12-1-2023

Drone Swarms in Adversarial Environment

Bhavana Sai Yadav Akula
Southern Illinois University Carbondale, bhavanaakula11@gmail.com

DRONE SWARMS IN ADVERSARIAL ENVIRONMENTS

by

Bhavana Sai Yadav Akula

B.Tech., Jawaharlal Nehru Technological University, 2021

A Thesis
Submitted in Partial Fulfillment of the Requirements for the
Master of Science Degree

School of Computing
in the Graduate School
Southern Illinois University Carbondale
December 2023

THESIS APPROVAL

DRONE SWARMS IN ADVERSARIAL ENVIRONMENTS

by

Bhavana Sai Yadav Akula

A Thesis Submitted in Partial

Fulfillment of the Requirements

for the Degree of

Master of Science

in the field of Computer Science

Approved by:

Dr. Henry Hexmoor, Chair

Dr. Bidyut Gupta

Dr. Koushik Sinha

Graduate School
Southern Illinois University Carbondale
November 3, 2023

AN ABSTRACT OF THE THESIS OF

Bhavana Sai Yadav Akula, for the Master of Science degree in Computer Science, presented on November 3, 2023, at Southern Illinois University Carbondale.

TITLE: DRONE SWARMS IN ADVERSARIAL ENVIRONMENTS

MAJOR PROFESSOR: Dr. Henry Hexmoor

Drones are unmanned aerial vehicles (UAVs) operated remotely with the help of cameras, GPS, and on-device SD cards. These are used for many applications including civilian as well as military. On the other hand, drone swarms are a fleet of drones that work together to achieve a special goal through swarm intelligence approaches. These provide a lot of advantages such as better coverage, accuracy, increased safety, and improved flexibility when compared to a single drone. However, the deployment of such swarms in an adversarial environment poses significant challenges. This work provides an overview of the current state of research on drone swarms in adversarial environments including algorithms for swarming formation of robotic attack drones with their strengths and weaknesses as well as the attack strategies used by attackers. This work also outlines the common adversarial counter-attack methods to disrupt drone attacks consisting of detection and destruction of drone swarms along with their drawbacks, a counter UAV defense system, and splitting large-scale drones into unconnected clusters. After identifying several challenges, an optimized algorithm is proposed to split the large-scale drone swarms more efficiently.

ACKNOWLEDGMENTS

I would like to take a moment to express my gratitude to many individuals who have supported me throughout my thesis journey. Without their help, my experience would not have been enriching and fulfilling on a personal level. Individuals both within and outside of academia have had a significant impact on my growth and transformation, shaping the development of this dissertation.

Firstly, I would like to thank my major professor Dr. Henry Hexmoor, for his unwavering guidance, support, and encouragement throughout my thesis journey. His expertise, insights, and dedication have been instrumental in shaping me into the scholar that I am today. I am indebted to him for all the time and effort he has invested in me and for his constant belief in my abilities. I could not have completed this journey without his guidance, and for that, I am truly grateful. Also, his mentorship has been critical to the success of my research, and I am grateful for his determined support throughout the writing of my thesis. His feedback on drafts, willingness to answer my questions, and insightful suggestions have made my defense a more robust and comprehensive piece of work.

Then, I would like to thank Dr. Bidyut Gupta and Dr. Koushik Sinha for their guidance, expertise, and persistent support that has been instrumental in helping me succeed and achieve my academic and professional goals. I express my sincere thanks to the committee professors for taking time out of their busy schedules to review my work and providing me with their valuable input and suggestions.

I also would like to thank Dr. Khaled R. Ahmed and the Department of Computer Science at Southern Illinois University, Carbondale for giving me a chance to perform this

research and also providing me with assistantships which have helped me develop as a person professionally and financially.

I thank my brother Dr. Omkar Dokur and my sister Sowmya Yadav Akula for their willingness to proofread my work, provide feedback on my research, and offer words of encouragement when I needed them most. Their insights and perspectives helped me to see things in a new light and challenged me to push myself further than I ever thought possible. Furthermore, I would like to acknowledge the support and love of my family, who have been my pillar of strength and have always believed in me.

DEDICATION

To my loving family, whose unwavering support and patience became my foundation.

PREFACE

In an age where technological advancements are rapidly evolving, the use of drones and drone swarms in various capacities has become prevalent. Their applications range from entertainment and photography to more critical functions like surveillance, reconnaissance, and even warfare. While the positive implications of drones are manifold, they also introduce unprecedented challenges, especially in defense sectors. The purpose of this study is not just to shed light on the world of drone swarms and their potential threats but to delve deeper into understanding the mechanisms behind their operations. Through a comprehensive examination of existing counter-attack methods and the development of an improved counter-attack algorithm, this work aims to fortify our defenses against potential drone swarm threats.

Throughout these chapters, insights will be provided into the intricate balance between attack and defense in the drone swarm realm. This work elaborates on the current state of affairs and envisions a future with fortified skies. This study aims to serve as a reference for researchers, defense professionals, and enthusiasts, navigating them through the complexities of drone technology and its implications. As the horizon of knowledge expands, may this work stand as a testament to the significance of continuous learning and innovation.

TABLE OF CONTENTS

LIST OF ALGORITHMS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION ON DRONES AND DRONE SWARMS

In this chapter, first drones, drone swarms, and swarm intelligence are introduced. Then the problem statement, novelty and contributions, and organization of the thesis are provided.

