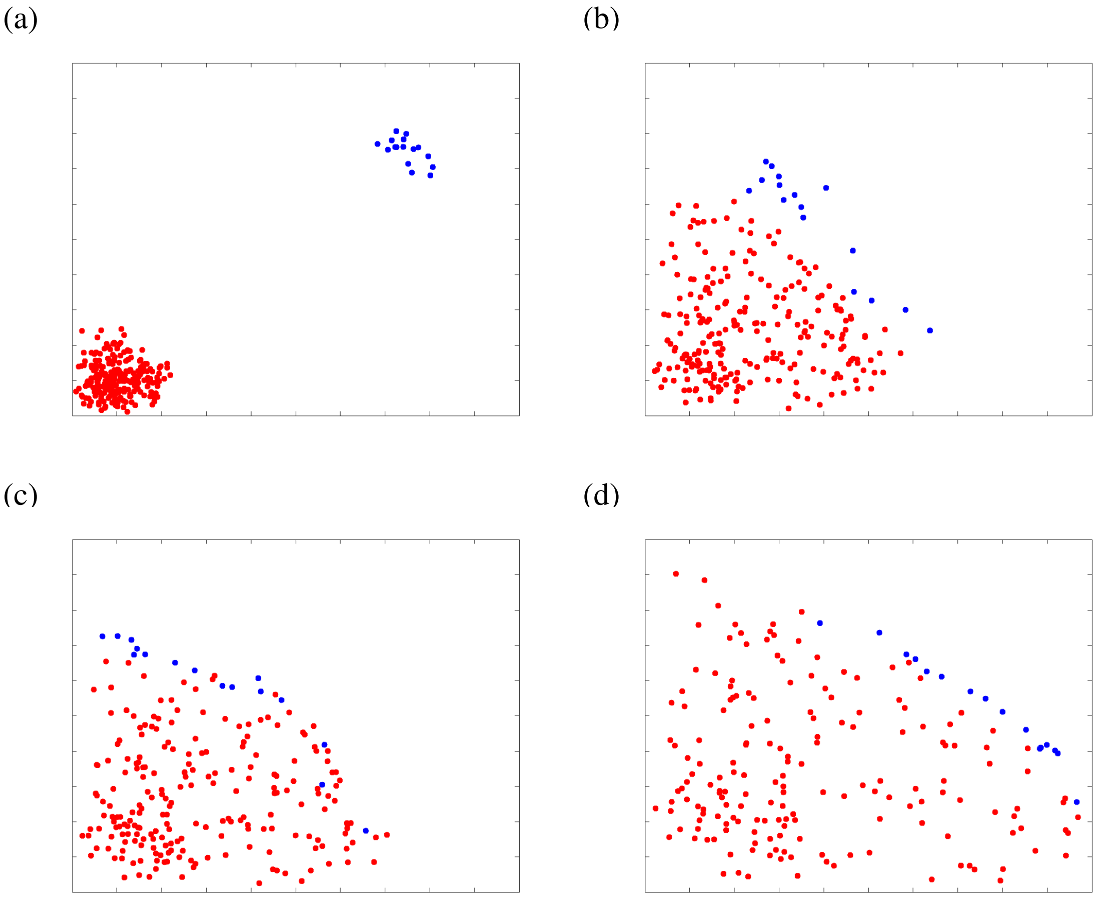

Figure 5.7. Predicted Attacker Win. Attackers overwhelm and bypass defenders which places the HVU at significant risk.

5.4 Use For Mission Planners

The swarm effectiveness function allows a mission planner to assess and certify that a potential swarm defense is sufficient and capable of defeating an adversarial drone swarm. Crucially, this analysis also allows mission planners, likely facing resource and material constraints, to ensure that a fielded drone swarm is not unnecessarily capable. Rather than relying on trial-and-error or expensive live-fly exercises, this method allows mission planners to expeditiously measure the relative effectiveness of various swarm compositions. Unintuitive relationships between the various weights and costs of changing parameters and swarm composition are also illuminated by this method.

CHAPTER 6:
Conclusion and Outlook

6.1 Conclusion

This thesis evaluated existing swarm algorithms to determine the effect of algorithm and parameter changes on swarm fitness. For changes in algorithm, the overall swarm behavior could change, such as between Greedy and Global Targeting, or the algorithm could cause incremental performance increases, such as between Smart and Intercept. Within an algorithm, the overall behavior remained largely the same and parameter changes strongly affected the fitness of the defending swarm. Therefore, functional forms were developed which combine swarm and individual swarm parameters to determine defender swarm success.

