5-12-2024

Path Planning and Cyber-Physical System Integration in Unmanned Aerial Vehicles for Wireless Communication

MOHAMAD HANI SULIEMAN
Syracuse University

Abstract

Unmanned Aerial Vehicles (UAVs) have become indispensable in a variety of fields, including surveillance, emergency response, packet delivery, and data collection for the Internet of Things (IoT). These systems are also critical in enhancing connectivity within cellular networks. This dissertation focuses on improving UAV operational efficiency and security by advancing trajectory optimization techniques, enhancing trajectory design through antenna radiation patterns, and increasing resilience against cyber-physical attacks, particularly GPS sensor faults.

The first part of the study addresses UAV trajectory optimization in wireless communications, highlighting the significance of trajectory planning in improving the efficiency and reliability of UAV operations. Effective trajectory planning ensures optimal energy usage and maximized coverage areas, crucial for maintaining robust communication links with ground base stations (GBS). This optimization is vital for enhancing both the performance and safety of UAV operations in complex environments.

Building on trajectory optimization, the second part of the research explores the impact of antenna radiation patterns on UAV trajectory design. The study develops an Enhanced Artificial Potential Field (Enhanced-APF) algorithm that integrates the 3D radiation patterns of antennas equipped on UAVs. This integration is essential for facilitating effective collision avoidance and smoother navigation paths, thereby optimizing UAV performance in scenarios involving multiple UAVs and ensuring safer operations across various applications.

The final part of the dissertation introduces a novel algorithm, the Resilient Cyber-Attack Artificial Potential Field (RCA-APF), designed to enhance the resilience of UAV path planning against permanent GPS faults within a cyber-physical system (CPS) framework. This algorithm employs a three-stage process: detecting GPS faults due to the attack, estimating UAV location using Received Signal Strength (RSS) trilateration, and adjusting the UAV's

path planning accordingly. The effectiveness of this approach is validated through rigorous experimental and simulation testing, demonstrating its capability to substantially improve the robustness of UAV operations against cyber-physical threats.

Overall, this research provides comprehensive strategies for improving UAV trajectory planning and resilience, offering significant advancements in the safe and efficient deployment of UAVs. By integrating advanced cyber-security measures with strategic communications engineering, the dissertation contributes to the development of more reliable and effective UAV systems, paving the way for their expanded use in increasingly complex scenarios.

PATH PLANNING AND CYBER-PHYSICAL SYSTEM INTEGRATION IN UNMANNED AERIAL VEHICLES FOR WIRELESS COMMUNICATION

By

Mohamad Hani Sulieman

B.S., Syracuse University, 2016

M.S., Syracuse University, 2022

Dissertation

Submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Electrical and Computer Engineering

Syracuse University

June 2024

Acknowledgments

First and foremost, I extend my deepest gratitude to my advisor, Dr. Mustafa Cenk Gursoy, whose patient guidance and unwavering support have been instrumental during my doctoral studies. His commitment to academia and passion for research inspired me to overcome numerous challenges throughout my dissertation journey. I could not have completed this work without his invaluable advice and encouragement.

I would also like to express my sincere thanks to the members of my defense committee, Dr. Shiu-Kai Chin, Dr. Can Isik, and Dr. Carlos E. Caicedo Bastidas, for their insightful comments and suggestions. Special thanks to Dr. Ruth Chen for her endless support throughout my research endeavors.

My gratitude extends to both my current and former colleagues at the Wireless Communication & Networking Lab. Their camaraderie and support have enriched both my professional and personal life. Special acknowledgment is due to my collaborator, whose stimulating academic discussions have greatly enhanced my research experience.

I am profoundly thankful to my friends at Syracuse University for their companionship and emotional support, especially during the challenging times posed by the COVID-19 pandemic. Most importantly, I owe my deepest gratitude to my family—my parents, aunt and her husband, and sisters—for their unwavering love and encouragement. The motivation and inspiration they instilled in me from childhood continue to drive me forward. Their understanding and care have enabled me to pursue my studies with a profound sense of peace. I dedicate this dissertation to my family.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 UAV Path Planning in Wireless Communication

The utilization of unmanned aerial vehicles (UAVs), also known as drones, has expanded into various civilian domains such as aerial mapping, delivery of goods and healthcare supplies, and search and rescue operations [1], [2]. Advances in battery power management and solar energy harvesting, coupled with their ability to bolster network capabilities, have led to the growing use of UAVs as aerial base stations. This development positions UAVs as key players in reshaping the future of broadband communication networks. Utilizing UAVs as aerial base stations brings several advantages. Their higher altitude increases the probability of establishing line-of-sight (LoS) connections with ground users. Additionally, the mobility and flexible deployment of UAVs facilitate rapid and adaptable communication services on demand [3].

However, the deployment of UAVs as airborne base stations is not without challenges. Critical issues include optimizing the 3D positioning of UAVs, managing energy constraints, controlling interference, and formulating efficient path planning strategies [4]. UAV path planning is particularly vital in enhancing wireless communication, involving the careful design of flight routes to optimize signal coverage, data collection, and transmission efficiency

[5], [6]. This is crucial in scenarios like establishing temporary communication networks in disaster-stricken areas or improving coverage in low-signal regions. UAVs, equipped with communication payloads, dynamically adjust their positions based on user distribution, terrain, and signal strength, thereby optimizing network performance [7]. Advanced algorithms that account for factors such as battery life, flight duration, and environmental challenges are used in path planning. This approach not only broadens coverage but also minimizes latency, enhancing the quality of service in wireless networks. The integration of UAVs into wireless communication systems represents a significant step towards more flexible, resilient, and efficient network infrastructures [8].

Furthermore, UAV trajectory optimization is a critical aspect of enhancing the effectiveness of UAVs as airborne base stations in wireless communication networks [9]. It involves the precise design of UAV flight paths to meet specific communication goals while considering operational constraints. This process is essential for ensuring effective area coverage, consistent signal quality, and optimal energy utilization of UAVs.

Overall, UAV trajectory optimization is a complex but crucial element that greatly enhances the functionality of UAVs in wireless communication networks. It ensures that UAVs provide not only extended coverage and improved connectivity but also operate in an efficient and sustainable manner, leading to more advanced and reliable wireless communication solutions [10].

1.2 Antenna Pattern Design for UAVs

Due to the UAVs' capability to navigate in any direction at varying speeds, there's a pressing need for innovative antenna designs tailored for airborne communication to achieve high data rates. A viable solution for facilitating high-speed data transmission between UAVs and ground base stations (GBSs) is the implementation of antennas on UAVs. These antennas leverage gyroscopic, accelerometer, and GPS data to maintain alignment with the

ground base station (GBS), adjusting their orientation as necessary [11]. Additionally, the limited space available on UAVs, particularly smaller models, poses a challenge for antenna installation [12]. To address this, the adoption of a tilted beam circularly polarized antenna mounted on the UAV's underside has been proposed [13], offering a space-efficient solution. Simulation studies have demonstrated that such an antenna configuration can deliver superior performance in terms of return losses, axial ratio, and radiation patterns, thereby enhancing airborne communication efficacy.

1.3 Cyber-Attacks to the UAV Systems

Since 2007, the surge in the popularity of drones has been paralleled by an increase in cyber-attacks targeting UAV systems, highlighting significant security concerns [14]. These attacks predominantly target the UAVs' radio links, essential for the transmission of data, control signals, and GPS navigation signals to and from cellular User Equipments (UEs). The interception of these signals by adversaries could lead to data theft or even the hijacking of UAVs, underscoring the critical need to secure these wireless communication channels for maintaining the integrity of UAV systems.

The vulnerability of UAVs is further exacerbated by their operation in complex and unregulated environments, compounded by the lack of stringent security protocols and the openness of wireless communication channels. This vulnerability landscape has prompted extensive research into the cyber-attack susceptibilities of UAVs, focusing on identifying and addressing potential security loopholes [15], [16].

UAVs, as cyber-physical systems (CPS), comprise an intricate network of sensors, communication frameworks, computational units, and control mechanisms. Each component within this network is a potential cyber-attack target, which could lead to critical system malfunctions and compromised operational states. Understanding these cyber-physical threats is imperative for developing robust defensive strategies. The study of UAVs, given

their complexity and role as safety-critical CPS, provides invaluable insights into the cyber-physical vulnerabilities that could affect other critical CPS infrastructures, highlighting the importance of comprehensive security measures in safeguarding these advanced systems.

1.4 Dissertation Organization

In Chapter 2, we conduct a detailed literature review and address the intricacies of optimizing the trajectory paths of Unmanned Aerial Vehicles (UAVs), a task that initially presents itself as a nonconvex optimization problem. Nonconvex problems are known for their complexity and computational challenges, often requiring sophisticated approaches to find solutions. The proposed methodology in the literature simplifies this complexity by transforming the problem into a convex format, which is significantly more manageable and solvable using standard optimization techniques. This transformation is achieved through the strategic introduction of an auxiliary variable, which serves as a pivotal element in reformulating the problem [2].

To validate the considered approach and ensure its practical applicability, we employ the CVX optimization tool, a powerful software package designed for solving convex optimization problems [17]. CVX provides a user-friendly interface and robust computational capabilities, making it an ideal choice for tackling complex optimization tasks. By leveraging CVX, we are able to precisely map out the optimal trajectories for UAVs as they navigate through a network of Ground Base Stations (GBSs) [2].

In Chapter 3, we delve deeper into the development of a cutting-edge narrowband shadowing model tailored for High Altitude Platforms (HAPs), such as Unmanned Aerial Vehicles (UAVs), operating within the urban fabric. This model is specifically designed for the 2-6 GHz frequency spectrum, which is pivotal for the infrastructure of contemporary mobile networks [18]. The essence of this model lies in its ability to accurately predict the probability of establishing Line-of-Sight (LoS) connections between HAPs and terrestrial mobile

stations, a critical factor in ensuring reliable communication links. Moreover, the model meticulously quantifies the additional path losses encountered in Non-Line-of-Sight (NLoS) scenarios, where physical obstructions lead to signal degradation, with a particular emphasis on how elevation angles influence these dynamics.

A unique aspect of this model is its capability to distinguish between LoS probabilities in varying urban densities, ranging from sparsely populated suburban areas to densely packed high-rise urban centers. This granularity allows for a nuanced understanding of how different urban landscapes impact the connectivity and performance of HAP-based systems, providing valuable insights for optimizing network designs in diverse urban settings.

Building on this foundation, the chapter also addresses the challenge of interference in heterogeneous aerial and terrestrial Internet of Things (IoT) networks. These networks often comprise a mix of simple wireless communication devices, where managing interference becomes crucial for maintaining network integrity. We discuss an innovative interference mitigation strategy that hinges on a cross-dipole antenna configuration. This setup intelligently switches between z-axis and y-axis dipole antennas depending on the specific characteristics of the receiving device, thereby optimizing signal reception.

The effectiveness of this antenna arrangement is rigorously analyzed through a comprehensive 3D channel model that incorporates the complex radiation patterns of the dipole antennas and the precise geographical positioning of IoT devices. Our analysis reveals that the y-axis dipole antenna configuration significantly enhances the performance of aerial-based receivers, outperforming the conventional z-axis setup [19]. This finding is pivotal, as it highlights a practical solution for improving aerial receiver performance in mixed IoT networks, thereby enhancing overall network efficiency and reliability in the intricate urban IoT ecosystems.

In Chapter 4, we refine the Artificial Potential Field (APF) algorithm [20], a cornerstone in UAV navigation technology, to better cater to the intricate demands of both individual UAV flights and coordinated swarm operations. This advancement was pivotal in overcoming

common navigational challenges, such as avoiding physical obstacles and preventing mid-air collisions among UAVs—a factor of paramount importance in scenarios involving multiple drones operating in close proximity, known as swarm dynamics.

A novel aspect of our approach was the integration of antenna radiation pattern considerations into the trajectory planning process. This inclusion was based on the understanding that the quality of communication links, which are vital for the control and coordination of UAVs, can be significantly influenced by the UAV's orientation and position relative to ground stations and other UAVs. By accounting for these factors, our algorithm was able to optimize flight paths not only for safety and efficiency but also for maintaining robust and reliable communication links.

The efficacy of our enhanced APF algorithm was validated through comprehensive simulations, which illustrated the algorithm's proficiency in guiding UAVs to their intended destinations while adeptly managing the dual objectives of navigational safety and communication integrity. The simulation outcomes highlighted the algorithm's potential to significantly improve operational outcomes in real-world UAV deployments. The content of this chapter is published as a conference paper in 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC) [21].

In Chapter 5, we consider the evolving security paradigm for Unmanned Aerial Vehicles (UAVs), shedding light on the intricate cyber and physical threats that these systems face. As UAVs become increasingly integrated into various sectors, their operation within Cyber-Physical Systems (CPS) exposes them to a unique blend of vulnerabilities that span both the digital and tangible realms. Our study adopts a comprehensive perspective, examining how cyber threats, such as data breaches, hacking, and cyber-physical interference, can transcend the digital boundary to induce tangible, often hazardous, consequences in the physical operation of UAVs. This includes scenarios where cyber intrusions lead to loss of control, collisions, or compromised mission integrity [22].

This holistic analysis is pivotal for several reasons. Firstly, it acknowledges that the

security of UAVs cannot be compartmentalized into separate cyber and physical domains. Instead, it underscores the necessity of a unified security strategy that addresses the continuum between cyber intrusions and their physical outcomes. Secondly, by exploring the symbiotic relationship between these threat vectors, our work illuminates the broader implications for CPS security. UAVs, as integral components of CPS, exemplify the challenges and complexities of securing systems where digital and physical elements are inextricably linked.

In Chapter 6, we introduce a two-step detection and recovery strategy to address cyber-physical attacks on UAV GPS systems. This strategy begins by detecting an attack when a UAV loses connection with its nearest ground base station (GBS), likely due to false data injections that alter its path. Our solution includes a novel detection and estimation architecture: initially, the UAV's location under GPS attack is estimated using Received Signal Strength (RSS) based trilateration. Subsequently, we implement a cyber-attack resilience procedure utilizing an enhanced version of the Artificial Potential Field (APF) algorithm, termed Resilience to Cyber-Attacks APF (RCA-APF).

The RCA-APF algorithm specifically addresses permanent GPS faults, effectively planning and recalibrating the UAV's path by utilizing real-time coordinates during flight. It not only facilitates obstacle avoidance but also ensures the UAV can navigate safely through potentially hazardous zones, even with compromised GPS data. The RCA-APF algorithm works in conjunction with the RSS trilateration to provide precise localization and safe navigation, forming a comprehensive solution to GPS inaccuracies.

In comparison to traditional APF algorithms, RCA-APF offers significant enhancements:

- It dynamically adjusts its responses based on environmental context, such as the proximity to obstacles and the severity of GPS faults.
- It demonstrates increased robustness in dynamic environments, crucial for UAV operation in GPS-compromised scenarios.

The effectiveness of this approach is validated through simulation-based experiments, demonstrating the algorithm's capability to maintain UAV safety and operational integrity under cyber-physical threats. The content of this chapter has been accepted for publication in the ACM Transactions on Cyber-Physical Systems [23].

Chapter 2

UAV Trajectory Optimization in Wireless Communication – Literature Review and Simulation Results

2.1 Introduction

Unmanned Aerial Vehicles (UAVs) are garnering significant interest for their potential in future applications that demand autonomous and swiftly deployable systems. Unlike traditional communication methods reliant on fixed infrastructure, UAV-aided networks offer enhanced benefits due to their inherent mobility [24], [5]. However, realizing the full potential of UAVs in such networks necessitates careful resource allocation, a task made complex by the UAVs' ability to freely navigate the airspace.

While utilizing UAVs as aerial base stations offers many benefits, several technical hurdles must be addressed. Key challenges encompass the strategic 3D positioning of UAVs, managing energy constraints, mitigating interference, and devising effective path planning strategies [25], [26]. Among these, the issue of deployment stands out due to its significant influence on both energy usage and the level of interference produced by the UAVs.