1.1 Drone and Drone Swarms

Drones or Unmanned Aerial Vehicles (UAVs) can be piloted from a distance without the need for an onboard human operator. They are equipped with advanced components such as cameras, which provide real-time visual feedback; GPS systems, ensuring precise navigation and location tracking; and SD cards, which store crucial data and flight logs [1]. Their applications are vast and varied. On the civilian front, they are employed for tasks like aerial photography, agricultural monitoring, and delivery services. In contrast, their military applications include surveillance, reconnaissance, and even targeted strikes, all facilitated through secure wireless networks [2]. The concept of drone swarms takes the capabilities of individual drones to the next level. Instead of operating in isolation, drone swarms consist of multiple drones that operate in a coordinated manner, much like a flock of birds. This coordination is achieved through the Swarm Intelligence Approach, a method inspired by the natural behaviors of colonies of ants, bees, and other organisms. It allows for decentralized control, adaptive task allocation, and robustness against individual failures [3].

To ensure seamless coordination within a drone swarm, specialized algorithms, often referred to as swarm algorithms, are employed. These algorithms allow drones to communicate with each other, share information, and make collective decisions based on the data they gather. This ensures that the swarm can adapt to changing environments, avoid obstacles, and achieve their objectives in a harmonized manner [4]. As technology continues to advance, the potential applications and capabilities of drone swarms are bound to expand, heralding a new era of autonomous aerial operations.

1.2 Swarm Intelligence

Swarm Intelligence (SI) is an interesting field that delves into the collective behavior exhibited by decentralized, self-organized systems, often drawing inspiration from nature. It is particularly pivotal in the realm of multiple UAV collaborations, commonly referred to as drone swarms. In these scenarios, SI ensures that individual drones, despite having limited capabilities on their own, can work together in a harmonized manner to achieve complex tasks that would be impossible for a single drone. One of the most intriguing applications of SI is in Swarm Robotics. In this domain, rather than relying on a few sophisticated robots, the emphasis is on deploying large numbers of relatively simple robots. These robots, though individually limited, leverage the principles of SI to self-coordinate, adapt to their environments, and collaboratively achieve objectives. This approach mimics behaviors observed in natural systems, such as ant colonies searching for food or birds flocking together.

The classification of SI is vast and multi-faceted, drawing inspiration from various disciplines. Evolutionary processes, for instance, have led to the development of algorithms that mimic the survival and reproduction strategies of organisms. Biological inspirations come from studying the behaviors of social insects like bees, ants, and termites. Physics-based SI takes cues from phenomena like magnetism and gravity, while human-inspired SI looks at our societal structures, decision-making processes, and collaborative behaviors [5]. Given this broad classification, it's no surprise that there are numerous SI approaches that have been developed over the years. Each approach offers unique strategies and solutions, tailored to specific challenges or objectives. While this thesis touches upon a few, it's worth noting that the world of

SI is vast and ever evolving, with researchers continuously uncovering new methods and refining existing ones to better harness the power of collective intelligence.

1.3 Problem Statement

This thesis describes algorithms for swarming formation of robotic attack drones in an adversarial environment. Then, the thesis delves into a comprehensive analysis of the strengths and weaknesses associated with swarm formation and their attack strategies. Later, common adversarial counter-attack methods are outlined to disrupt drone attacks. Further, this work seeks to address the challenges associated with the deployment and defense of drone swarms in adversarial environments and aims to develop an optimized algorithm for effectively splitting large-scale drone swarms.

1.4 Novelty and Contributions

This thesis introduces a novel hybrid GA-PSO algorithm that seamlessly combines the exploration capabilities of the Genetic Algorithm (GA) with the exploitation strengths of the Particle Swarm Optimization (PSO). This innovative approach is designed to strike a balance between global and local search, ensuring a comprehensive exploration of the solution space. Another groundbreaking feature of this research is the adaptive parameter tuning for PSO. By dynamically adjusting the PSO's parameters, the work addresses the longstanding challenge of parameter sensitivity, which has been a concern in its standalone applications. Furthermore, the continuous integration and comparison of solutions from both GA and PSO ensure that the algorithm is always evolving, leading to more reliable and efficient outcomes.

In terms contributions of, the research offers a detailed overview of the current state of drone swarms in adversarial environments. It delves deep into the algorithms for swarming formation, their inherent strengths and weaknesses, and the various attack strategies employed by adversaries. The thesis also provides insights into the common adversarial counter-attack methods designed to disrupt drone attacks. It meticulously outlines both detection and destruction methods, highlighting their respective drawbacks. A significant portion of the research is dedicated to the swarm-based counter UAV defense system, showcasing its capabilities in patrolling, detection, interception, and counter-attacking drones. One of the standout contributions of this work is the identification of challenges in existing methods of splitting large-scale drone swarms. To address these challenges, an optimized hybrid GA-PSO algorithm is proposed, offering a sophisticated solution to the complex optimization problems associated with drone swarms. Lastly, the research provides a comparative analysis between the proposed hybrid algorithm and existing algorithms, emphasizing the strengths and potential areas of improvement of each approach. In essence, this work significantly contributes to the field by offering a holistic understanding of drone swarms in adversarial environments and introducing innovative methods to counteract drone threats.