The swarm functional form is, therefore, a powerful tool which can be utilized by mission planners to assess and ensure the capability of defensive drone swarms. By quantifying drone swarm fitness, a mission planner is better able to ensure swarm performance is achieved. The functional form method can also be extended beyond the simple cases presented here to include drone swarms with an arbitrary number of parameters and with increasing levels of complexity. Fundamentally, any rule-based physical system can be reduced to a non-dimensional form which can be modeled using a similar methodology.

6.2 Outlook

Improvements of this method include increasing the number of drone parameters, the complexity of the simulation, and the sophistication of swarm behaviors. Adding an extra spatial dimension to model behaviors in three spatial dimensions could allow the creation of more advanced swarm behaviors though preliminary analysis of higher-order spatial simulations have not yielded significant differences in overall behavior.

More sophisticated defender behaviors can also be studied. For example, defenders attacking in waves may reduce the ability of attackers to get behind the defending force, helping to prevent inefficient tail-chases. Preliminary results from such a situation are shown in Figure

6.1. In these simulations, the first half of the defending force is released at the beginning of the simulation, and the second half is released when the first half begins engaging the attackers. The two-wave tactics are outperformed by simple intercept with low numbers of attackers, but a two-wave strategy outperforms intercept in high attacker cases. This supports that the second defender wave prevents the overall swarm from being bypassed and entering into tail-chases. The scaling behavior of crossover points could in principle be described using Buckingham π and scaling analysis.

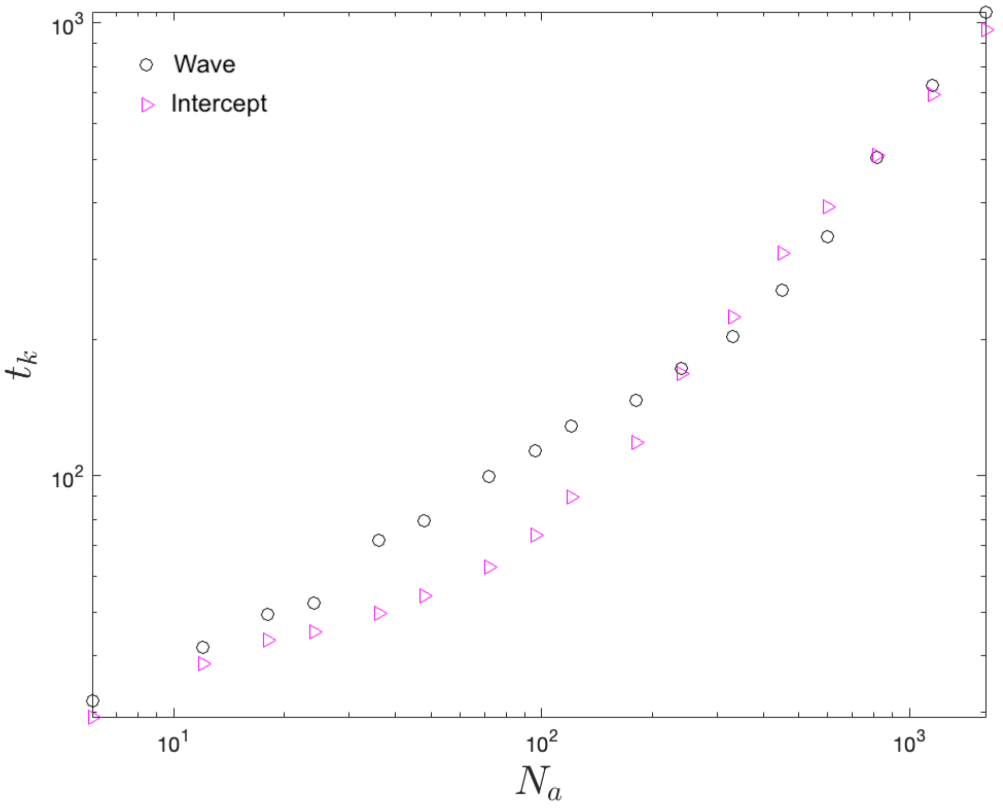

Figure 6.1. Defender Wave Tactic. The wave tactic outperforms intercept for high numbers of attackers, likely due to the defenders avoiding tail-chases.