Yet, only a few studies have explored the relationship between UAV deployment and its impact on wireless performance [24], [5]. For example, research presented in [26] examines the role of multiple UAVs serving as wireless relays to support ground sensors, focusing on the balance between maintaining UAV connectivity and maximizing coverage. However, this study does not explore the concept of UAVs functioning as aerial base stations or consider the potential interference in downlink communications between them. In contrast, [27] employs evolutionary algorithms to determine the optimal positioning of Low Altitude Platforms (LAPs). The approach in [27], though, is based on the premise that LAPs can have overlapping coverage areas without issue, thanks to the use of Inter-Cell Interference Coordination (ICIC), a solution that necessitates additional communication measures.

To the best of our understanding, Zeng et al. [28] were the pioneers in examining the optimization of power and trajectory for UAV-assisted mobile relay systems, demonstrating that substantial throughput improvements are attainable by leveraging channel fluctuations. Lyu et al. [29] delve into a more straightforward scenario, considering users uniformly distributed in a linear arrangement on the ground. These insights have inspired us to leverage the mobility of UAVs to enhance service quality for ground users scattered randomly, by dynamically modifying the UAVs' positions and transmission power.

In this chapter, we perform a detailed literature review and delve into the challenges of power distribution and trajectory optimization within UAV-assisted networks, focusing on a scenario where a UAV simultaneously facilitates network connectivity for multiple nodes. We consider a non-convex optimization framework aimed at maximizing the minimum average throughput over a specified duration, taking into account both trajectory limitations and power constraints. Leveraging the unique properties of the problem at hand, we analyze an effective algorithm that concurrently optimizes transmit power and UAV trajectory. This involves initially tackling two separate subproblems: optimizing transmit power with a fixed trajectory and optimizing the trajectory with a set transmit power. Additionally, we consider a lower bound for the non-convex function in the trajectory optimization subproblem to

facilitate its resolution. The efficacy of the approach is corroborated by simulation results, which also highlight a water-filling characteristic of the optimized transmit power across the spatial domain.

2.2 Introduction to Convex Optimization

A mathematical optimization problem, often simply referred to as an optimization problem, is presented in the following format [30]:

$$\begin{aligned} &\text{minimize} \quad h_0(x) \\ &\text{subject to } h_j(x) \leq b_j, \quad j = 1, ..., m \end{aligned} \tag{2.1}$$

In this context, the vector $x = (x_1, ..., x_n)$ represents the set of variables to be optimized in the problem. The function $h_0 : \mathbb{R}^n \to \mathbb{R}$ serves as the objective function to be minimized or maximized. The functions $h_j : \mathbb{R}^n \to \mathbb{R},\ j = 1, ..., m$, act as the inequality constraints of the problem, and the constants $b_j, ..., b_m$ define the bounds or limits for these constraints. A vector x^* is deemed optimal or a solution to the problem (2.1) if it yields the lowest objective value while adhering to all the constraints: for any vector z that meets $h_1(z) \leq b_1, ..., h_m(z) \leq b_m$ it holds that $h_0(z) \geq h_0(x^*)$.

We typically examine specific families or categories of optimization problems, distinguished by the distinct structures of their objective and constraint functions. A notable instance is when the optimization problem, as outlined earlier (2.1), is termed a linear program. This classification arises when both the objective and the constraint functions exhibit linear characteristics $h_0, ..., h_m$ to satisfy the following

$$h_i(\alpha x + \beta y) = \alpha h_i(x) + \beta h_i(y) \tag{2.2}$$

for all $x, y \in \mathbf{R}^n$ and all $\alpha, \beta \in \mathbf{R}$. When the optimization problem does not adhere to linearity, it is referred to as a nonlinear program.

Indeed, a convex optimization problem is characterized by having both objective and constraint functions that are convex. This implies that these functions fulfill the specific inequality condition associated with convexity which given as follows

$$h_i(\alpha x + \beta y) \leq \alpha h_i(x) + \beta h_i(y) \tag{2.3}$$

for all $x, y \in \mathbf{R}^n$ and all $\alpha, \beta \in \mathbf{R}$ with $\alpha + \beta = 1, \alpha \geq 1, \beta \geq 1$.

Given that every linear program inherently qualifies as a convex optimization problem, it's accurate to view convex optimization as an extension or broader category encompassing linear programming.

2.2.1 Solving Optimization Problems

A solution method for a category of optimization problems refers to an algorithm designed to find a solution to a specific problem within that category, achieving a predetermined level of accuracy. Since the late 1940s, there has been significant investment in creating algorithms to solve various optimization problems, analyzing their characteristics, and developing robust software implementations. The efficiency of these algorithms, meaning our capacity to resolve the optimization problem, can greatly vary. This variability is influenced by factors such as the specific nature of the objective and constraint functions, the number of variables and constraints involved, and any unique structures like sparsity. A problem is considered sparse if each constraint function is influenced by only a limited subset of the variables [30].

However, there are notable exceptions to the general notion that most optimization problems pose significant challenges to solve. For certain classes of problems, we possess effective algorithms capable of reliably solving large-scale instances, involving hundreds or even thousands of variables and constraints. Prominent examples include least-squares problems and linear programs. Less commonly recognized is that convex optimization also falls into this category of exceptions. Similar to least-squares and linear programming, convex optimiza-

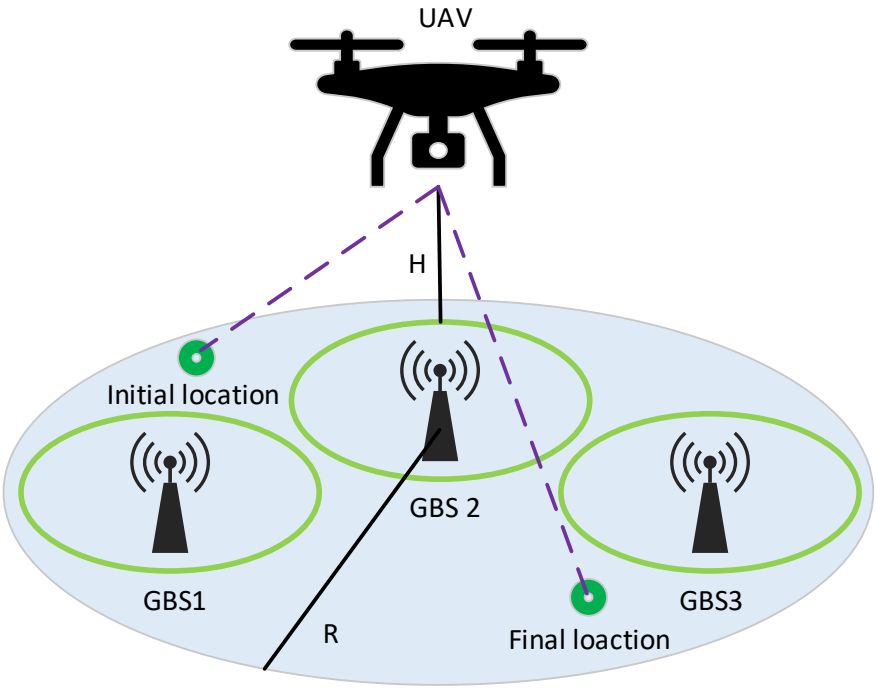


Figure 2.1: UAV Trajectory System Model

tion benefits from highly efficient algorithms that can dependably and effectively tackle large convex problems.

2.3 System Model And Problem Formulation

In this section, consider a situation where a group of N Ground Base Stations (GBSs), denoted as $N = \{1, 2, ..., n, ..., N\}$, are scattered randomly on the ground, and a UAV, cruising at a constant altitude H, offers network connectivity to these nodes over a limited time period T. Given that the UAV's takeoff and landing spots are typically predetermined for specific tasks, the starting and ending coordinates are specified as $[x_0, y_0, H]$ and $[x_F, y_F, H]$, respectively. By the same token, we consider a system model for UAV trajectory optimization, starting from an initial location and concluding at a final location, all within a specified circular geographical area with a radius of R, as illustrated in Figure 2.1. For simplicity, let's

consider $[x_0, y_0, 0]$ as the origin of the coordinate system in question. The entire duration T is segmented into M brief intervals, each of a duration δ, such that $T = M\delta$. Consequently, the UAV's path can be represented as a series of points $x[m], y[m], H$, where m belongs to the set $M = \{1, ..., M\}$. The choice of M, the count of discrete points, balances computational complexity against the precision of the trajectory approximation. In essence, a larger M or a smaller δ increases the number of optimization variables, thereby elevating the complexity. Conversely, it allows for a more finely detailed and accurate representation of the trajectory. Given that the UAV's maximum flight speed is capped at V, it is necessary to impose constraints on the UAV's positions as outlined below:

$$\begin{aligned} (x[1] - x0)^2 + (y[1] - y_0)^2 &\leq (V\delta)^2, \\ (x[m] - x[m-1])^2 + (y[m] - y[m-1])^2 &\leq (V\delta)^2, \\ (x_F - x[M])^2 + (y_F - y[M])^2 &\leq (V\delta)^2. \end{aligned} \tag{2.4}$$

Given that the UAV maintains a constant altitude H throughout its flight, we can, for the sake of simplicity, concentrate on the horizontal coordinates $\{x[m], y[m]\}$ in our subsequent analysis. In particular, we consider a downlink orthogonal frequency division multiple access scheme. The total available bandwidth and the transmit power are represented by B and P_T, respectively. Bandwidth is evenly distributed among all the nodes being served. The channel power gain between the UAV and the nth node during the mth time slot, denoted as $g_n[m]$, is primarily influenced by the line-of-sight component [31], [29], [10].

$$g_n[m] = \frac{\beta_0}{(x[m] - x_n)^2 + (y[m] - y_n)^2 + H^2} \tag{2.5}$$

where β_0 represents the channel power gain at the reference distance d_0, and $(x_n, y_n, 0)$ denotes the coordinates of the nth GBS. As indicated by equation (2.5), the channel power gain diminishes as the altitude H increases. Consequently, a lower altitude is preferable as it yields optimal channel conditions. Given this, the optimization of the UAV's altitude is

not addressed in this work. The average throughput experienced by the nth GBS over the time period T is as follows [5]:

$$R_n = \frac{1}{T}\sum_{m=1}^{M}\frac{B}{N}\log_2(1+\frac{p_n[m]g_n[m]}{B/N\sigma^2}) \tag{2.6}$$

where $p_n[m]$ denotes the transmit power of the UAV directed towards the nth GBS, and σ^2 represents the noise power spectral density. To guarantee communication access for all ground GBSs, as opposed to adopting a winners-take-all approach, the focus is on maximizing the minimum average throughput. This is achieved by judiciously allocating transmit power and fine-tuning the UAV's flight trajectory. The problem under consideration is mathematically expressed as follows [5]:

$$\begin{aligned}
&\max_{\{x[m],y[m]\},\{p_n[m]\}} \min_n \quad R_n \\
&\text{subject to } C1: \sum_{n=1}^{N}\sum_{m=1}^{M} p_n[m] \le P_T, \\
&\qquad C2: p_n[m] \ge 0, \forall n \in N, \forall m \in M, \\
&\qquad C3: (x[1]-x0)^2 + (y[1]-y_0)^2 \le (V\delta)^2, \\
&\qquad C4: (x[m]-x[m-1])^2 + (y[m]-y[m-1])^2 \le (V\delta)^2, m = 2,...M, \\
&\qquad C5: (x_F - x[M])^2 + (y_F - y[M])^2 \le (V\delta)^2
\end{aligned} \tag{2.7}$$

Constraints C1 and C2 pertain to the power budget, while C3 to C5 relates to the spatial limitations as outlined in equation (2.4). The challenge in this optimization problem stems from its non-convex nature, caused by the interdependence of transmit power and trajectory variables. This complexity renders the problem unsolvable using conventional convex optimization methods.

2.4 Trajectory Optimization and Transmit Power

By incorporating a new variable s, the initial problem stated in equation (2.7) can be redefined as presented in references [29] and [32].

$$
\begin{aligned}
&\max_{\{x[m],y[m]\},\{p_n[m]\},s} \quad s \\
&\text{subject to } R_n \geq s, \forall n \in N, \\
&\qquad C1: \sum_{n=1}^{N}\sum_{m=1}^{M} p_n[m] \leq P_T, \\
&\qquad C2: p_n[m] \geq 0, \forall n \in N, \forall m \in M, \\
&\qquad C3: (x[1]-x0)^2 + (y[1]-y_0)^2 \leq (V\delta)^2, \\
&\qquad C4: (x[m]-x[m-1])^2 + (y[m]-y[m-1])^2 \leq (V\delta)^2, m = 2, ...M, \\
&\qquad C5: (x_F - x[M])^2 + (y_F - y[M])^2 \leq (V\delta)^2
\end{aligned}
\tag{2.8}
$$

Despite that equation (2.8) is still non-convex nature, it's noteworthy that R_n exhibits concavity with respect to the transmit power $p_n[m]$ when $g_n[m]$ is fixed. Additionally, a lower bound for R_n can be established when the transmit power is specified. Building on these insights, the approach initially tackles two separate subproblems: optimizing the transmit power with a predetermined trajectory, and optimizing the trajectory with a fixed transmit power. Subsequently, an integrated algorithm for optimizing both transmit power and trajectory is developed in the literature.

2.4.1 Transmit Power Optimization With Given Trajectory

When UAVs are deployed for particular tasks or services, such as aerial photography or cargo delivery, a third party may initiate the activation of service to GBSs. In these scenarios, the trajectory is predetermined. Given this fixed trajectory, represented by $\{x[m], y[m]\}, m = 1, ..., M$, the problem of optimizing transmit power is formulated as follows:

$$
\begin{aligned}
&\max_{\{p_n[m]\},s} \quad s \\
&\text{subject to } C1: \frac{1}{T}\sum_{m=1}^{M}\frac{B}{N}\log_2(1+\frac{Np_n[m]g_n[m]}{B\sigma^2}) \geq s, \forall n \in N, \\
&\qquad\qquad C2: \sum_{n=1}^{N}\sum_{m=1}^{M} p_n[m] \leq P_T, \\
&\qquad\qquad C3: p_n[m] \geq 0, \forall n \in N, \forall m \in M
\end{aligned}
\tag{2.9}
$$

This problem (2.9) falls within the realm of standard convex optimization, for which established algorithms, like the interior point method with a computational complexity of $O(N^3M^3)$, are applicable [30]. Additionally, by adhering to the guidelines in [33], an algorithm with reduced complexity can be devised.

2.4.2 Trajectory Optimization With Given Transmit Power

Given the constraints imposed by the UAV's hardware capabilities, the transmit power might be predetermined or fixed. Under these conditions, the problem of optimizing the UAV's trajectory, with the transmit power $\{p_n[m]\}$ set in advance, can be redefined as follows:

$$
\begin{aligned}
&\max_{\{x[m],y[m]\},s} \quad s \\
&\text{subject to } C1: \frac{1}{T}\sum_{n=1}^{N}\frac{B}{N}\log_2(1+\frac{Np_n[m]\beta_0}{B\sigma^2(x[m]-x_n)^2+(y[m]-y_n)^2+H^2}) \geq s, \forall n \in N, \\
&\qquad\qquad C2: (x[1]-x_0)^2+(y[1]-y_0)^2 \leq (V\delta)^2, \\
&\qquad\qquad C3: (x[m]-x[m-1])^2+(y[m]-y[m-1])^2 \leq (V\delta)^2, m=2,...M, \\
&\qquad\qquad C4: (x_F-x[M])^2+(y_F-y[M])^2 \leq (V\delta)^2
\end{aligned}
\tag{2.10}
$$

Given that constraint C1 is non-convex, an effective algorithm has been formulated, as per reference [31], by iteratively refining the objective using the lower bound of constraint C1.