1.5 Organization of the Thesis

The rest of the thesis is organized as follows. In Chapter 2, delves into the current drone swarm formation algorithms and their respective attack strategies. It provides a comprehensive overview of various algorithms, including Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Ant Colony Optimization, Cuckoo Search, and Artificial Potential Field. Chapter 3 discusses various methods to counteract drone swarm attacks. It covers detection and destruction methods, counter UAV systems, and techniques for splitting large-scale drone swarms. In Chapter 4, the challenges associated with existing methods of splitting large-scale drone swarms are identified. An optimized hybrid GA-PSO algorithm is proposed to address these challenges, and a comparative analysis is provided to compare the proposed algorithm with existing ones. Lastly, Chapter 5 summarizes the key findings of the research and discusses potential avenues for future work in the realm of drone swarms in adversarial environments.

1.6 Chapter Summary

This chapter offers a comprehensive introduction to the realm of drones and their collective operation as drone swarms. It delves into the intricacies of Unmanned Aerial Vehicles (UAVs), highlighting their remote operation capabilities, advanced components like cameras and GPS systems, etc. This chapter further explores the Swarm Intelligence Approach, the underlying principle facilitating this coordination, drawing parallels to behaviors observed in natural colonies of ants, bees, and other organisms. The significance of specialized swarm algorithms, which enable drones to communicate, share information, and make collective decisions, is underscored, emphasizing the swarm's adaptability and harmonized functioning. By providing a foundational understanding of drones, their collaborative potential as swarms, and the intelligence mechanisms that drive their coordinated actions, this chapter then presents the problem statement, novelty and contributions, and organization of the thesis.

CHAPTER 2

EXISTING DRONE SWARM FORMATION ALGORITHMS

This chapter elucidates current drone swarm formation algorithms and explores the potential misuse in the form of attack strategies.

2.1 Drone Swarm Algorithms

Drone swarm algorithms provide the foundation for multiple drones to coordinate, collaborate, and harmoniously complete tasks. Emulating natural swarm behaviors like bird flocking, these algorithms empower drone swarms to tackle intricate tasks that single drones might find challenging. This section examines some prevalent drone swarm algorithms.

2.1.1 Genetic Algorithm (GA)

Genetic algorithm is a search algorithm that is inspired by the process of natural selection. As shown in the algorithm 1, the population of drones has evolved over time to find the best solution [3]. As it can be seen that the design depends on Selection, Crossover, Mutation and fitness functions [2]. The algorithm can be used to optimize the formation of the drones. This algorithm is robust, flexible, and easy to implement but it is sensitive to parameters, needs a well-designed fitness function and requires complex computation.

Algorithm: GA

```
Generate the initial population
Compute fitness()
while (termination criteria reached) do
{
    parent Selection();
    Crossover;
    Mutation;
    Compute fitness();
    survivor selection;
    find best;
}
return best
```

Algorithm 1: Pseudo code for GA

2.1.2 Particle Swarm Optimization (PSO)

Particle Swarm Optimization is a search algorithm and is inspired by the flocking behavior of birds in search of food [3,6]. As shown in the algorithm 2, the position of each particle is updated based on its own knowledge and the swarm's knowledge. Also, random variables and coefficients are introduced in order to avoid stagnation. This algorithm is simple and efficient [2] but it falls easily into local optimum in high-dimensional space, and has low convergence rate, requires a large number of particles leading to high computation cost [7].

```
Algorithm: PSO
Initialize velocity and position of each particle
while (iteration equals max iterations) do for each particle
{
    calculate fitness value;
    calculate individual optimal fitness value;
    calculate global optimal fitness value;
    update velocity and position;
}
return global optimum
```

Algorithm 2: Pseudocode for PSO

2.1.3 Ant Colony Optimization

Ant colony Optimization is based on the behavior of ants searching for food to find the shortest path between nest and their food source [3]. As shown in the algorithm 3, it mimics the processing of pheromones by ants where ants can leave a substance called a pheromone on their path, and other ants can perceive the strength of this substance to guide their direction of action during foraging. It is a population-based algorithm [8], robust and flexible, simple and intuitive but requires a large number of iterations to converge. Due to this, it suffers from the problem of premature convergence.

Algorithm: ACO

```
Initialize necessary parameters and pheromone trials;
while not termination do:
        generate ant population;
        calculate fitness values associated with each ant;
        find best solution through selection methods;
        update pheromone trial;
end while
```

Algorithm 3: Pseudocode for ACO

2.1.4 Cuckoo Search (CS)

Cuckoo search is based on the reproductive behavior of Cuckoos [6]. As shown in the algorithm 4, the search for a nest is based on Levy flights where it uses the Levy flights parameters to maintain a balance between local and global random flights. This algorithm is simple and easy-to-implement, and can find high-quality solutions quickly but it suffers from the problem of premature convergence.

```
**Algorithm:** CS
Generate initial population of n host nest
Evaluate fitness and rank egg
while (t > max generation) do
{
    Get cuckoo randomly by Levy flights
    Evaluate fitness Fi
    Choose a random nest among n (say, j) randomly
    if (Fi > F j) then
        Replace j by new solution
    end if
    Worst nest is abandoned with a fraction Pa and new nests are built
    Keep the best solutions (or nests with quality solutions)
    Rank the solutions and find the current best
}
Return postprocess results
```