Additional attacker behaviors might include attackers which actively or intelligently evade defenders (rather than simply scattering) or attack defenders. Snapshots from a preliminary simulation with intelligent attacker evasion behavior is shown in Figure 6.2. Here, the attackers pursue a virtual HVU located behind the defender swarm. The attackers also maintain both a minimum and maximum distance to fellow attackers to remain in a coherent swarm. When an attacker senses a defender in a preset range, the attacker changes behavior and begins to accelerate away from the incoming defenders. This situation is similar to the primary case study for this thesis (attacker scattering), but changes in the algorithm might yield small or large changes to the scaling functions.

In Figure 6.2.(a), the swarms are generated and they reach each other by Figure 6.2.(b). By Figure 6.2.(c), the defenders have flown into the attackers however the attackers begin to actively evade and fly around the defenders. In Figure 6.2.(d), two discrete groups of attackers have evaded the defenders and regrouped into a swarm which could imperil the HVU.

The ability of attackers to evade defenders and regroup into a swarm represents complex behavior which would affect defender effectiveness and the respective functional form.

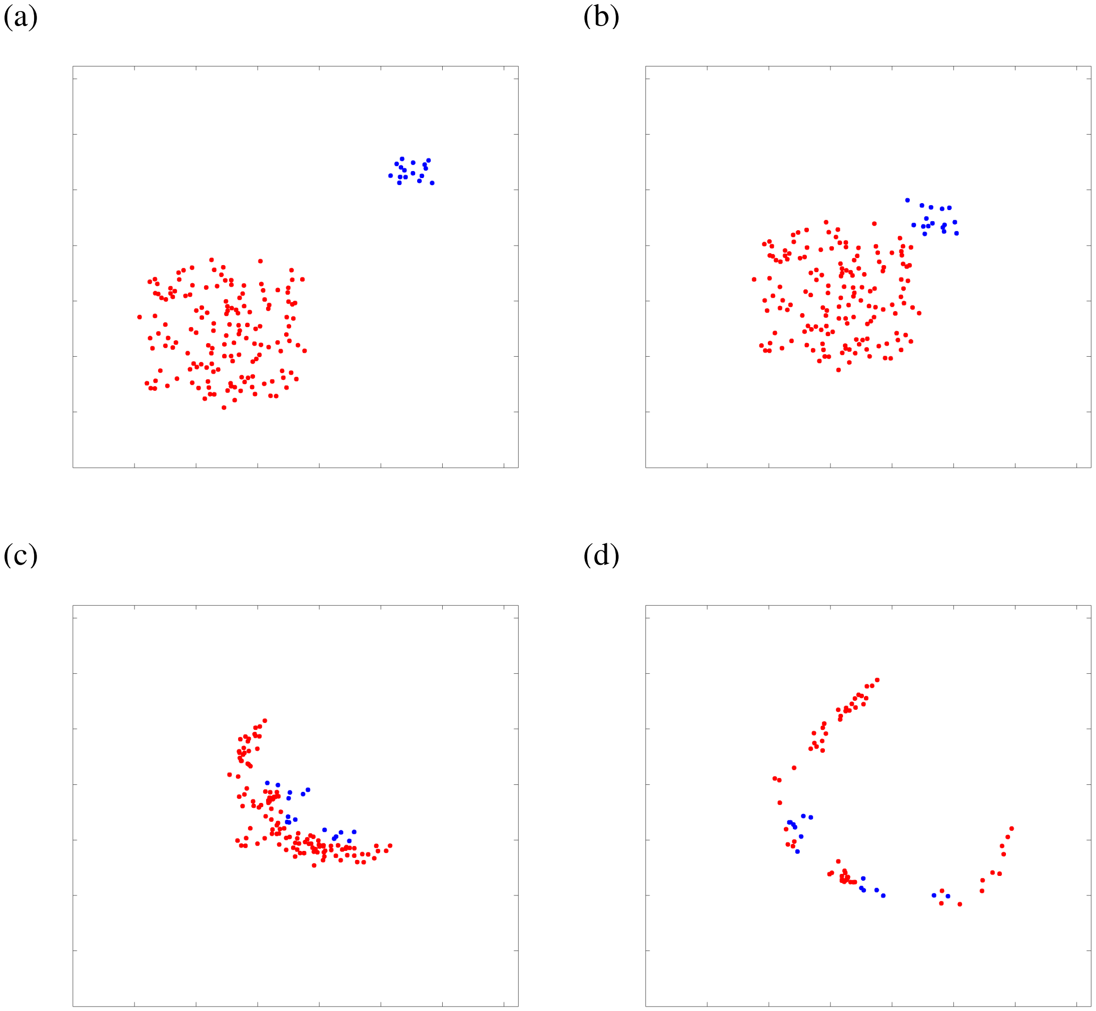

Figure 6.2. Attacker Evasion. Attackers bypass defenders and regroup after the initial encounter.