Let the trajectory at the j-th iteration be represented by $\{x^j[m], y^j[m]\}$. The trajectory for the subsequent $j+1$-th iteration is denoted as $\{x^{j+1}[m], y^{j+1}[m]\}$, where $x^{j+1}[m] = x^j[m] + \Delta_x^j[m]$ and $y^{j+1}[m] = y^j[m] + \Delta_y^j[m]$. Here, $\Delta_x^j[m]$ and $\Delta_y^j[m]$ signify the adjustments made at the j-th iteration. Consequently, the rate R_n^{j+1} can be expressed as $R_n^{j+1} = \frac{1}{T}\sum_{m=1}^{M} \frac{B}{N} r_{n,m}^{j+1}$, where $r_{n,m}^{j+1}$ denotes the rate at the $j+1$-th iteration for the n-th GBS and the m-th time slot.

$$r_{n,m}^{j+1} = \log_2\left(1 + \gamma \frac{\beta_0}{d_{n,m}^j + f\left(\{\Delta_x^j[m], \Delta_y^j[m]\}\right)}\right) \tag{2.11}$$

where

$$\begin{aligned}
&\gamma = Np_n[m]/B\sigma^2, \\
&d_{n,m}^j = \left(x^j[m] - x_n\right)^2 + \left(y^j[m] - y_n\right)^2 + H^2, \\
&f\left(\{\Delta_x^j[m], \Delta_y^j[m]\}\right) = \Delta_x^j[m]^2 + \Delta_y^j[m]^2 + 2\left(x^j[m] - x_n\right)\Delta_x^j[m] + 2\left(y^j[m] - x_n\right)\Delta_y^j[m].
\end{aligned} \tag{2.12}$$

Given that the function $\log_2(1 + \frac{a}{b+x})$ exhibits convexity, it follows that

$$\log_2\left(1 + \frac{a}{b+x}\right) \geq \log_2\left(1 + \frac{a}{b}\right) - \frac{a}{\ln 2b(a+b)}x \tag{2.13}$$

which results from the first order condition of convex functions [30]. This further leads to

$$r_{n,m}^{j+1} \geq lbr_{n,m}^{j+1} = \log_2\left(1 + \gamma\frac{\beta_0}{d_{n,m}^j}\right) - \frac{\gamma\beta_0}{\ln 2 d_{n,m}^j\left(\gamma\beta_0 + d_{n,m}^j\right)} f\left(\{\Delta_x^j[m], \Delta_y^j[m]\}\right). \tag{2.14}$$

Starting with the trajectory $\{x_j[m], y_j[m]\}$ at the j-th iteration, the trajectory for the $j+1$-th iteration is determined by addressing the subsequent optimization problem:

$$\max_{\{\Delta_x^j[m],\Delta_y^j[m]\},s} \quad s$$

$$\text{subject to } C1: \frac{1}{T}\sum_{m=1}^{M}\frac{B}{N} lbr_{n,m}^{j+1} \geq s, \forall n \in N,$$

$$C2: (x^j[1] + \Delta_x^j[1] - x_0)^2 + (y^j[1] + \Delta_y^j[1] - y_0)^2 \leq (V\delta)^2, \tag{2.15}$$

$$C3: (x^j[n] + \Delta_x^j[n] - x^j[n-1] - \Delta_x^j[n-1])^2 +$$

$$(y^j[n] + \Delta_y^j[n] - y^j[n-1] - \Delta_y^j[n-1])^2 \leq (V\delta)^2, n = 2, ...N,$$

$$C4: (x_F - x^j[N] - \Delta_x^j[N])^2 + (y_F - y^j[N] - \Delta_y^j[N])^2 \leq (V\delta)^2$$

This constitutes a convex optimization problem that can be resolved through established convex optimization methods [30]. The optimization variables, representing the increments at each iteration, yield a sequence of non-decreasing values. However, these values are constrained to not exceed the optimal solution of problem (2.10), ensuring that convergence is assured.

2.5 Simulation Results

In this section, we employ CVX [17], [34], a software package for convex optimization referenced in [30], to address the convex optimization problem at hand. CVX is specifically designed for solving convex problems efficiently. The simulations were conducted using this technique, and for clarity, the environment setup parameters governing these simulations are detailed in Table 2.1. This table offers a detailed summary of the simulation parameters, elucidating the setup used to both illustrate the efficacy of the proposed approach and to tackle the convex optimization challenge presented.

For the initial and final locations specified in Table 2.1, we examine two scenarios regarding the positioning of the Ground Base Stations (GBSs). In Figure 2.2, showcases the UAV's flight path, initiating from a starting point and culminating at a designated endpoint.

Table 2.1: Parameters for UAV Simulation Analysis

Parameters	**Parameter Description**	**Values**
H	The fix height of the UAV	$100\ m$
(x_0, y_0, H)	Initial location of the UAV	$(55\ m, 83\ m, 100)$
(x_F, y_F, H)	Final Location of the UAV	$(1945\ m, 83\ m, 100)$
σ^2	The unit bandwidth	$-169\ dBm/Hz$
V	UAV speed	$100\ m/s$
T	Time	$50\ sec$
P_T	Transmit Power	$5\ W$
M	The number of discrete points	50
δ	The time slot length	$1\ sec$
β_0	The channel power gain	10^{-3}

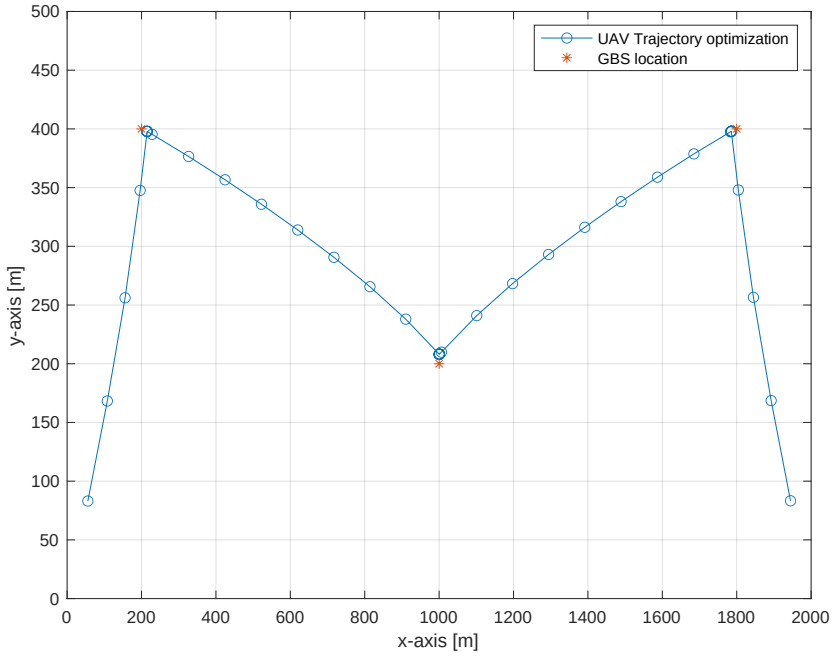


Figure 2.2: The UAV Trajectory Optimization case I

Additionally, the Ground Base Stations (GBSs) are strategically positioned at three distinct coordinates: $(200, 400, 0)$, $(1000, 200, 0)$, and $(1800, 400, 0)$. The depicted optimized trajectory thoughtfully includes all GBS locations, ensuring comprehensive coverage. Notably, this particular flight route offers a significant benefit: it affords the UAV ample opportunity to hover over each GBS, facilitating thorough data exchange or surveillance before proceeding to the subsequent station. This aspect of the trajectory underscores its efficiency and strategic

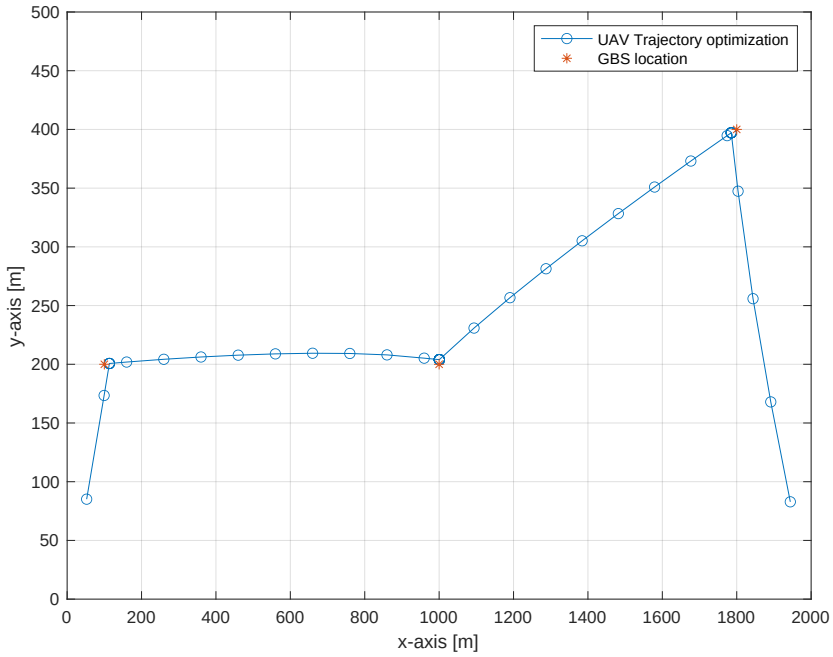


Figure 2.3: The UAV Trajectory Optimization case II

Table 2.2: Ground Base Stations (GBSs) coordinates for each scenario

	Parameters	**Coordinates Value** (x, y, z)
Case I	GBS_1	$(200\ m, 400\ m, 0)$
	GBS_2	$(1000\ m, 200\ m, 0)$
	GBS_3	$(1800\ m, 400\ m, 0)$
Case II	GBS_1	$(100\ m, 200\ m, 0)$
	GBS_2	$(1000\ m, 200\ m, 0)$
	GBS_3	$(1800\ m, 400\ m, 0)$

trajectory planning in maximizing the UAV's operational effectiveness over the GBSs.

Similarly, Figure 2.3, depicts the UAV's optimized flight path in case II, which includes visits to Ground Base Stations (GBSs) placed at fixed location $(100m, 200m, 0)$, $(1000m, 200m, 0)$, and $(1800m, 400m, 0)$, respectively. The UAV embarks on its route from the starting point, navigating through each GBS en route to its final destination. In addition, observations from 2.3 reveal that the GBSs are positioned at distinct locations. Despite this, the UAV's optimized trajectory ensures it passes over each GBS, demonstrating the ef-

fectiveness of the trajectory planning in accommodating the varied positions of the GBSs.

2.6 Conclusion

In this chapter, we investigate the trajectory optimization of a UAV by transforming a non-convex optimization challenge into a convex optimization problem, a process that includes the introduction of an auxiliary variable, s. We then leverage the CVX optimization framework to validate the approach, effectively mapping out the UAV's path as it traverses the strategically positioned Ground Base Stations (GBSs). This methodology not only showcases the practical implementation of convex optimization strategies in UAV route planning but also emphasizes the effectiveness of the CVX tool in both visualizing the optimized flight path and ensuring its compliance with the predetermined GBS coordinates.

Chapter 3

Designing 3D Antenna Patterns for UAV-Enabled Wireless Connectivity

3.1 Introduction

Drones, also known as Unmanned Aerial Vehicles (UAVs), have captured widespread interest in recent times, thanks to their vast array of promising uses. Their application spans across military, commercial, and public safety sectors, encompassing tasks such as surveillance, delivery services, drone taxis, live video feeds, and search and rescue operations [35]. However, to unlock the full potential of these emerging applications, establishing reliable wireless connectivity for UAVs in beyond-visual-line-of-sight (BVLOS) conditions is essential. This objective can be met by integrating UAVs with cellular networks (Cellular-Connected UAVs or C-UAVs), facilitating uninterrupted communication and data transfer between the UAVs and ground base stations (BS) [36], [37].

For the effective deployment of Cellular-Connected UAVs (C-UAVs) within existing terrestrial networks, a thorough understanding of the distinct air-to-ground signal propagation characteristics is essential. Specifically, the radio propagation model for C-UAVs is influenced by two primary factors: 1) the dependency of antenna radiation patterns on the elevation

angle, and 2) the pronounced impact of ground reflections. In traditional ground-to-ground wireless communications, the altitudes of the transmitter (Tx) and receiver (Rx) are typically constant and comparable, allowing for a simplified 2D modeling of radio propagation. However, the introduction of 3D spatial considerations in air-to-ground C-UAV scenarios necessitates a more detailed examination of 3D antenna patterns and ground reflection effects [19]. Beyond influencing wireless coverage, the air-to-ground propagation traits of Cellular-Connected UAVs (C-UAVs) play a vital role in determining the accuracy of 3D wireless localization involving C-UAVs. The ability to swiftly and precisely pinpoint signal origins using UAVs is crucial across a range of applications in commercial, public safety, and military contexts [38].

Recent studies have delved into UAV air-to-ground propagation models, taking into account the influences of ground reflection and three-dimensional antenna radiation patterns. For instance, research documented in [39] utilized flight measurement datasets to characterize air-to-ground channels, finding that the two-ray path loss model, which accounts for ground reflection, offers a more precise representation of air-to-ground signal data. Another study in [40] assessed UAV air-to-ground channels in open rural settings with various antenna orientations, uncovering a significant reliance of received signal strength on the elevation angle of the antenna pattern. Research presented in [41] explored the additional path loss in cellular-to-UAV channels attributable to 3D antenna patterns. Furthermore, the study in [42] examined how a UAV's structure, along with the positioning and alignment of antennas, affects the azimuth antenna pattern and polarization properties, utilizing an anechoic chamber for antenna pattern assessments and conducting field tests through UAV-to-UAV and ground-to-UAV configurations.

The study in [43] analyzed the effects of 3D antenna radiation patterns on the accuracy of time difference of arrival (TDOA)-based three-dimensional localization of UAVs within a terrestrial wireless network. The findings indicate that antenna patterns play a crucial role in determining the precision of UAV localization.

In this chapter, we delve into the influence of three-dimensional antenna patterns and ground reflections on the path loss models for air-to-ground communication involving Cellular-Connected UAVs (C-UAVs). We provide a detailed examination of the UAV's air-to-ground propagation model, highlighting how these factors affect signal transmission. Additionally, we explore how the path loss varies with altitude across different environmental conditions, offering insights into the complex interplay between UAV altitude, antenna design, and the surrounding landscape on communication efficacy. This comprehensive analysis aims to enhance our understanding of the critical parameters shaping UAV communication systems in diverse settings.

3.2 UAV Propagation Model

The likelihood of establishing line-of-sight (LoS) connections predominantly influences interactions between UAVs and ground-based entities (such as ground base stations and mobile devices). In such scenarios, the Free Space Loss (FSL) model is applicable for calculating average path loss. Additionally, it's essential to account for extra path loss caused by the shadowing effects of buildings in Non-Line-of-Sight (NLoS) connections. In the context of High Altitude Platforms (HAPs) like UAVs, especially for mobile applications in urban environments, realistic elevation angles usually span from 60 to 90 degrees. This positioning places the HAP directly above the mobile terminal, optimizing the line-of-sight and enhancing connectivity within densely built-up areas. However, lower elevation angles are also relevant, particularly in contexts such as interference analysis or other specialized studies. For example, at a 5-degree elevation angle, the distance from a user to a point directly beneath the HAP on the ground spans approximately 211 km at an altitude of 22 km (factoring in Earth's curvature) and about 168 km at an altitude of 17 km [18].