Algorithm 4: Pseudocode for CS

2.1.5 Artificial Potential Field (APF)

This algorithm creates an artificial field around the goal. Then, it treats each agent as an equal signal [9] to introduce repulsive forces between them so this moves the drones along the direction of resulting force as shown in the algorithm. It is an easy-to-implement, requires minimal computational resources but sensitive to the choice of parameters and also does not guarantee global optimality.

```
Algorithm: APF
Initialize position and velocity of drone;
Define attractive and repulsive potentials
while (goal reached) do:
        calculate attractive potential between drone and goal;
        calculate repulsive potential between drone and obst;
        calculate resultant force;
        update drone velocity using resultant force;
        update drone position using updated velocity;
end while
```

Algorithm 5: Pseudocode for APF

2.2 Attack Strategies

Harnessing the capabilities of drone swarm algorithms extends beyond benign applications. When misused, these algorithms can lead to potentially disruptive and dangerous activities. Based on their mode of operation, drone swarm attack strategies can be broadly classified into two types: physical and logical [10].

2.2.1 Physical Attack Strategies

Physical attacks exploit the tangible capabilities of drone swarms to commit illicit actions. Some examples of these attacks include:

- Smuggling: By utilizing drone swarms, it becomes possible to penetrate geo-boundaries while evading conventional surveillance systems. This can be particularly beneficial for malicious individuals looking to deliver contraband items like drugs, weapons, or communication devices to specific locations, such as inside prison walls.

- Assault: Weaponizing drones opens up a plethora of harmful possibilities. Drones can be equipped with blades, explosives, or other dangerous payloads. These weaponized drones can then be directed towards individuals or gatherings, leading to potential harm or even fatalities. For instance, a drone might be programmed to crash into a specific target.
- Sabotage: The physical capabilities of drone swarms extend to causing disruptions in key infrastructures. Swarms can target power lines, interfere with airport operations, or initiate mechanical failures in critical facilities.
- Terrorist Activities: There's a growing concern about militant groups employing drone swarms. They could deploy explosives overpopulated areas, military bases, or strategic locations, augmenting the unpredictability and scale of their attacks.

2.2.2 Logical Attack Strategies

Logical attacks focus on exploiting digital vulnerabilities. By leveraging their numbers and mobility, drone swarms can become powerful tools for cyber-espionage and other cybercrimes:

- Wi-Fi Deception: By creating rogue Wi-Fi hotspots, drone swarms can deceive individuals into connecting to malicious networks. Once connected, data transfer can be intercepted, monitored, and even altered. This makes it easy for attackers to capture sensitive details like login credentials or financial information.
- Data Espionage: Drones, when equipped with advanced surveillance technology, can act as mobile spying devices. Hovering around office buildings or private residences allows them to intercept communications or capture valuable data from unsuspecting victims.
- Propaganda: In volatile regions, drone swarms can capture footage which can then be manipulated or taken out of context. Such misleading videos can be powerful tools for

propaganda, furthering a particular narrative or agenda.

- GPS Spoofing: Another cyber threat posed by drone swarms is GPS spoofing. Drones can send out false GPS signals, leading navigation systems of vehicles or other drones astray, or even directing them into hazardous zones. As drone technology continues to evolve, understanding these potential attack strategies becomes paramount. It's vital for research to stay a step ahead, ensuring the benefits of drone swarms are harnessed without compromising security.

As drone technology continues to evolve, understanding these potential attack strategies becomes paramount. It's vital for research to stay a step ahead, ensuring the benefits of drone swarms are harnessed without compromising security.

2.3 Chapter Summary

In this chapter, we summarized the current drone swarm formation algorithms and their attack strategies.

CHAPTER 3

DRONE SWARM COUNTER-ATTACK METHODS

In this chapter, drone swarm counter methods are discussed.

3.1 Detection Methods and Drawbacks

Chen et al. [2] presented drone detection methods that use Radars, RF scanners, Acoustic, and Video techniques. But each of these detection methods have their own drawbacks. Radar is a mature approach to detect and locate drones, but it suffers from high, false-positive rates with a high cost to deploy. RF Scanners are used to detect drones by capturing the radio signals transmitted by drones that suffer from a high probability of false alarms. Acoustic method captures noise of the drones, but the range is limited by the sensitivity to the ambient noise and the necessity of calibration for different environments. Video based method uses computer vision and pattern recognition technology to detect and track drones. Object detection based on video images has been well studied, but it still has some shortcomings such as relatively short detection ranges, dependency on the sightline and easily being affected by adverse weather conditions.

3.2 Destruction Methods and Drawbacks

Chen et al. [2] presented drone destruction methods consisting of cyberspace-oriented and hardware-oriented. In the cyberspace-oriented method, it includes sending interference signals aimed at the drone’s controller using GPS spoofing and jamming [11]. This will result in the drone falling into location confusion. In the hardware-oriented method, it aims at destroying the drones using the following ways: missile damage, weapon damage, physical capture, disabling electronic components, and deployment of defensive drone swarms. Both of these methods are suitable for countering a single drone. However, drone attacks are more likely to occur as swarms which consist of a large number of tiny drones. It is difficult to target and shoot down them separately in a limited time.