List of References

[1] Z. Kallenborn, *Are Drone Swarms Weapons of Mass Destruction?* U.S. Air Force Center for Strategic Deterrence Studies, Air University, Maxwell AFB, AL: U.S., 2020.

[2] T. Hamilton and D. Ochmanek, “Operating low-cost, reusable unmanned aerial vehicles in contested environments: preliminary evaluation of operational concepts,” RAND Project Air Force, Santa Monica, CA: U.S., Tech. Rep., 2020.

[3] Z. Kallenborn and P. C. Bleek, “Swarming destruction: drone swarms and chemical, biological, radiological, and nuclear weapons,” *The Nonproliferation Review*, vol. 25, no. 5-6, pp. 523–543, 2018.

[4] M. Mackin, “Ford-class aircraft carrier: Follow on ships need more frequent and accurate cost estimates to avoid pitfalls of lead ship,” Government Accountability Office, Washington DC: U.S., Tech. Rep., 2017.

[5] S. Kreps, “Democratizing harm: Artificial intelligence in the hands of nonstate actors,” *Brookings Institution, Washington, D.C.: U.S.*, Nov. 2021.

[6] J. D. Ellis, “Directed-energy weapons: Promise and prospects,” Center for a New American Security, Washington, D.C.: U.S., Tech. Rep., 2015. Available: http://www.jstor.org/stable/resrep06352

[7] S. J. A. Edwards, “Swarming and the future of warfare,” Ph.D. dissertation, Dept of Public Policy, Pardee RAND Graduate School, Santa Monica, CA: U.S., 2005.

[8] T. Tsatsanifos, A. H. Clark, C. Walton, I. Kaminer, and Q. Gong, “Modeling large-scale adversarial swarm engagements using optimal control,” in *2021 60th IEEE Conference on Decision and Control (CDC)*. IEEE, 2021, pp. 1244–1249.

[9] C. Walton, I. Kaminer, Q. Gong, A. H. Clark, and T. Tsatsanifos, “Defense against adversarial swarms with parameter uncertainty,” *Sensors*, vol. 22, no. 13, p. 4773, 2022.

[10] H. Park, Q. Gong, W. Kang, C. Walton, and I. Kaminer, “Observability analysis of an adversarial swarm’s cooperation strategy,” in *2018 IEEE 14th International Conference on Control and Automation (ICCA)*. IEEE, 2018, pp. 992–997.

[11] C. Walton, P. Lambrianides, I. Kaminer, J. Royset, and Q. Gong, “Optimal motion planning in rapid-fire combat situations with attacker uncertainty,” *Naval Research Logistics (NRL)*, vol. 65, no. 2, pp. 101–119, 2018.

[12] T. Tsatsanifos, "Computationally efficient algorithms for optimal motion planning against multi-domain super swarms," Ph.D. dissertation, Dept. of Physics, Monterey, CA; Naval Postgraduate School, 2020.

[13] T. Brick, M. Lanham, A. Kopeikin, C. Korpela, and R. Morales, "Zero to swarm: Integrating suas swarming into a multi-disciplinary engineering program," in *2018 International Conference on Unmanned Aircraft Systems (ICUAS)*, 2018, pp. 308–314.

[14] J. J. Dawkins, F. L. Crabbe, and D. Evangelista, "Deployment and flight operations of a large scale uas combat swarm: Results from darpa service academies swarm challenge," in *2018 International Conference on Unmanned Aircraft Systems (ICUAS)*, 2018, pp. 1271–1278.

[15] J. H. Williams, *Dimensional Analysis* (2053-2563). Bristol, United Kingdom: IOP Publishing, 2021. Available: https://dx.doi.org/10.1088/978-0-7503-3655-0

Initial Distribution List

1. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

2. Defense Technical Information Center
   Ft. Belvoir, Virginia