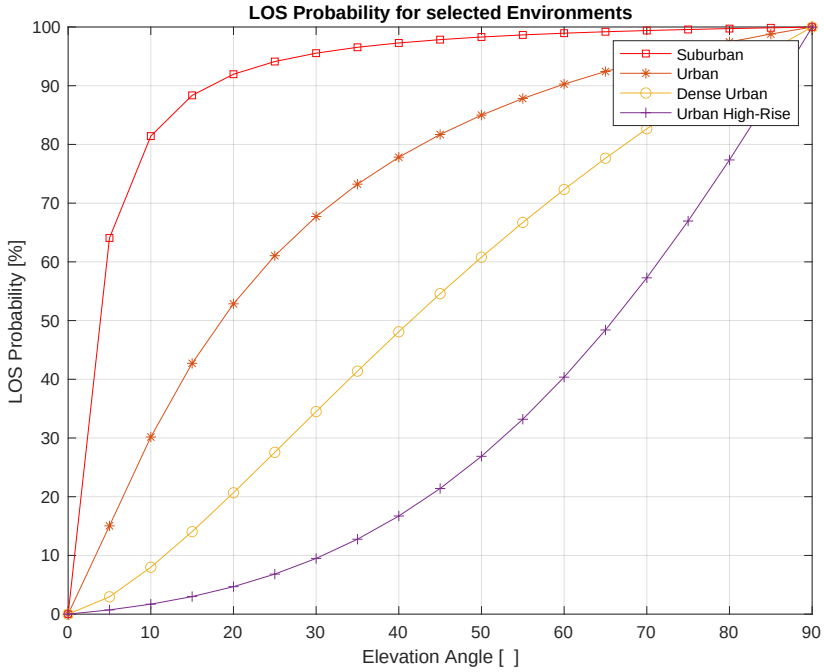


Figure 3.1: LOS probability in the ground as a function of the elevation angle for selected environments

3.2.1 LOS Probability of the UAV

The probability of Line-of-Sight (LoS) occurrences within ground-level environments, as influenced by the elevation angle, was determined for four distinct settings, as illustrated in Figure 3.1. As demonstrated in [18], a precise function was developed to accurately align with the simulation results presented in Figure 3.1.

$$P_{LOS}(\theta) = A - \frac{A - B}{1 + (\frac{\theta - C}{D})^E} \tag{3.1}$$

where P_{LOS} is the probability of Line-of-Sight (LoS), expressed as a percentage, is a function of the elevation angle θ measured in degrees, with A, B, C, and D representing empirical parameters specific to four typical environments, as detailed in Table 3.1. Additionally, parameters characterizing an environment defined by arbitrary values of α, β, and γ in accordance with the ITU-R Rec. P. 1410 statistical model can also be readily deduced from

the simulation outcomes [44].

Table 3.1: Parameters for LOS Probability

Environment	**A**	**B**	**C**	**D**	**E**
Suburban	101.6	0	0	3.25	1.241
Urban	120	0	0	24.3	1.229
Dense Urban	187.3	0	0	82.1	1.478
Urban High-Rise	352	-1.37	-53	173.8	4.67

3.2.2 Shadowing Loss of the UAV

This section delves into the effects of building-induced shadowing on Non-Line-of-Sight (NLOS) connections. A notable advantage of using UAVs as high altitude aerial stations over traditional satellites is their relatively shorter path length. This characteristic significantly enhances the feasibility of establishing NLOS links between mobile stations and the UAVs, thereby improving connectivity in urban environments where direct line-of-sight may be obstructed. Figure 3.2 presents a normalized histogram showcasing the simulation outcomes, specifically the additional rooftop diffraction loss at 2.0 GHz for vertical polarization with an elevation angle of 70 degrees. From the figure, a normal distribution pattern is discernible. Additionally, the Probability Density Function (PDF) corresponding to the normal distribution, which has been fitted to the simulated data, is depicted in Figure 3.2. The expression for the PDF of the normal distribution is as follows [18]:

$$p_n(x) = \frac{1}{\sigma\sqrt{2\pi}} exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \tag{3.2}$$

where p_n is normalized probability, μ the mean value in dB, and σ the standard deviation in dB.

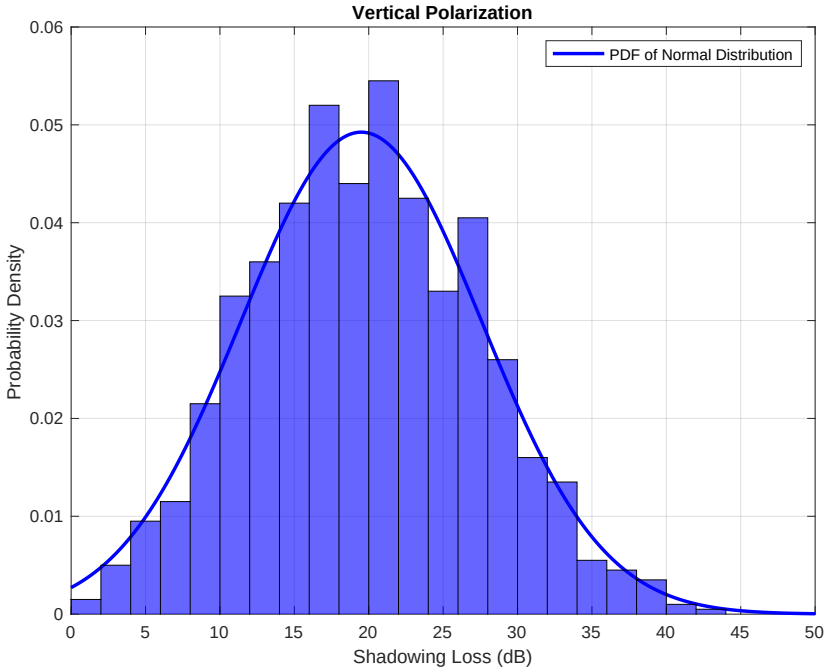


Figure 3.2: Normalized histogram and PDF of shadowing loss at 2.0 GHz for vertical polarization in a dense urban area

3.3 Modeling Air-to-Ground Path Loss of the UAV

In this section, we incorporate path loss models and three-dimensional antenna patterns to examine and model the received signal strength. The expression for received signal strength can be articulated as follows:

$$R = P_{Tx} - PL + \sigma \tag{3.3}$$

where P_{Tx}, PL and σ denote the transmit power, the path loss, and the shadowing component, respectively.

3.3.1 UAV Path Loss Model

To depict the air-to-ground communication channel in rural settings, we utilize the two-ray path loss model, which describes the interaction between a Ground Base Station (GBS) tower and a UAV. This model accounts for both the direct line-of-sight (LoS) path and a

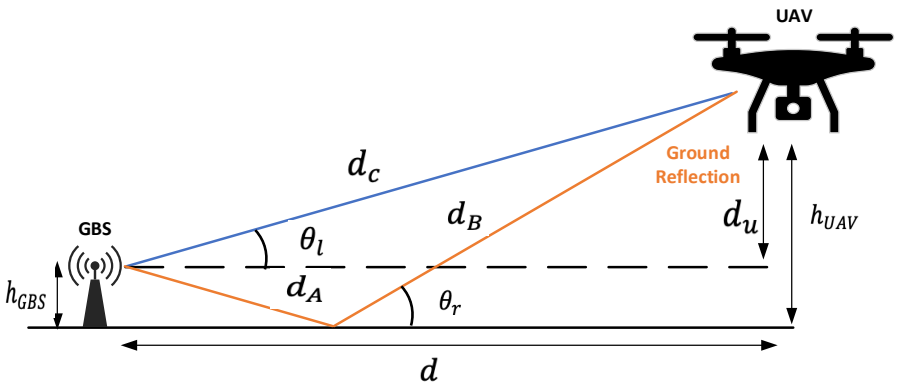


Figure 3.3: The two-ray ground reflection model of the UAV

significant ground-reflected path, each playing a role in the signal received by the UAV. The path loss as defined by this two-ray ground reflection model is formulated as follows [45]:

$$PL_{2r} = \left(\frac{\lambda}{4\pi}\right)^2 \times \left| \frac{\sqrt{G_{Tx}(\phi_l,\theta_l)G_{Rx}(\phi_l,\theta_l)}}{d_c} + \frac{\Gamma(\theta_r)\sqrt{G_{Tx}(\phi_r,\theta_r)G_{Rx}(\phi_r,\theta_r)}e^{-j\Delta\tau}}{d_a+d_b} \right|^2 \quad (3.4)$$

where $G_{Tx}(\phi,\theta)$, $G_{Rx}(\phi,\theta)$ denote the antenna gain of the transmitter and a receiver from 3D antenna radiation pattern depending on azimuth ϕ and elevation θ angles, λ, $\theta_r = \tan^{-1}\left(\frac{h_{GBS}+h_{UAV}}{d}\right)$ indicate wave-length and the ground reflection angle, and $\Delta\tau = \frac{2\pi(d_a+d_b+d_c)}{\lambda}$ indicates the phase difference of two paths at the UAV. In the two-ray ground reflection model, the parameters for distance and angle are depicted in Figure 3.3. The reflection coefficient for a vertically polarized signal off the ground can be characterized as follows:

$$\Gamma(\theta_r) = \frac{\epsilon_0 \sin\theta_r - \sqrt{\epsilon_0 - \cos^2\theta_r}}{\epsilon_0 \sin\theta_r + \sqrt{\epsilon_0 - \cos^2\theta_r}} \quad (3.5)$$

where ϵ_0 is the relative permittivity of the ground, which can be varied depending on the ground condition. By incorporating the Line-of-Sight (LoS) component within the two-ray

path loss framework, we derive the free-space path loss model, which is expressed as follows:

$$PL_{FS} = \left(\frac{\lambda}{4\pi}\right)^2 \left| \frac{\sqrt{G_{Tx}(\phi_l, \theta_l) G_{Rx}(\phi_l, \theta_l)}}{d_c} \right|^2 \tag{3.6}$$

3.3.2 UAV 3D Antenna Radiation Pattern

In this section, we delve into the significance of precise 3D antenna radiation patterns for UAV air-to-ground propagation models. Terrestrial networks often assume isotropic antenna gains, effectively representing the influence of omnidirectional antenna patterns within the azimuth angle domain. However, this method may not account for the variation in antenna gain with elevation angles, which is crucial in the 3D structure of air-to-ground networks.

To examine the effects of various 3D antenna patterns, we explore a theoretical dipole antenna pattern. The radiation pattern of a dipole antenna is characterized by the normalized antenna field pattern, denoted as L. When the dipole antenna is oriented along the z-axis, its radiation pattern exhibits omnidirectional behavior with respect to the azimuth angle (ϕ). The expression for the normalized antenna field pattern for a dipole antenna positioned on the z-axis is given as follows [46], [47]:

$$L_z(\theta) = \frac{\cos\left(\frac{\pi l_0 d_{len}}{c} \cos\theta\right) - \cos\left(\frac{\pi l_0 d_{len}}{c}\right)}{\sin\theta} \tag{3.7}$$

where d_{len}, c, l_0 denote the length of dipole antenna, the speed of light, and the carrier frequency, respectively. Assuming a half-wavelength dipole antenna, where the antenna length (d_{len}) equals half the wavelength ($\lambda/2$), the relationship $\frac{\pi f_0 d_{\text{len}}}{c} = \frac{\pi}{2}$ is satisfied. Under this condition, equation (3.7) can be reformulated as follows [48]:

$$L_z(\theta) = \frac{\cos(\frac{\pi}{2}\cos\theta)}{\sin\theta}. \tag{3.8}$$

Positioning the dipole antenna along the y-axis, the angle between the antenna's orientation

and the direction of signal propagation is determined by $\cos^{-1}(\hat{s} \cdot \hat{y}) = \cos^{-1}(\sin(\theta)\sin(\phi))$, where $\hat{s}$ and $\hat{y}$ represent the unit vectors of the signal and the y-axis, respectively. Consequently, the normalized antenna field pattern for a dipole antenna aligned with the y-axis can be expressed as follows [48]:

$$L_y(\theta, \phi) = \frac{\cos\left(\frac{\pi}{2}\cos\left(\cos^{-1}(\sin(\theta)\sin(\phi))\right)\right)}{\sin\left(\cos^{-1}(\sin(\theta)\sin(\phi))\right)}. \tag{3.9}$$

In this expression, θ represents the elevation angle, and ϕ denotes the azimuth angle. The equation captures how the antenna's response varies with these angles, illustrating the directional characteristics of the antenna's radiation pattern. In addition, it is important to recognize that the antenna's field pattern along the y-axis is influenced by both the azimuth angle (ϕ) and the elevation angle (θ). This implies that adjustments to either the azimuth or elevation angle can result in variations in the antenna's gain. Figure 3.4 displays the dipole antenna pattern aligned along the z-axis which is derived from the analytical expression in equation (3.8), showcasing the distinctive donut shape that is emblematic of a standard dipole antenna. Similarly, the normalized field patterns for dipole antennas aligned along the y-axis, as derived from equations (3.9), are depicted in Figure 3.5 using Cartesian coordinates.

3.4 Conclusion

In this chapter, we consider a narrowband elevation-dependent shadowing model specifically devised for mobile systems operated by High Altitude Platforms (HAPs), such as UAVs, within urban settings. This model, which is applicable in the 2–6 GHz frequency spectrum, is pertinent to the infrastructure of mobile networks. It meticulously assesses the probability of establishing Line-of-Sight (LoS) connections between HAPs and ground-based mobile stations, and also quantifies the additional path loss due to shadowing in Non-Line-of-Sight (NLoS) scenarios, with a particular focus on the impact of elevation angles. The model fur-

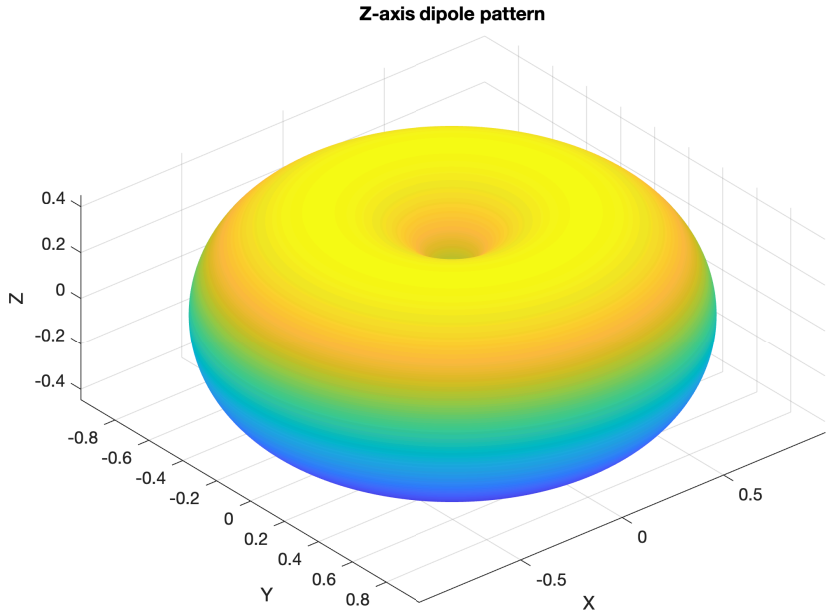


Figure 3.4: The 3D dipole antenna pattern along Z-axis coordinate

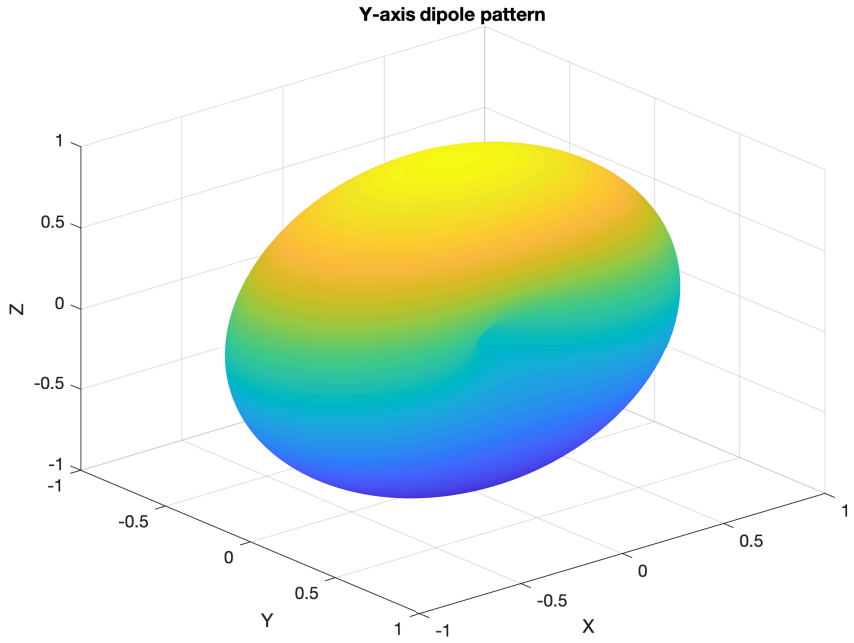


Figure 3.5: The 3D dipole antenna pattern along Y-axis coordinate

ther stratifies the LoS probabilities across a spectrum of urban environments, from the less dense suburban areas to the highly congested high-rise urban centers, providing a comprehensive understanding of connectivity dynamics in diverse urban landscapes. Moreover, this work delves into the development and scrutiny of an interference mitigation technique tailored for heterogeneous aerial and terrestrial IoT networks, which are distinguished by their utilization of straightforward wireless communication technologies. Central to this strategy is the innovative deployment of a cross-dipole antenna setup at the transmission point, which adeptly switches between the z-axis and y-axis dipole antennas contingent upon the receiver's characteristics. An in-depth exploration of the 3D channel model, which integrates the intricate 3D radiation patterns of the dipole antennas and the geographical positioning of IoT devices, substantiates the enhanced efficacy of the y-axis dipole antenna for servicing aerial-based receivers, thereby outperforming the traditional z-axis configuration. This nuanced approach not only augments the performance of aerial receivers but also contributes significantly to the optimization of network efficiency in complex urban IoT ecosystems.