3.3 Counter UAV Systems

In this section, the swarm-based counter UAV defense system [12] is discussed. As shown in Figures 1-4, the counter UAV system includes patrolling, detection, interception, and counter-attacking the drones. This is achieved through Autonomous defense system which is capable of self-organizing their formation. These defense drones intercept malicious drones, capture and escort them. Here, defense drones form a 3-dimensional cluster around malicious

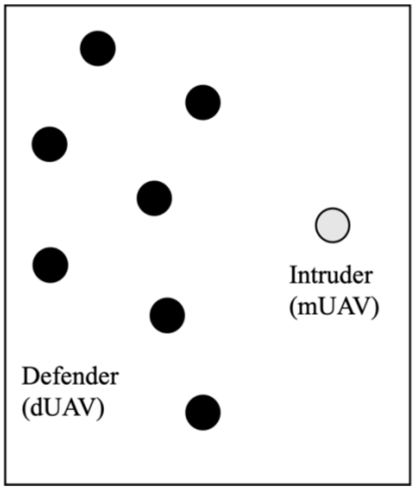

Figure 1: Patrolling by UAV system

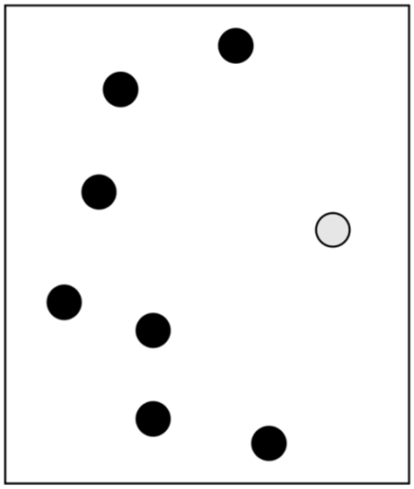

Figure 2: Detection by UAV system

drones using local clustering and positioning in 3D-space.

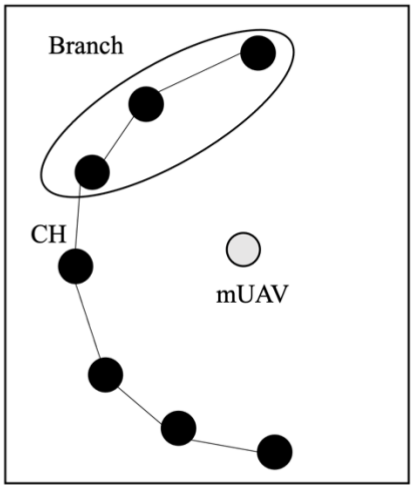

Figure 3: Interception by UAV system

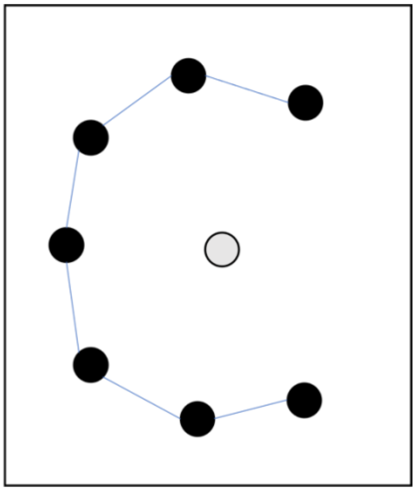

Figure 4: Counter-attack by UAV system

3.4 Splitting Large-Scale Drone Swarms

Apart from detecting, destructing, and counter-attacking drone swarms, splitting them seems to be an effective way [2]. To address this, critical nodes in the drone swarm are identified and disabled as shown in Figures 5, 6, and 7. This will have a greater effect on the drone swarm

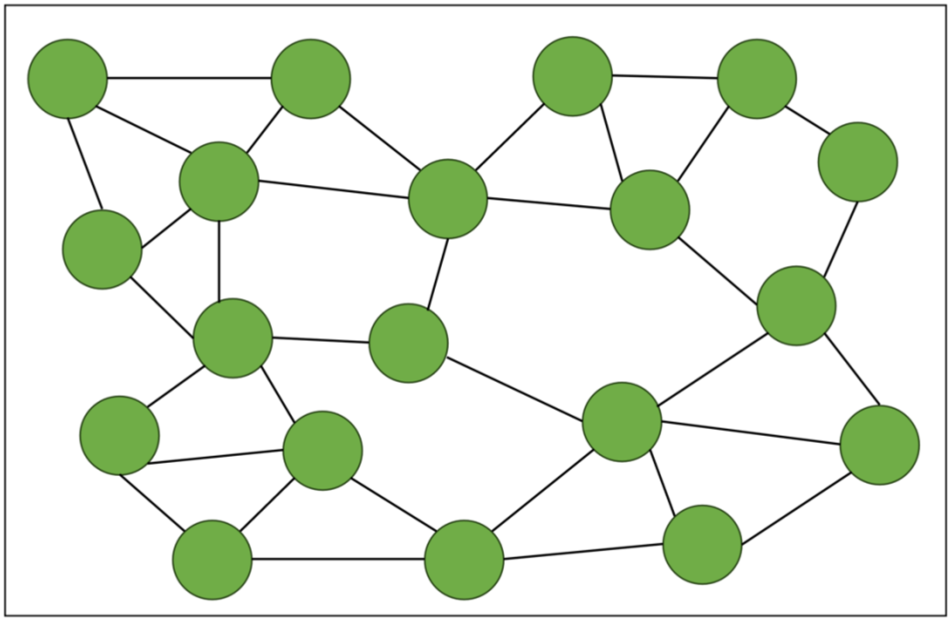

Figure 5: Drone Swarm Network

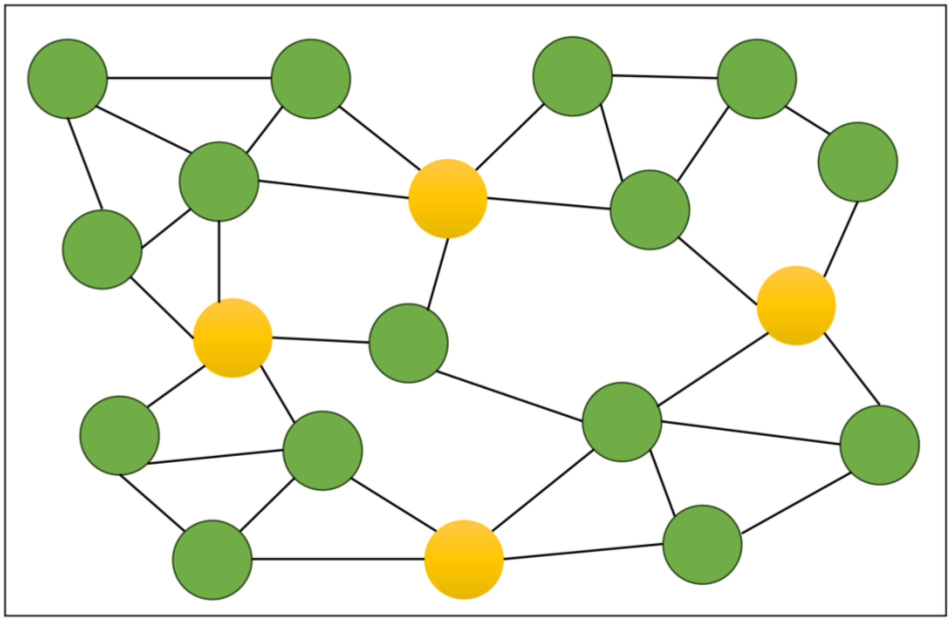

Figure 6: Critical nodes of the Drone Swarm

by reducing their overall strength. For this, they have proposed two algorithms known as the Genetic algorithm (GA) and the Particle Swarm Optimization (PSO) algorithm. These algorithms take a graph G of the drone swarm as input, identify and output the critical nodes and edges. This will lead to unconnected clusters thereby destroying the communication. Out of the two algorithms, PSO is the simpler and faster approach. To validate the proposed algorithms, a Qualnet simulator is used to test the algorithms and provide the effectiveness of the approach.

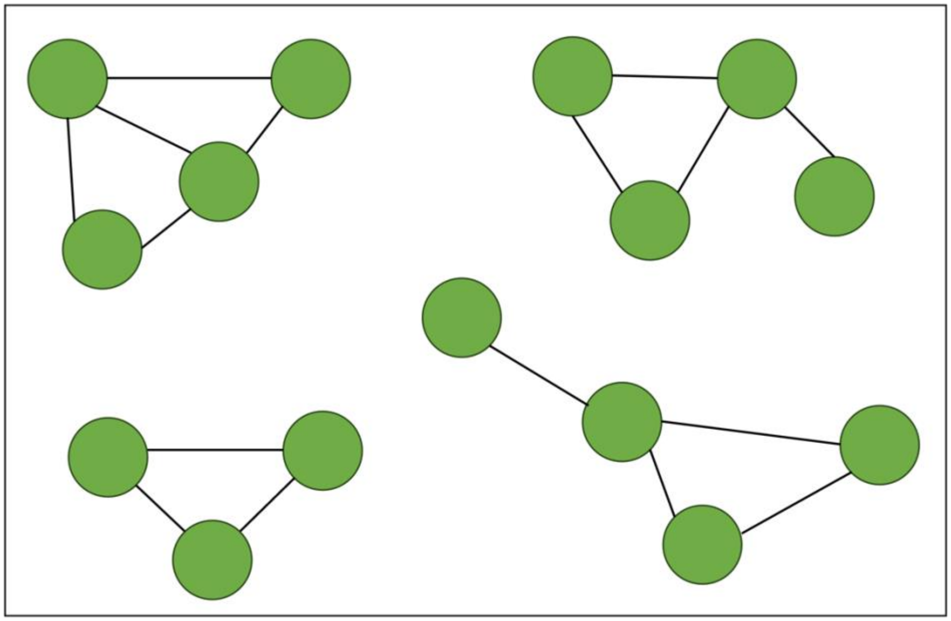

Figure 7: Disabling critical nodes of the Drone Swarm

3.5 Discussion

In this section, a discussion on the strengths and weaknesses of the current drone swarm counter-attack methods is presented. From above, both detection and destruction methods do not work efficiently against drone swarms. To counter-attack drone swarms in a fast, efficient, and low-cost approach, counter UAV systems and splitting large-scale drones were proposed. Out of these two approaches, the latter one seems to be promising. Some of the strengths of splitting large-scale drone swarms include:

- This approach can find the optimal solution with high accuracy and efficiency, which is crucial for quickly suppressing drone swarm attacks in practical environments.
- When the optimization algorithms (GA and PSO) are compared with the brute-force method, the brute-force search time becomes infinitely long with an increase in the

number of nodes, while the convergence time of GA and PSO remains under 20 seconds, making them more practical for real-world applications.