Chapter 4

Antenna Pattern Aware UAV Trajectory Planning Using Artificial Potential Field

4.1 Introduction

Recently, unmanned aerial vehicles (UAVs) have attracted much interest in both academia and industry. UAVs have a wide range of commercial, civilian, and military applications. Indeed, the new technological advances in autonomous drones have led to numerous beneficial applications, e.g., in food delivery and humanitarian aid during disasters [49]. In wireless communication systems, UAVs can also provide significant improvements to the existing terrestrial communication infrastructure. Additionally, they can assist the 5G and beyond wireless applications [50]. Also, UAVs can be quickly deployed to support the cellular networks and enhance the quality of service (QoS) [51]. In many cases, QoS is strongly dependent on the location of a UAV determined by taking into account the ground users and the number of base stations.

The optimal trajectory design of a UAV becomes a key challenge to provide the best

wireless connectivity for ground users. Therefore, many studies in the literature have addressed the trajectory design of UAVs. Finding the optimal position for UAVs to maximize the throughput was studied in [52]. The authors of [2] considered the entire trajectory of multiple UAVs to jointly optimize scheduling and user association. In [53], the 3D placement of a single UAV and the base station, maximizing the number of covered users, and minimizing the transmit power was considered. In the same direction, the authors of [25] studied the optimal 3D deployment of multiple UAVs, maximizing the total coverage area of the ground users. In addition to designing the UAV's trajectory for its ability to be considered as an aerial base station, the authors of [54] studied the cellular-enabled UAV communication system, in which a UAV flies from an initial to a final location via the shortest path determined by applying graph theoretical tools.

One approach in UAV path planning is to use artificial potential field (APF) algorithms. The APF method is a virtual force method that was first introduced by Khatib in [20]. It is developed to avoid collisions among multiple real-time robots operating in a complex environment [20]. Recently, multiple studies have been published in the literature on UAV path planning using APF. For instance, in [55], the authors developed dynamic APF path planning for multirotor UAVs for following a ground moving target. Also, the optimized APF for multi-UAV operation in 3-D dynamic space was studied in [56]. In [57], the authors introduced and evaluated the artificial potential field approach with simulated annealing (SA) which has been applied to local and global path planning. However, the artificial potential field algorithm in UAV path planning and trajectory design depends on distance calculations at each step the UAV makes in the system. Additionally, the initial and final locations of UAVs are predefined, and coordination between agents is required for collision avoidance.

As also noted above, numerous studies have considered the applications of APF and the implementations on robots and to a limited extent on UAVs. To the best of our knowledge, prior work has not taken into account the impact of antenna patterns on the UAV trajec-

tory when using the APF algorithm. With this motivation, this work focuses primarily on improving and implementing an APF-based algorithm for single-UAV and multiple UAV trajectory designs while taking into account antenna radiation patterns, connectivity requirements, and collision avoidance constraints. We implement and simulate circular regions for UAVs to maintain the connectivity constraint, which is ensured by having a sufficiently large signal-to-noise ratio (SNR) between the UAV and the nearest ground base station. Additionally, we show the impact of adding 3D antenna patterns on the trajectory design of the UAV. The algorithm chooses the shortest path for the UAV to reach its final destination. We consider the UAV collision avoidance and obstacle avoidance in the entire system, where UAVs avoid hitting each other while at the same time avoiding the fixed obstacles. The critical part of the enhanced-APF algorithm finds the appropriate values for the parameters such as UAV altitude, the threshold, attraction and repulsion gain coefficients, etc. Simulation results demonstrate the impact of the antenna pattern on the UAV trajectory using the enhanced-APF algorithm.

4.2 System Model

In this chapter, we consider a graphical area with a $3D$ Cartesian coordinate system, where the horizontal coordinate of ground base station (GBS) k is fixed at $W_k = [x_k, y_k]$. All UAVs are assumed to fly at an altitude of H_u above the ground, and the time-varying horizontal coordinate of the UAV at time instant t is denoted by $\mathbf{Z_u} = [x_u(t), y_u(t)]$. In this model, we assume that each UAV starts from a fixed initial location $\mathbf{Z_s} = [x_s, y_s]$, and aims to reach a target $\mathbf{Z_g} = [x_g, y_g]$. Also, we assume that the fixed obstacles are randomly distributed and the location of the obstacle j is denoted by $\mathbf{Z_o} = [x_j, y_j]$. It is worth noting that obstacles are assumed to have an altitude closer to the UAVs' altitude. Figure 4.1 illustrates the system model for UAV trajectory design.

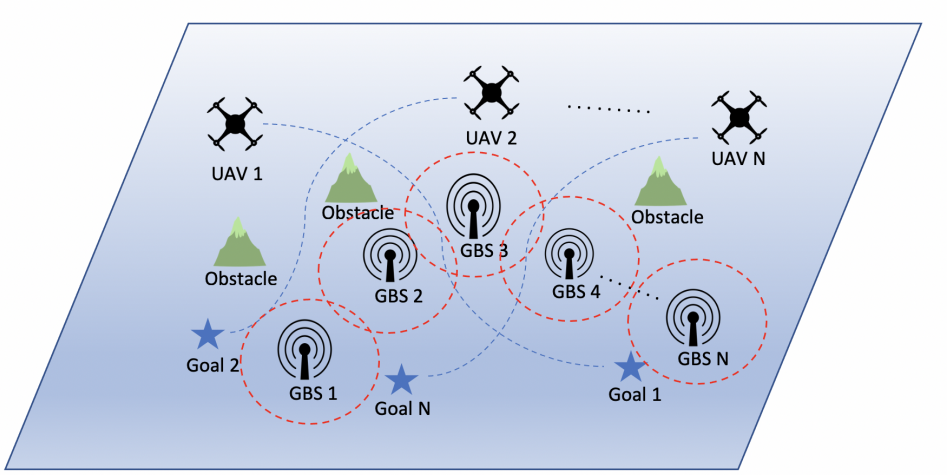


Figure 4.1: UAVs trajectory design system model.

4.2.1 Channel Model between UAVs and GBSs

The communication link between a UAV and the k^{th} GBS is typically dominated by line-of-sight (LOS) [10]. Assuming that all GBS locations are known, the distance from the i^{th} UAV to the k^{th} GBS at time t is given by

$$d_k(t) = \sqrt{H_u^2 + (x_i(t) - x_k)^2 + (y_i(t) - y_k)^2}. \tag{4.1}$$

Similarly, the distance from the i^{th} UAV to the j^{th} obstacles at time t is given by

$$d_j(t) = \sqrt{H_u^2 + (x_i(t) - x_j)^2 + (y_i(t) - y_j)^2}. \tag{4.2}$$

4.2.2 3D Antenna Patterns for UAVs

In this section, we define the types of antenna patterns. Each UAV can follow and connect with its nearest GBS. The antenna patterns of the UAV can be determined by the gain in the vertical and horizontal planes. We consider the following two types of UAV antenna patterns [58]:

Sine Pattern

When the UAV is equipped with horizontally oriented directional antenna, the horizontal pattern as a function of elevation angle θ can be expressed as

$$\sin(\theta) = \frac{H_u}{\sqrt{H_u^2 + x_u^2}} \tag{4.3}$$

where $x_u^2 = (x_i(t) - x_k)^2 + (y_i(t) - y_k)^2$ is the distance from the UAV to the nearest GBS impacted by the directional antenna. From (5) the maximum antenna gain of the UAV is experienced when $\sin(\theta) = 1$ that occurs when the UAV is right above the GBS.

Cosine Pattern

When the UAV is equipped with vertically oriented directional antenna, the vertical pattern as a function of elevation angle θ can be expressed as

$$\cos(\theta) = \frac{x_u}{\sqrt{H_u^2 + x_u^2}}. \tag{4.4}$$

From 4.5, we note that the directional antenna is tilting down to give a cone-shaped radiation lobe directly beneath the UAV. Considering similar sine and cosine patterns at the base station, we can express the overall antenna gain in the links as

$$G_s(x) = \sin(\theta)\sin(\theta) \tag{4.5}$$

$$G_c(x) = \cos(\theta)\cos(\theta) \tag{4.6}$$

where $G_s(x)$ and $G_c(x)$ are the antenna gains in the horizontal and vertical orientation, respectively. At time t, each UAV connects to its nearest GBS, providing the best signal-to-

noise ratio (SNR), which can be expressed as

$$SNR_s = \frac{P_T G_s(x)}{d_k^2(t)}, \forall t \tag{4.7}$$

$$SNR_c = \frac{P_T G_c(x)}{d_k^2(t)}, \forall t \tag{4.8}$$

where P_T denotes the transmit power.

4.3 Basic Analysis of Artificial Potential Field Algorithm

The artificial potential field (APF) approach provides a simple and effective motion planning method for unmanned vehicles. Also, it is used for robotic collision avoidance because of its simple and effective structure. Therefore, it is a frequently used technique for trajectory planning design. Additionally, this algorithm generates a real-time trajectory for single or multiple agents. Indeed, the APF algorithm can transfer all the information about the environment, such as obstacles, final location, and other agents. However, in some complex environments, the algorithm needs some improvements and modifications accordingly [56].

In [20], Khatib first introduced the artificial potential algorithm to the robot obstacle avoidance and trajectory planning. The basic idea behind this algorithm is that the agent moves in a field of forces.

In Khatib's algorithm, UAVs and obstacles are treated as objects inside a two-dimensional space. These obstacles have a repulsion effect on the UAV that varies inversely proportional to the distance. In other words, if the UAV gets closer to the obstacles, the repulsion force will be greater. And the attraction force will be greater when the UAV gets closer to its final destination. The potential energy of a location near a target is low, while the potential energy near an obstacle is high. The obstacles are distributed randomly, while the initial

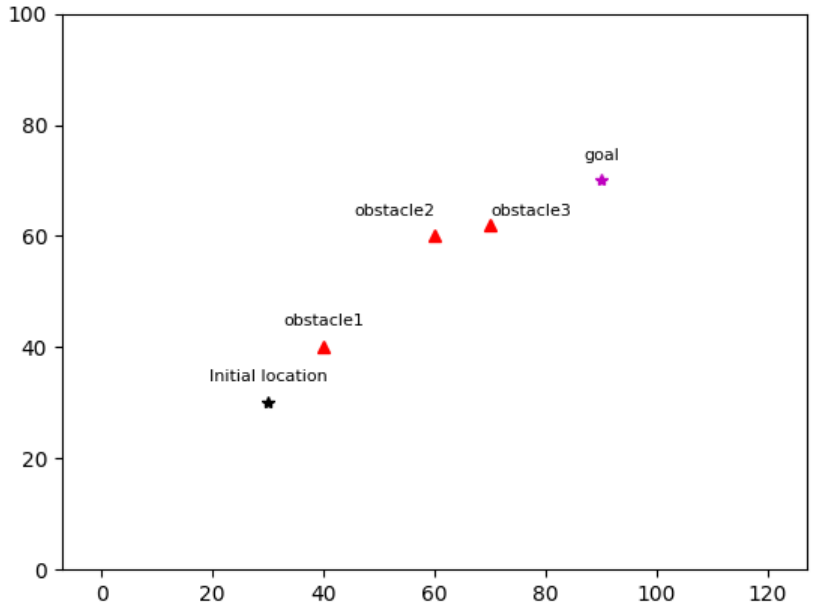


Figure 4.2: The original map of the traditional artificial potential field.

and final locations are located in a fixed position, as shown in Figure 4.2.

Khatib considered collision avoidance with a single obstacle. The attractive potential field function and repulsive potential function can be expressed as [56]

$$U_{tot}(\mathbf{Z}) = U_{rep}(\mathbf{Z}) + U_{att}(\mathbf{Z}) \tag{4.9}$$

where $U_{tot}(\mathbf{Z})$ is the total potential field, $U_{rep}(\mathbf{Z})$ is the repulsive potential field, and $U_{att}(\mathbf{Z})$ is the gravitational potential field.

The gravitational potential field can be defined as

$$U_{att}(\mathbf{Z}) = q_{att}\frac{(\mathbf{Z} - \mathbf{Z_g})^2}{2} \tag{4.10}$$

where $\mathbf{Z_g}$ is coordinate of the goal. $\mathbf{Z} = [x(t), y(t)]^T \ \forall t$ is coordinate position of the agent. q_{att} is the attractive force gain coefficient.

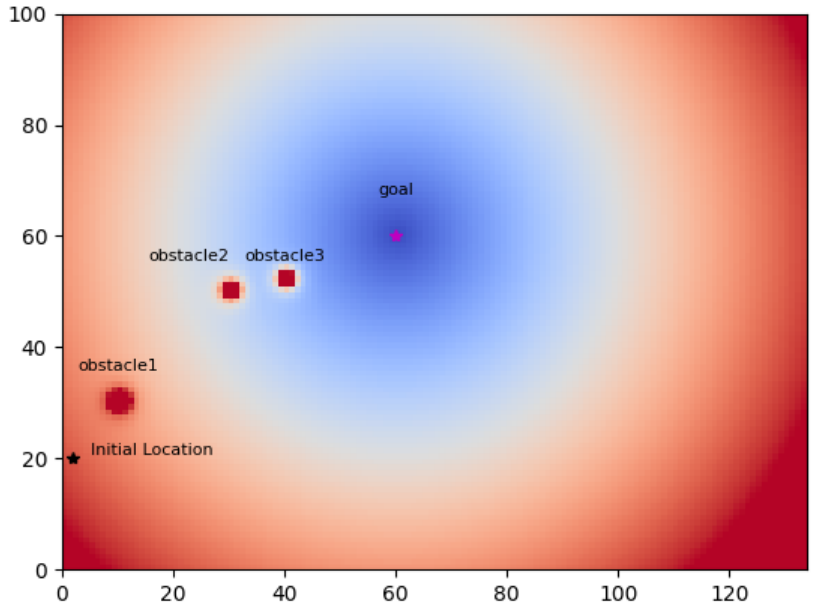


Figure 4.3: The original map of the traditional artificial potential field.

The repulsive potential field of the traditional artificial potential field is defined as

$$U_{rep}(\mathbf{Z}) = \begin{cases} \frac{q_{rep}}{2}\left(\frac{1}{\mathbf{Z}-\mathbf{Z_0}} - \frac{1}{\mathbf{p_0}}\right)^2, & \mathbf{Z}-\mathbf{Z_0} \leq \mathbf{p_0} \\ 0 & \mathbf{Z}-\mathbf{Z_0} > \mathbf{p_0}. \end{cases} \tag{4.11}$$

$U_{rep}(\mathbf{Z})$ is the repulsive force in position $\mathbf{Z}$, q_{rep} is repulsive force gain coefficient, $\mathbf{Z}-\mathbf{Z_0}$ is the distance from the obstacle $\mathbf{Z_0}$, and $\mathbf{p_0}$ is the range of repulsive field of the obstacles.

In (4.11), when the final destination is farther away from the UAV, both the gravitational potential energy and attraction function to UAV are greater. On the other hand, when UAV is at the final destination, the gravitational potential energy is 0. The heat map of the traditional potential energy is shown in Figure 4.3. The potential field transforms gradually at the position away from the target point, but the potential field disappears rapidly in the position near to the target point.