3.6 Chapter Summary

In this chapter, the current drone detection and destruction methods along with their drawbacks are discussed. As these techniques are limited to detect and destruct a single drone, counter UAV and splitting large scale drones are used. These approaches are summarized along with their strengths.

CHAPTER 4

IMPROVED COUNTER-ATTACK ALGORITHM

This chapter presents an improved counter-attack algorithm to split large scale drone swarms. First, the challenges in the current method are presented followed by an improved algorithm. Further, a comparative analysis is provided to compare existing algorithms with the improved one.

4.1 Current Challenges

In this section, we discuss the challenges associated with the algorithms associated in splitting the large-scale drone swarms discussed in [2]. The brute-force search time presented becomes infinitely long when the number of nodes exceeds 10. This makes it impractical for larger drone swarms. The quality of the optimal solution obtained by GA and PSO might be lacking as the number of nodes increases. However, the solutions obtained by these algorithms are close to the brute-force method, indicating their relative reliability. The PSO algorithm is sensitive to parameter configurations which means that the performance of PSO can vary based on the chosen parameters. Also, GA sometimes finds a poorer solution compared to PSO. This indicates that neither algorithm is perfect, and there's room for improvement. To address these challenges, an optimized algorithm is proposed that combines the strengths of both GA and PSO algorithms.

4.2 Hybrid GA-PSO Algorithm

In this section, a hybrid GA-PSO algorithm is proposed along with a pseudo-code as shown in Algorithm 6 that combines both GA and PSO. The proposed hybrid algorithm aims to combine the exploration capabilities of GA with the exploitation capabilities of PSO, ensuring a balance between global and local search. The adaptive parameter tuning for PSO addresses the challenge of parameter sensitivity, allowing the algorithm to self-adjust for better performance. By continuously comparing and integrating solutions from both algorithms, the hybrid approach ensures that it benefits from the strengths of both GA and PSO.

i. **Initialization:** The algorithm is initialized first as below:

   a. Define the drone swarm topology.

   b. Initialize populations for both GA and PSO with random solutions.

   c. Set parameters for GA (crossover rate, mutation rate) and PSO (inertia weight, cognitive and social components).

ii. **Evaluation:** Evaluate the fitness of each solution in the GA and PSO populations based on the objective function (e.g., minimizing the number of critical nodes to split the drone swarm).

iii. **Selection and Crossover:** Select pairs of solutions based on their fitness and perform crossover on selected pairs to produce offspring.

iv. **Mutation:** Apply mutation to the offspring with a certain probability of introducing genetic diversity.

v. **Update Velocities and Positions:** Calculate the new velocity for each particle in PSO based on its previous velocity, personal best position, and global best position. Then, update the particle's position using the new velocity.

vi. **Adaptive Parameter Tuning:** Monitor the convergence of the PSO algorithm. If the algorithm is stuck in a local optimum, adjust the inertia weight or cognitive and social components dynamically.

vii. **Combination of GA and PSO:** Compare the best solutions obtained from GA and PSO. If the PSO solution is better, introduce it into the GA population and vice versa. This ensures that both populations benefit from the strengths of the other algorithm.

viii. **Termination:** Check the termination criteria (e.g., a maximum number of iterations or a satisfactory fitness level). If the criteria are met, terminate the algorithm else return to the evaluation step.

ix. **Post-Processing:** Once the algorithm terminates, select the best solution from both GA and PSO populations. Implement the solution to split the drone swarm efficiently.

Next, we provide a pseudocode for the hybrid GA-PSO algorithm:

```
function HybridGA_PSO():
    // Initialization
    Define drone_swarm_topology
    Initialize GA_population, PSO_population, GA_parameters, and PSO_parameters

    while not TerminationCriteriaMet(iteration_count, max_iterations):
        // Evaluation
        Evaluaye GA_fitness with GA_population and PSO_fitness with PSO_population

        // GA Operations
        selected_pairs = SelectPairs(GA_population, GA_fitness)
        offspring = Crossover(selected_pairs)
        offspring = Mutate(offspring)
        GA_population = IntegrateOffspring(GA_population, offspring)
        // PSO Operations
        for particle in PSO_population:
            velocity = UpdateVelocity(particle, PSO_parameters)
            position = UpdatePosition(particle, velocity)
            particle.Update(velocity, position)

        // Adaptive Parameter Tuning for PSO
        if PSOIsStuckInLocalOptimum():
            PSO_parameters = AdjustPSOParametersDynamically()

        // Combination of GA and PSO
        Obtain best_GA_solution and best_PSO_solution
        if Fitness(best_PSO_solution) > Fitness(best_GA_solution):
            IntegrateSolutionIntoPopulation(best_PSO_solution, GA_population)
        else:
            IntegrateSolutionIntoPopulation(best_GA_solution, PSO_population)
        iteration_count += 1

    // Post-processing
    final_best_solution = GetBestSolutionFromBoth(GA_population, PSO_population)
    ApplySolutionToSplitDroneSwarm(final_best_solution)
    return final_best_solution
```