The corresponding attractive force function $F_{att}(\mathbf{Z})$ is described as the negative gradient

expressed as follows:

$$F_{att}(\mathbf{Z}) = -\nabla U_{att}(\mathbf{Z}) = -q_{att}|\mathbf{Z} - \mathbf{Z_g}|. \tag{4.12}$$

The repulsion force function $F_{rep}(\mathbf{Z})$ is described as the negative gradient of the repulsive potential field as follows:

$$F_{rep}(\mathbf{Z}) = -\nabla[U_{rep}(\mathbf{Z})] = \begin{cases} q_{rep}(\frac{1}{\mathbf{Z}-\mathbf{Z_0}} - \frac{1}{\mathbf{p_0}})\frac{1}{(\mathbf{Z}-\mathbf{Z_0})^2}, & \mathbf{Z} - \mathbf{Z_0} \leq \mathbf{p_0} \\ 0, & \mathbf{Z} - \mathbf{Z_0} > \mathbf{p_0} \end{cases} \tag{4.13}$$

In (4.13), no repulsion function will be generated when obstacle is out of the influence range of the UAV.

The total force $F_{\mathbf{Z}}$ at position $\mathbf{Z}$ is calculated by superimposing the potential forces of both obstacles and targets as follows:

$$F_{\mathbf{Z}} = \sum_{l=1}^{t} F_{att}(l) + \sum_{r=1}^{i} F_{rep}(r). \tag{4.14}$$

The traditional algorithm of the artificial potential field has advantages in applications involving real-time path planning for UAVs. In some cases, the APF algorithm has a local point, and this creates a problem in reaching some targets located in narrow regions. Specifically, this issue can appear in a more complex environment where many goals and obstacles are deployed. The agent will stop at the local point between the goals without reaching the final destination.

4.4 Enhanced Artificial Potential Field Algorithm

4.4.1 Enhanced-APF Algorithm for Single Agent UAV

In this section, we consider a single UAV moving toward the target point in 3D space. Also, we assume a simple environment with one goal and multiple obstacles. To overcome the problem with the local minimum point, we adopt the same approach in [59] and include

additional attractive potential field and modify the potential field to guarantee that the UAV avoids stopping between the obstacles and the target. The UAV flies in the horizontal axis of the space and its 2D position is $\mathbf{Z}_u = [x_u(t), y_u(t)]^T \forall t$. The target is fixed at $\mathbf{Z}_g = [x_g, y_g]^T$ Thus, the definition of the single UAV attractive potential function is given by

$$U_{att}(\mathbf{Z}_u) = q_{att}\frac{(\mathbf{Z}_u - \mathbf{Z_g})^2}{2}. \tag{4.15}$$

The single UAV case is similar to the attractive potential function of the traditional APF. The attractive force of the UAV $F_{att}(\mathbf{Z}_u)$ is the negative gradient of the attractive potential function given as

$$F_{att}(\mathbf{Z}_u) = -\nabla U_{att}(\mathbf{Z}_u) = -q_{att}(\mathbf{Z}_u\mathbf{Z_g}). \tag{4.16}$$

The additional field function helps the UAV to avoid the local minimum point by pulling it toward the target. The additional field force $U_{add}(\mathbf{Z}_u)$ is given by [59]

$$U_{add}(\mathbf{Z}_u) = \begin{cases} \frac{q_{add}}{2}\Big[(\mathbf{Z_u} - \mathbf{Z_g}) - \mathbf{p_{add}}\Big]^2, & \mathbf{Z_u} - \mathbf{Z_g} \leq \mathbf{p_{add}} \\ 0, & \mathbf{Z_u} - \mathbf{Z_g} > \mathbf{p_{add}} \end{cases} \tag{4.17}$$

where q_{add} is the additional field coefficient, $\mathbf{Z_u} - \mathbf{Z_g}$ is the distance between the UAV and the goal, $\mathbf{p_{add}}$ is the impact of the field on the distance between the UAV and the goal.

The additional field force $F_{add}(\mathbf{Z}_u)$ is represented as follows:

$$F_{add}(\mathbf{Z_u}) = -\nabla[U_{add}(\mathbf{Z_u})] = \begin{cases} q_{add}\Big[(\mathbf{Z_u} - \mathbf{Z_g}) - \mathbf{p_{add}}\Big], & \mathbf{Z_u} - \mathbf{Z_g} \leq \mathbf{p_{add}} \\ 0, & \mathbf{Z_u} - \mathbf{Z_g} > \mathbf{p_{add}} \end{cases} \tag{4.18}$$

The modified repulsive potential function, which takes the relative distance between the

UAV and the target into consideration is given as

$$U_{rep}(\mathbf{Z_u}) = \begin{cases} \frac{q_{rep}}{2}\left(\frac{1}{\mathbf{Z_u}-\mathbf{Z_0}} - \frac{1}{\mathbf{p_0}}\right)^2, & \mathbf{Z_u}-\mathbf{Z_0} \leq \mathbf{p_0} \\ 0, & \mathbf{Z_u}-\mathbf{Z_0} > \mathbf{p_0}. \end{cases} \tag{4.19}$$

The repulsion force function $F_{rep}(\mathbf{Z_u})$ for the single UAV is given by

$$F_{rep}(\mathbf{Z_u}) = -\nabla[U_{rep}(\mathbf{Z_u})] = \begin{cases} q_{rep}(\frac{1}{\mathbf{Z_u}-\mathbf{Z_0}} - \frac{1}{\mathbf{p_0}})\frac{1}{(\mathbf{Z_u}-\mathbf{Z_0})^2}, & \mathbf{Z_u}-\mathbf{Z_0} \leq \mathbf{p_0} \\ 0, & \mathbf{Z_u}-\mathbf{Z_0} > \mathbf{p_0}. \end{cases} \tag{4.20}$$

As shown in (4.19) and (4.20), the formulations are identical to the original APF. The critical change is presented by introducing the additional force, which guarantees that the UAV will avoid the local minimum point. The total potential field at every move the UAV makes can be expressed as follows:

$$U_{\mathbf{Z_u}} = \sum_{r=1}^{i} U_{rep}(r) + \sum_{l=1}^{t}[U_{att}(l) + U_{add}(l)] \tag{4.21}$$

where i is the number of the obstacles, and t is the number of the goals. Similarly, the total force that affects the UAV and applies to multiple targets and obstacles is given as follows:

$$F_{\mathbf{Z_u}} = \sum_{r=1}^{i} F_{rep}(r) + \sum_{l=1}^{t}[F_{att}(l) + F_{add}(l)]. \tag{4.22}$$

There are other factors that can effect the performance of the APF algorithm. Therefore, in the next section, we will consider the effect of other UAVs on the single UAV.

4.4.2 Enhanced-APF Algorithm for Multiple UAVs

In this section, we apply the APF algorithm on multiple UAVs flying in an area where the UAVs are considered as moving obstacles with position and speed. Moreover, the UAVs have repulsion forces which can be enforced depending on their distance to other UAVs, obstacles,

and targets. The APF algorithm can provide the UAVs with all the information that is required for collision avoidance, and the repulsive and attractive forces are the important key components of the algorithm. Similar to a single UAV, the APF algorithm will run into the same local minimum problems. To overcome this problem, we apply the enhanced-APF algorithm based on a new set of formulations. In addition to the repulsion of obstacles, we also consider the impact of the repulsion between UAVs. Specifically, when the distance between UAVs is less than the desired distance, a repulsive force is generated. When the distance between the UAVs is greater than the desired distance, this force is zero. The critical change is considered in representing the repulsion function. Therefore, the formulation for attractive force is similar to the case with single UAV. The repulsion function of two UAVs can be given as [60]

$$U_{rep}(\mathbf{Z_{uu}}) = \begin{cases} q_u(\frac{1}{\mathbf{Z_{ui}}-\mathbf{Z_{uj}}} - \frac{1}{\mathbf{p_{uu}}})^2, & \mathbf{Z_{ui}} - \mathbf{Z_{uj}} < \mathbf{p_{uu}} \\ 0, & \mathbf{Z_{ui}} - \mathbf{Z_{uj}} \geq \mathbf{p_{uu}}. \end{cases} \tag{4.23}$$

where $\mathbf{Z_{ui}} - \mathbf{Z_{uj}}$ is the distance between two UAVs. q_u represents the force gain coefficient between UAVs. $\mathbf{p_{uu}}$ is the safety distance between two UAVs for collision avoidance.

The total force for the entire system includes a combination of multiple repulsive and attractive forces. The targets have gravitational force, obstacles have repulsive force, and additionally, each UAV moves toward the target under the superposition of various potential fields. The following equation combines all the potential fields that are required in the multi-UAV enhanced-APF algorithm:

$$U_{\mathbf{u}} = U_{rep}(\mathbf{Z_u}) + U_{att}(\mathbf{Z_u}) + U_{add}(\mathbf{Z_u}) + U_{rep}(\mathbf{Z_{uu}}) \tag{4.24}$$

4.4.3 Impact of 3D Antenna Radiation on UAV Trajectory

In this part, we consider the radiation pattern of the directional antenna which is mounted at the UAV. The trajectory of the UAVs can be affected by the deployment of these antennas.

For connectivity between the UAV and GBS, the SNR level should exceed a certain threshold β. Since SNR is proportional to the antenna gain, connectivity requirement translates into antenna gain being larger than a threshold. This proportionality further has an impact on the design of the UAV trajectory.

Hence, the trajectory of the UAV gets affected by applying the antenna gain formulas with antenna patterns in the APF algorithm. In the next section, we provide more details on the implemented enhanced-APF algorithm for UAV path planning.

4.5 The Proposed Solution of the Enhanced-APF Algorithm

Based on the equations in the previous section, we construct an iterative algorithm for the best UAV trajectory by applying the enhanced-APF method. Specifically, at each step, the UAV calculates the functions of attraction and repulsion potential fields. In this way, the UAV collects information about the position of the target, obstacles, and GBS. Additionally, inside a small grid with dimension $[q \times q]$, the UAV will decide for the next move. The geographical area of our system is defined as $[M \times Z]$. Furthermore, the UAV has eight moves to chose from starting at the initial location until it reaches the final destination. After that, the directional antenna of the UAV affects the trajectory of the UAV. The antenna can be oriented either horizontally or vertically. In the end, the UAV coordinates will get updated and finalized inside the matrix P. The rows and columns of the matrix represent x_u and y_u positions of the UAV, respectively. The details of the algorithm are summarized in Algorithm 1. It is worth pointing out that this algorithm is derived from the traditional AFP algorithm.

Similarly, Algorithm 2 is also adaptable for use with multiple UAVs. In such scenarios, each UAV is programmed to navigate around obstacles and maintain a safe distance from other UAVs, ensuring a collision-free path to the final destination. The subsequent section

Algorithm 1 Enhanced-APF Algorithm for single UAV

Input: for given position of initial location $\mathbf{Z_s}$, position of final location $\mathbf{Z_g}$, position of GBS W_k, position of obstacles $\mathbf{Z_o}$, the attraction gain coefficient q_{att}, the repulsive gain coefficient q_{rep}, additional field coefficient q_{add}, the UAV height H_u, antenna gain threshold β,
Output: trajectory of the UAV $\boldsymbol{P}$
for s = 1 : S **do**
  calculate equation (4.15) and (4.17) and (4.19) and (4.23) for given input
  calculate the total force potential field (4.21)
  while $d_k(t)$, $d_j(t) \geq [q \times q]$ **do**
    for each UAV step **do**
      Update $x_u(t)$ and $y_u(t)$
      if $x_u(t)$, $y_u(t) < 0$ or $x_u(t)$, $y_u(t) > [M \times Z]$ **then**
        Break;
      else if solve (4.7) for Sin patterns or (4.8) for Cos patterns **then**
        Update UAV coordinate $x_u(t)$ and $y_u(t)$
      end if
    end for
    if the UAV have reached the final location $\mathbf{Z_g}$ **then**
      Break;
    end if
  end while
end for
return P;

will present our findings, showcasing the results and simulations conducted to validate the algorithm's effectiveness in multi-UAV environments.

Table 4.1: Table of Parameter Values

Parameters	**Values**
H_u	$60m, 80m$
β	0.1
q_{att}	10
q_{rep}	100
q_{add}	18

4.6 Simulations And Numerical Results

This section presents simulation results to demonstrate the effectiveness and efficiency of the implemented enhanced-APF algorithm. We conducted multiple experiments and set up the appropriate values for the parameters.

Algorithm 2 Enhanced-APF Algorithm for Multiple UAVs

Input: for given position of initial location $\mathbf{Z_s}$, position of final location $\mathbf{Z_g}$, number of UAVs N, position of GBS W_k, position of obstacles $\mathbf{Z_o}$, the attraction gain coefficient q_{att}, additional field coefficient q_{add}, the force gain coefficient for multiple UAVs q_u, the repulsive gain coefficient q_{rep}, the UAV height H_u, antenna gain threshold β,
Output: trajectory of the UAV $\boldsymbol{P}$
for s = 1 : S **do**
  for i = 1 : N **do**
    calculate equation (4.15) and (4.17) and (4.19) and (4.23) for given input
    calculate the total potential field (4.24)
    while $d_{ki}(t)$, $d_{ji}(t) \geq [q \times q]$ **do**
      for each UAV step **do**
        Update $x_{ui}(t)$ and $y_{ui}(t)$
        if $x_{ui}(t)$, $y_{ui}(t) < 0$ or $x_{ui}(t)$, $y_{ui}(t) > [M \times Z]$ **then**
          Break;
        else if solve (4.7) for Sin patterns or (4.8) for Cos patterns **then**
          Update UAV coordinate $x_{ui}(t)$ and $y_{ui}(t)$;
        end if
      end for
    end while
  end for
  if the UAV have reached the final location $\mathbf{Z_g}$ **then**
    Break;
  end if
end for
return P;

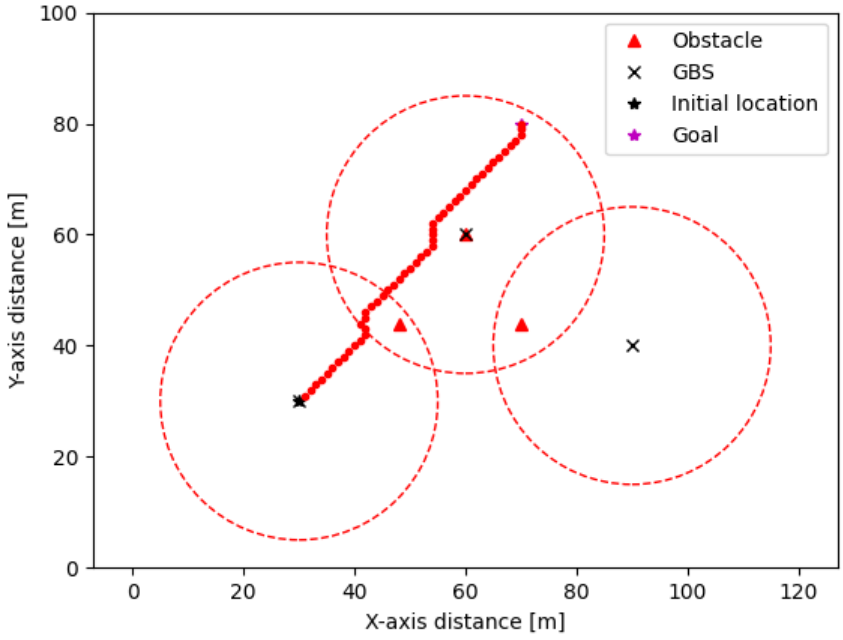


Figure 4.4: The original map of the traditional artificial potential field

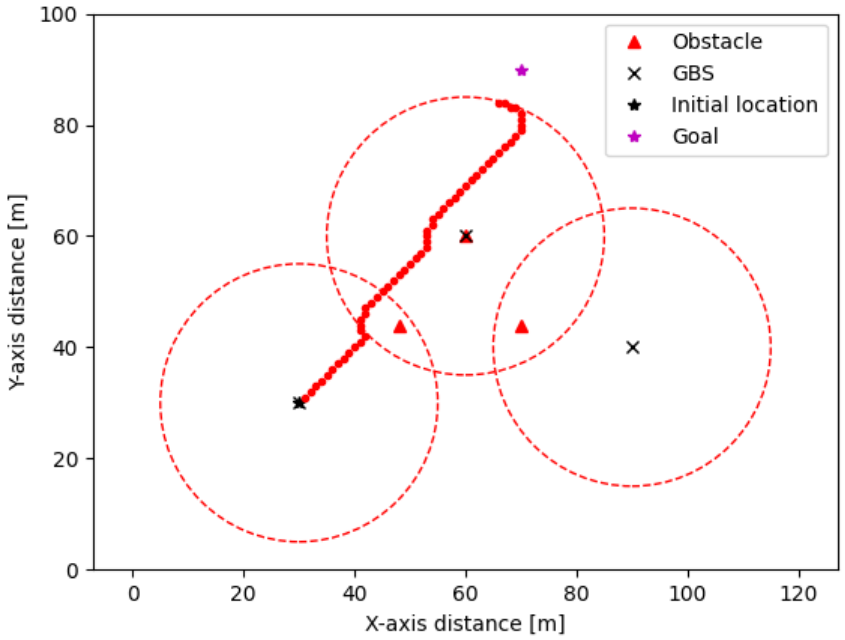


Figure 4.5: The original map of the traditional artificial potential field

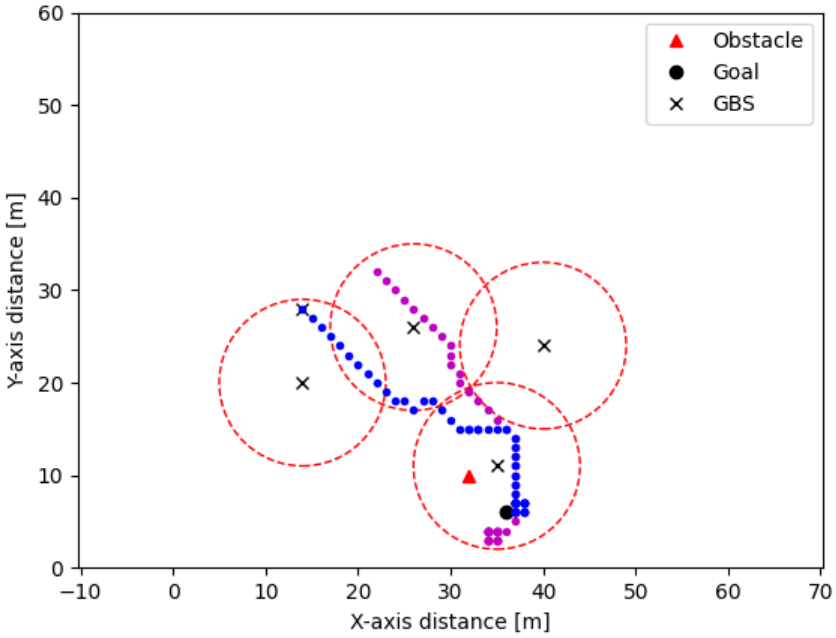


Figure 4.6: Trajectory Design for 2 UAVs Using Enhanced-APF Algorithm with Integrated Collision Avoidance

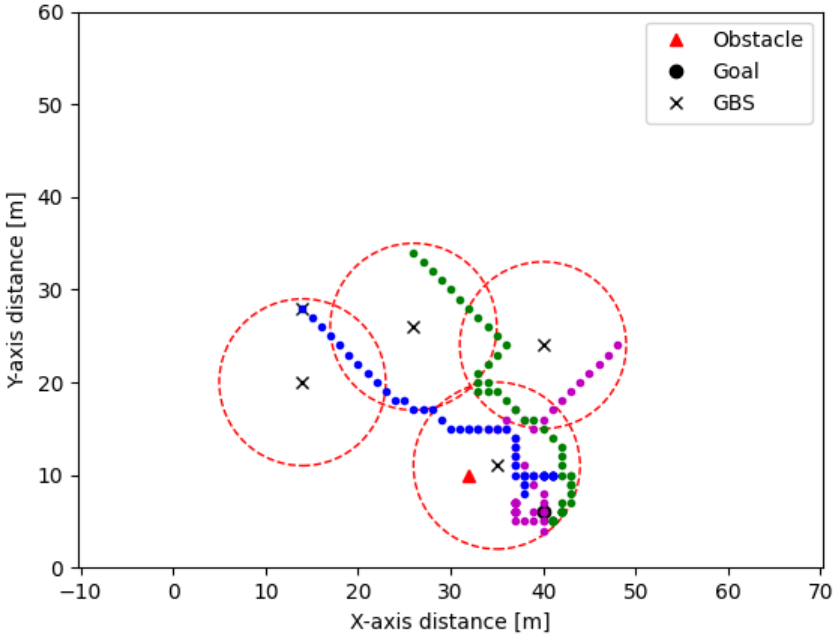


Figure 4.7: Trajectory Design for 3 UAVs Using Enhanced-APF Algorithm with Integrated Collision Avoidance

In Figure 4.4, we show a trajectory design of a single UAV traveling from an initial location to a final destination, as it strictly flies inside circular coverage regions of the ground base stations while avoiding obstacles. On the other hand, in Figure 4.5, the UAV fails to reach its final destination due to the constraint that does not allow the UAV to fly outside the coverage area.

In Figure 4.6, we show the trajectory design for two UAVs reaching their final destinations while they satisfy the connectivity requirements (by staying in the coverage regions) as well as avoiding the collision with obstacles and other UAVs. Similarly, the trajectory design for three UAVs as they travel within the communication region with obstacle avoidance and other UAVs is shown in Figure 4.7.

In Figure 4.8, we illustrate the trajectory planning for a UAV that is influenced by an antenna with a horizontally oriented gain pattern. This specific orientation of the antenna gain affects how the UAV navigates through its environment, as the signal strength and

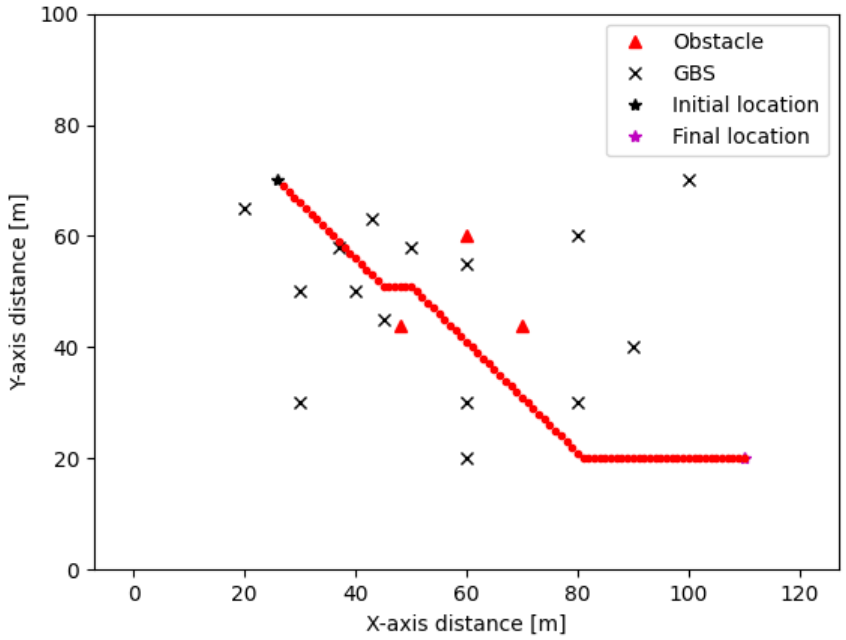


Figure 4.8: Trajectory Design using Enhanced-APF Algorithm on Single UAV equipped with horizontally oriented antenna

coverage are optimized along the horizontal plane. As a result, the UAV's path is strategically designed to maximize communication efficiency by aligning its flight route with areas of strong signal reception, which are predominantly spread out horizontally due to the antenna's orientation.

Conversely, Figure 4.9 showcases the trajectory planning for a UAV that utilizes an antenna with a vertically oriented gain pattern. This vertical orientation significantly alters the UAV's optimal flight path. The vertical gain pattern provides enhanced signal strength and coverage in the vertical dimension, which influences the UAV to adjust its altitude more frequently to remain within areas of optimal signal reception. This results in a trajectory that may include more vertical movements or altitude adjustments compared to the horizontally influenced path seen in Figure 4.8.

The comparison between these two figures highlights the profound impact that antenna radiation patterns can have on UAV trajectory planning. The orientation of the antenna gain

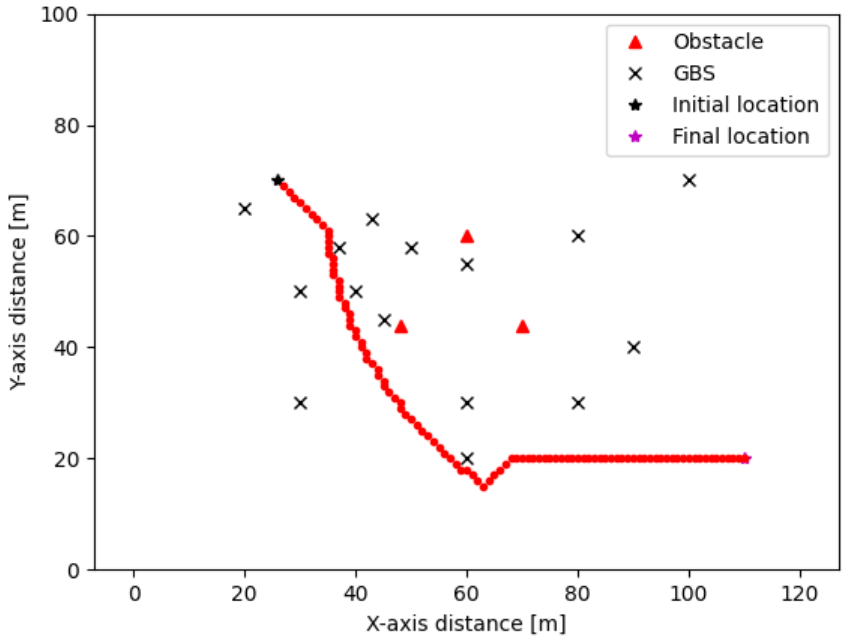


Figure 4.9: Trajectory Design using Enhanced-APF Algorithm on Single UAV equipped with vertically oriented antenna

not only dictates the UAV's ability to maintain a strong communication link with ground stations or other aerial platforms but also directly influences the UAV's path to ensure it remains within the antenna's optimal coverage area. This emphasizes the importance of considering antenna characteristics in the design and optimization of UAV flight paths, especially in applications where reliable communication is critical.

In Figures 4.10 and 4.11, we present the UAV flight paths at varying altitudes, details of which are also tabulated in Table 4.1. Figure 4.10 illustrates the UAV's trajectory at a lower altitude of 60 meters. At this height, the UAV successfully navigates to its intended endpoint, adeptly circumventing any obstacles in its path while ensuring a stable communication link with the ground stations. This is attributed to the optimal altitude facilitating a balance between obstacle avoidance and maintaining a strong signal for reliable connectivity.

Conversely, Figure 4.11 depicts the UAV's flight path at a higher altitude of 80 meters. Despite the increased elevation offering a broader line-of-sight and potentially easier obstacle

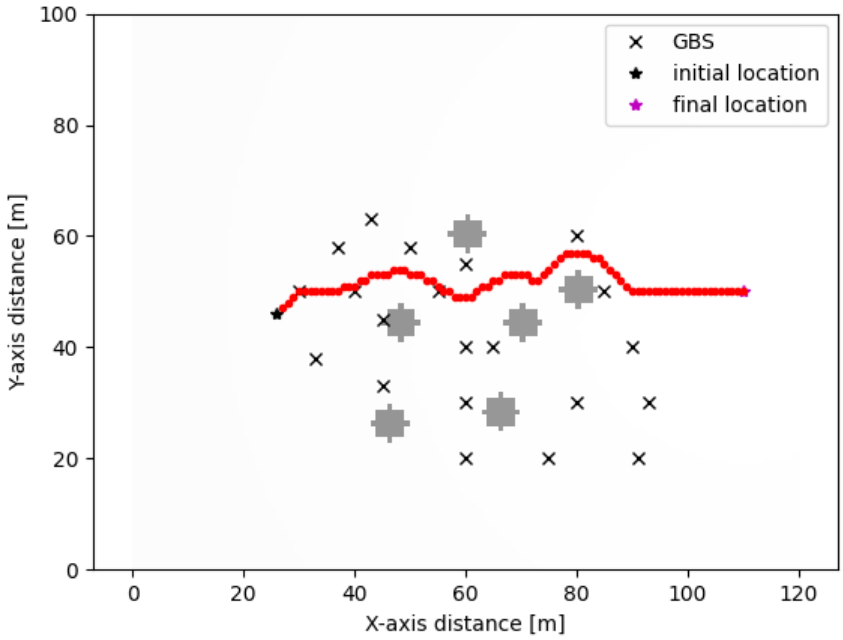


Figure 4.10: Trajectory Design using Enhanced-APF Algorithm when the UAV at altitude $H_u = 60m$

avoidance, the UAV fails to reach its designated target. This failure is primarily due to the exacerbated path loss associated with the higher altitude, which is a consequence of the specific antenna radiation pattern in use. At this elevated height, the signal attenuation becomes significant enough to disrupt the UAV's communication with the ground stations, thereby hindering its ability to complete the designated route effectively. This scenario underscores the critical interplay between altitude, antenna radiation characteristics, and path loss in UAV navigation and communication systems, highlighting the need for careful consideration of these factors in UAV path planning.

4.7 Conclusion

In this study, we introduced and applied an advanced version of the Artificial Potential Field (APF) algorithm, tailored for both individual and collective UAV navigation scenarios. This refined algorithm facilitated the derivation of optimized flight paths, ensuring operational

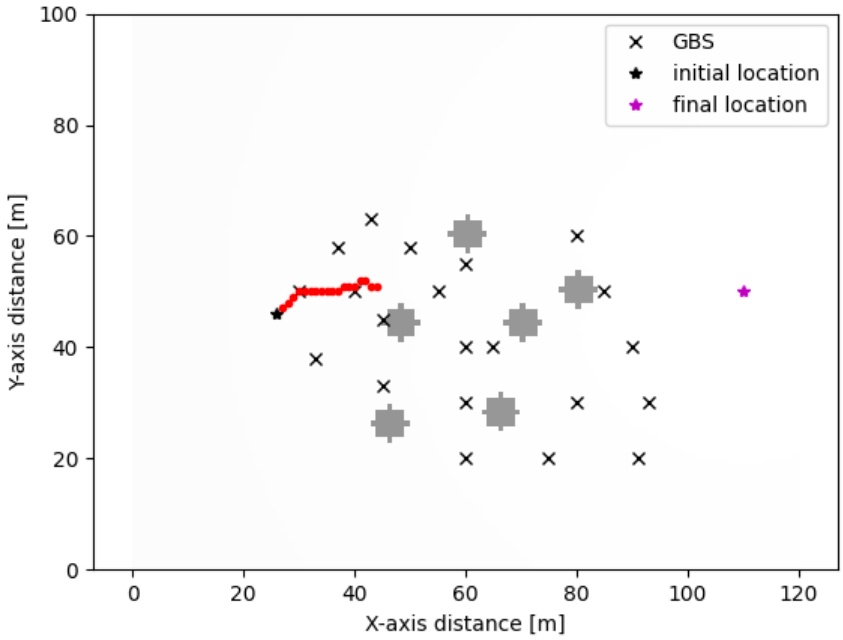


Figure 4.11: Trajectory Design using Enhanced-APF Algorithm when the UAV at altitude $H_u = 80m$

efficiency and safety. Our approach meticulously tackled the challenges of navigating around obstacles and preventing in-flight collisions among UAVs, a critical consideration for swarm operations. Furthermore, we delved into the nuanced effects of antenna radiation patterns on flight path optimization, revealing how these technical specifications can significantly influence trajectory planning to ensure robust communication links.

The simulation outcomes have been illuminating, showcasing the algorithm's capability to guide UAVs to their designated locations effectively. These results underscore the algorithm's adeptness in maintaining essential communication links with ground stations or other UAVs while simultaneously navigating around obstacles and avoiding potential aerial conflicts. This balance is crucial for the practical deployment of UAVs in complex environments, where operational reliability and safety are paramount.

Looking ahead, our research will venture into uncharted territories by integrating more sophisticated constraints and operational parameters into the trajectory planning algorithm.