Algorithm 6: Pseudocode for hybrid GA-PSO Algorithm

```
function PSOIsStuckInLocalOptimum():
    // Check if the PSO best solution hasn't changed for a certain number of iterations
    if number_of_iterations_without_change > stagnation_threshold:
        return True
    else:
        return False

function AdjustPSOParametersDynamically():
    // Based on the performance of the PSO population, adjust parameters
    Calculate average_fitness with PSO_population
    Initialize default parameters
    if average_fitness < threshold:
        Adjust parameters
    return updated_parameters
```

Algorithm 7: Pseudocode for PSO Adaptive Parameter Tuning Helper Functions

4.3 Comparative analysis

The proposed hybrid algorithm not only combines the strengths of both GA and PSO but also mitigates their individual limitations. By leveraging the exploration capabilities of GA, the algorithm can search through a broader solution space, ensuring a diverse set of potential solutions. On the other hand, the exploitation capabilities of PSO allow the algorithm to delve deeper into promising regions of the solution space, refining and optimizing solutions. This duality ensures that the algorithm doesn't get prematurely trapped in local optima and has a higher chance of finding a global optimum.

Furthermore, the challenge of PSO's parameter sensitivity, which has been a concern in its standalone applications, is addressed through adaptive parameter tuning. This dynamic adjustment means that the algorithm can better respond to different problem landscapes, making it more versatile and robust. Instead of relying on static parameters, which might not be optimal for all scenarios, the self-adjusting nature of the hybrid algorithm ensures it remains efficient across a variety of challenges.

Lastly, the continuous integration and comparison of solutions from both GA and PSO mean that the hybrid algorithm is always equipped with the best solutions from both worlds. This iterative feedback loop ensures that the algorithm is always evolving and improving, leading to more reliable and efficient outcomes. In essence, the hybrid approach is designed to be greater than the sum of its parts, offering a sophisticated solution to complex optimization problems.

CHAPTER 5

CONCLUSION

In this work, first drones and drone swarms are introduced. Then, the drone swarm formation algorithms are discussed including their strengths and weakness. Next, various attack strategies used by the attackers are presented by providing existing detection and destruction methods. As the detection and destruction methods are limited to a single drone, techniques such as counter UAV systems and splitting large scale drone swarms is discussed. Although the existing work on splitting large scale drone swarms is effective, several challenges associated with it are identified. To address these challenges, an optimized hybrid GA-PSO algorithm is proposed to identify and split large scale drones more efficiently.

REFERENCES

[1] Tahir, A., Böling, J., Haghbayan, M. H., Toivonen, H. T., & Plosila, J. (2019). Swarms of unmanned aerial vehicles—a survey. Journal of Industrial Information Integration, 16, 100106.

[2] Chen, W., Meng, X., Liu, J., Guo, H., & Mao, B. (2022). Countering Large-Scale Drone Swarm Attack by Efficient Splitting. IEEE Transactions on Vehicular Technology, 71(9), 9967-9979.

[3] Tang, J., Duan, H., & Lao, S. (2022). Swarm intelligence algorithms for multiple unmanned aerial vehicles collaboration: A comprehensive review. Artificial Intelligence Review, 1-33.

[4] Jung, C., Ahad, A., Jeon, Y., & Kwon, Y. (2022, May). SWARMFLAWFINDER: Discovering and Exploiting Logic Flaws of Swarm Algorithms. In 2022 IEEE Symposium on Security and Privacy (SP) (pp. 1808-1825). IEEE. Chicago

[5] Innocente, M. S., & Grasso, P. (2019). Self-organising swarms of firefighting drones: Harnessing the power of collective intelligence in decentralised multi-robot systems. Journal of Computational Science, 34, 80-101.

[6] Pliatsios, D., Goudos, S. K., Lagkas, T., Argyriou, V., Boulogeorgos, A. A. A., & Sarigiannidis, P. (2021). Drone-base-station for next-generation internet-of-things: A comparison of swarm intelligence approaches. IEEE Open Journal of Antennas and Propagation, 3, 32-47.

[7] Li, M., Du, W., & Nian, F. (2014). An adaptive particle swarm optimization algorithm based on directed weighted complex network. Mathematical problems in engineering, 2014.

[8] Dorigo, M., & Stützle, T. (2019). Ant colony optimization: overview and recent advances (pp. 311-351). Springer International Publishing.

[9] deOliveira, N. S. D. M. M., Moreira, E. M., & Rosa, P. F. F. (2019, October). Particle swarm optimization algorithm implementation for multiple drones control in continuous task simulation.

In 2019 Latin American Robotics Symposium (LARS), 2019 Brazilian Symposium on Robotics (SBR) and 2019 Workshop on Robotics in Education (WRE) (pp. 363-368). IEEE.

[10] Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, 11, 100218.

[11] He, D., Yang, G., Li, H., Chan, S., Cheng, Y., & Guizani, N. (2020). An effective countermeasure against UAV swarm attack. IEEE Network, 35(1), 380-385.

[12] Brust, M. R., Danoy, G., Stolfi, D. H., & Bouvry, P. (2021). Swarm-based counter UAV defense system. Discover Internet of Things, 1, 1-19.

VITA

Graduate School
Southern Illinois University Carbondale

Bhavana Sai Yadav Akula

bhavanaakula11@gmail.com

Jawaharlal Nehru Technological University
Bachelor of Technology, Computer Science, July 2021

Thesis Paper Title:
Drone Swarms in Adversarial Environments

Major Professor: Dr. Henry Hexmoor