We aim to explore the incorporation of advanced security measures and safety protocols, addressing the growing concerns surrounding UAV cybersecurity and the need for fail-safe mechanisms. This future work will not only enhance the operational integrity of UAVs but also expand their applicability in sensitive and critical missions, paving the way for more autonomous, secure, and reliable UAV operations in diverse application domains.

Chapter 5

Cyber-Physical Attacks on UAV Systems

5.1 Introduction

As networked embedded control technology advances and manufacturing costs decline, Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, have become increasingly prevalent for executing tasks that are hazardous, monotonous, physically challenging, or economically impractical for humans. In military contexts, UAVs are revolutionizing warfare tactics and strategies. Concurrently, the civilian applications of UAVs have seen rapid expansion. In these applications, a notable trend is the shift from solitary UAV operation to collaborative efforts, forming dependable networks. This is because a collective of UAVs offers broader coverage, enhanced flexibility, and increased robustness due to redundancy [61]. Consequently, the complexities associated with managing a network of multiple UAVs are substantially greater than those encountered with a single UAV. As a result, multi-UAV networks have garnered considerable interest over the past decade. Advances in wireless communication, high-performance computing, and flight control have significantly augmented the capabilities of UAV networks in terms of communication, computation, and

control. However, this surge in usage has also brought UAV security issues to the forefront, drawing heightened scrutiny in recent years.

The intricate and unpredictable environments, along with open wireless communication channels and the absence of robust security protocols for UAVs, render them susceptible to attacks. Studies in [62], [63] predominantly delve into the analysis of vulnerabilities to cyber-attacks on UAVs. Yet, UAVs embody cyber-physical systems (CPS) composed of various elements such as sensors, communication networks, computational units, and control mechanisms, all of which could potentially be targeted by cyber-attacks, thereby compromising the system's integrity and leading to adverse operational outcomes and significant malfunctions. As outlined in [64], attacks that manifest physical repercussions through cyber means are termed "cyber-physical" attacks. Such attacks pose a significant risk of catastrophic outcomes for UAVs and other cyber-physical systems (CPS). Therefore, examining the cyber-physical threats and the implications of cross-domain attacks on UAVs is imperative. This area of inquiry represents a critical research trajectory within the domain of CPS security.

Comprehending and scrutinizing cyber-physical threats are crucial for formulating robust defense strategies against them. Using UAVs as a prime illustration of a complex, safety-critical cyber-physical system (CPS), it is beneficial to explore their cyber-physical vulnerabilities to gain insights applicable to other critical CPS. This work delves into the potential cyber-physical threats faced by UAVs and examines how these threats propagate, viewed from a CPS standpoint.

5.2 Cyber-Physical Attack on the UAV

Cyber-physical systems (CPS) create a seamless integration between the cyber and physical realms by embedding cybernetic functionalities—namely communication, computation, and control—directly into physical devices [65]. This integration facilitates real-time, depend-

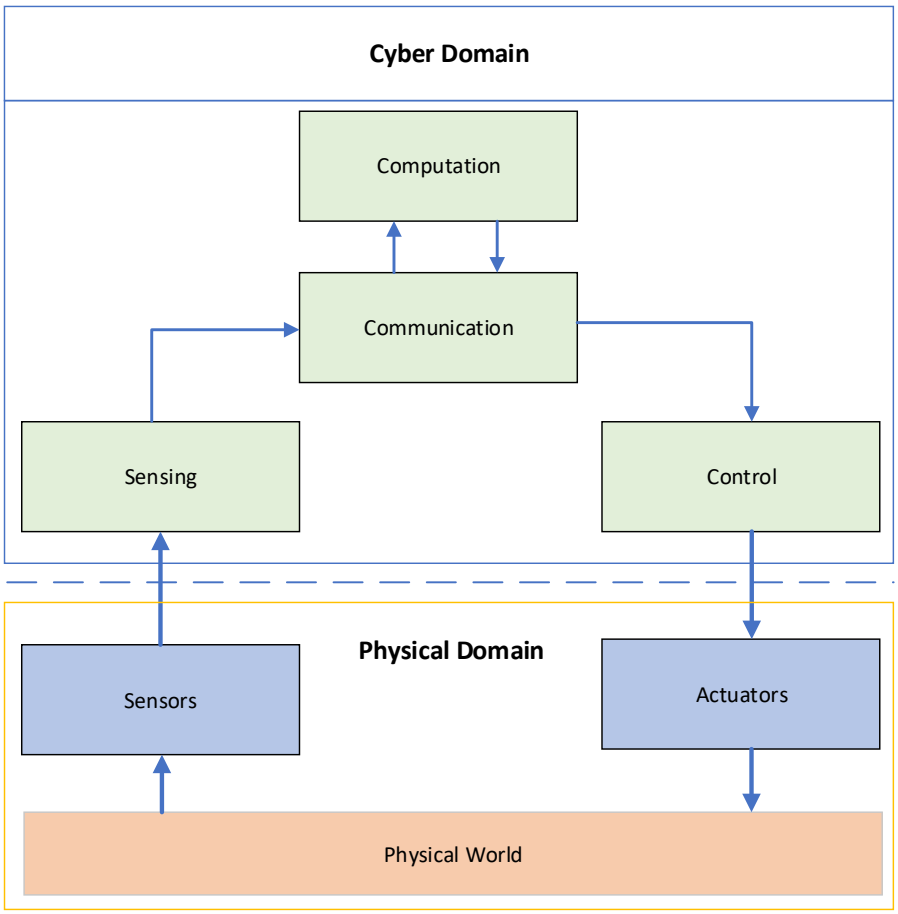


Figure 5.1: The interactions and data exchange between sensing, communication, computation, and control within UAV networks, viewed through the spectrum of CPS.

able oversight and manipulation of physical entities, thereby enhancing the management of resources and the fine-tuning of system performance. As outlined in [66], Figure 5.1 illustrates the architecture of a typical UAV from a Cyber-Physical System (CPS) perspective. It's important to highlight that within the CPS framework, each component not only fulfills its designated role but also collaborates seamlessly with others to ensure efficient coordination. The communication architecture encompasses both UAV-to-Ground Control Station (UAV-GCS) and UAV-to-UAV interactions. In UAV-to-UAV communications, any UAV can establish direct communication with its peers or utilize multi-hop links for extended connectivity. Furthermore, the communication and control modules are equipped with capabili-

ties for mission coordination, collaborative path planning, cooperative control, monitoring and diagnostics, as well as data interoperability. UAV networks epitomize this integration through a cyclical process that encompasses the initial gathering of data, the exchange of information, the formulation of decisions, and the execution of actions [67]. Within these networks, sensor-acquired data is rooted in the physical environment (reflecting the operational context of the UAV), while the resultant decisions, shaped by computational processes and communicated across the network, manifest in the physical domain via actuator-driven actions. Viewed through this lens, the intricate structure of UAV networks exemplifies a CPS. Given the expansive scope of CPS, UAV networks—ranging from individual UAVs at the cellular level, to coordinated groups forming a UAV swarm at the system level, and even to conglomerates of diverse UAV swarms at the system-of-systems level—can all be conceptualized and developed as CPS. In critical societal sectors such as transportation, energy, healthcare, and manufacturing, the adoption of CPS paves the way for enhanced intelligence and efficiency. As a cornerstone of next-generation systems, CPS is poised to play a pivotal role in the practical application of artificial intelligence. Consequently, the incorporation of CPS principles into UAV networks holds the potential to substantially elevate the overall efficacy of these systems. UAV's actions.

5.3 Cyber-Physical Threats of UAVs

In the context of cyber-physical attacks, every element within the UAV architecture in a CPS framework can be considered a potential target for attacks. This section is dedicated to examining the array of cybersecurity threats and exploring the mechanisms through which these threats could extend their impact to the physical functionalities of the system.

5.3.1 Attack on UAV Sensors

Sensors play a crucial role in UAVs, gathering data about the drone and its surroundings. Modern drone technologies depend on the integration of multiple sensors, including gyroscopes, accelerometers, magnetometers, Global Positioning Systems (GPS), and barometers, among others. These essential sensors enable UAVs to acquire information about their altitude, position, and environment, ensuring safe and stable operation. For enhanced safety, UAVs are additionally outfitted with supplementary sensors like infrared and ultrasonic detectors, as well as vision sensors, to facilitate obstacle avoidance. The flight controller, guided by data from an array of sensors, commands the power system to ensure the UAV's stable flight and successful mission completion. Consequently, inaccurate data can lead the controller to make erroneous decisions, jeopardizing flight safety and potentially leading to a crash. Therefore, attacks on sensors are recognized as a significant and widespread threat [22].

5.3.2 UAV GPS Spoofing/Jamming

The navigation of Unmanned Aerial Vehicles (UAVs) is heavily reliant on the Global Positioning System (GPS), where the UAV's onboard GPS receiver captures and processes signals transmitted by satellites. However, the GPS signals designed for civilian applications are freely available, unencrypted, and lack authentication measures. This openness makes GPS systems particularly vulnerable to spoofing attacks, a prevalent form of cyber assault on UAV navigation systems. Spoofing attacks come in two primary variants: the repeater type and the generating type [68]. The repeater attack involves capturing genuine satellite signals and rebroadcasting them to the UAV, misleading its navigation system. On the other hand, the generating type of attack employs specialized software to create counterfeit GPS signals that mimic authentic ones. These fabricated signals are indistinguishable from real ones to the UAV's receiver due to the public availability of the encryption and testing algorithms used for civilian GPS signals.

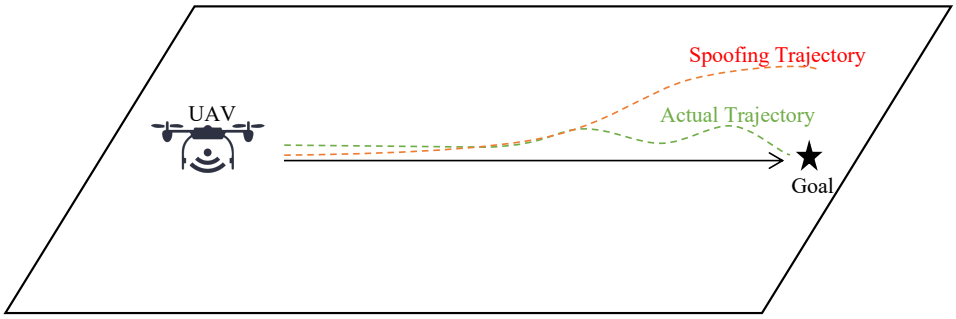


Figure 5.2: The UAV trajectory path scenario under spoofing attack

In addition to spoofing, GPS jamming represents another significant threat, albeit one that is simpler to execute. Jamming involves the emission of disruptive signals that overpower or interfere with the GPS signals, preventing the UAV's receiver from accurately receiving and interpreting the navigation data [69]. This interference can lead to a loss of orientation for the UAV, potentially resulting in catastrophic outcomes, including crashes. The simplicity of mounting jamming attacks, coupled with the critical reliance of UAVs on GPS for navigation, underscores the urgent need for robust countermeasures to protect UAV systems from such vulnerabilities, ensuring their safe and reliable operation in various applications.

5.3.3 Attacks on UAV Computation/Control Units

False Data Injection Attacks (FDIAs) [70], also known as stealthy deception attacks, represent a sophisticated form of cyber assault that targets the state estimation processes within various control systems, notably in power systems [71]. These attacks subtly alter measurement data to skew state estimations without triggering alarms in the system's bad data detection mechanisms. Accurate state estimation is crucial for the reliable operation of drones, particularly for navigation and flight control functionalities.

In a notable study [72], UAV navigation was examined through the lens of a stochastic linear Cyber-Physical System (CPS) framework, incorporating Gaussian noise to reflect real-world conditions. This research highlighted the vulnerabilities of the Kalman Filter (KF), a

prevalent method for state estimation in such systems. The study outlined specific conditions under which the system dynamics could be exploited by stealthy deception attacks, thereby compromising the integrity of state estimations.

Furthermore, this research broadened the scope of potential attack vectors by considering simultaneous attacks on both sensor and actuator components. This approach contrasts with much of the existing literature, which typically focuses on cyber-attacks targeting either sensors or actuators exclusively. Another study [73], introduced several attack strategies against two common altitude estimation techniques: KF-based estimation and sensor-model-based estimation. For KF-based systems, a maximal FDI attack was proposed and thoroughly analyzed. In the case of sensor-model-based estimation, the researchers devised strategies to disrupt GPS signals and alter barometer readings, thereby affecting the system's confidence in altitude estimations and enabling the manipulation of perceived altitude.

In addition to FDIA, communication link attacks pose a significant threat to UAV operations. These attacks specifically target the data exchange channels between UAVs and Ground Base Stations (GBS), compromising the integrity of telemetry feeds and command signals issued by the GBS. The vulnerability arises when these communication links lack robust encryption, making them susceptible to interception.

Much like GPS signals, the control signals from the GBS are prone to spoofing and jamming attacks. In a typical scenario, attackers might intercept authentic commands from the GBS, substitute them with malicious instructions directed at the UAV, and then relay altered responses back to the GBS, effectively conducting a "man-in-the-middle" attack. This type of cyber assault not only jeopardizes the safety and operational integrity of the UAV but also undermines the reliability of the control and monitoring systems managed by the GBS. Ensuring secure and encrypted communication channels is paramount to safeguarding UAVs from such sophisticated cyber threats.

5.4 Conclusion

Historically, the security assessments of Unmanned Aerial Vehicles (UAVs) have been segmented into two distinct realms: flight safety and information security. However, as the integration of cyber-physical system (CPS) components within UAVs becomes more intricate, cyber-attacks targeting the information systems not only compromise data integrity but also precipitate erroneous control commands. Such breaches can critically undermine the overall safety and operational reliability of UAVs. Consequently, it becomes imperative to examine the cascading effects of security threats from the informational layer to the physical layer, understanding how vulnerabilities in the cyber domain can manifest as tangible risks in the physical domain.

In this work, we provide an overview of how the security landscape for UAVs is evolving, highlighting the interconnected nature of cyber and physical threats. This holistic approach to analyzing the interplay between cyber-attacks and their physical repercussions forms the cornerstone of this study and offers valuable insights for the security evaluation of broader CPS frameworks.

Chapter 6

Path Planning for UAVs Under GPS Permanent Faults

6.1 Introduction

Unmanned aerial vehicles (UAVs) have attracted significant interest in civilian and military applications. Indeed, many new technologies have been involved in designing and building UAVs that have different capabilities in rescue missions and emergency response. Additionally, UAV technology is expected to become a crucial part of aerial surveillance systems, particularly in smart cities. Also, in wireless communication systems, UAVs will play a significant role in assisting and improving the existing communication infrastructure and helping the deployment of the 5G technology in rural and remote regions [50]. UAV trajectory planning is one of the most critical components in controlling and monitoring UAVs during flight. Therefore, the UAV must stay connected with its associated ground base station (GBS) to make sure that the position and location of the UAV have been updated regularly. Additionally, the path planning and the trajectory design of a UAV becomes a key challenge to provide the best wireless connectivity and enhance the system's security and robustness. The air-to-ground channel model has been studied in [74]. Also, new studies

started to look at UAVs as aerial base stations [75], [5]. Authors in [52], have studied the optimal position for UAVs to maximize the throughput. In UAV positions and placement scenarios, authors in [76] have considered the entire trajectory design for multiple UAVs to jointly optimize scheduling and user association. In the deployment and trajectory planning in UAV communication with jamming, authors in [6] proposed a trajectory planning method in three-dimensional (3D) and introduced an anti-jamming approach by dynamically adjusting the UAV's trajectory. Moreover, authors in [77] present an intelligent UAV anti-jamming strategy, in which the optimal trajectory of the typical UAV is obtained via dueling double deep Q-network (D3QN). A low-power robust learning framework to deal with adversarial attacks has been introduced in [78], the authors propose a staged ensemble defense strategy in the framework, which achieves better defensive performance than a single defense algorithm.

One approach in trajectory design planning is to apply the artificial potential field (APF) algorithm. The APF method is a virtual force method that was first introduced by Khatib in [20]. The APF algorithm is developed to avoid collisions among multiple real-time autonomous vehicles and robots operating in a complex environment [20]. Recently, several studies have been conducted on UAV path planning using APF. For instance, the authors in [56] study the optimized APF for multiple UAVs operating in a 3-D dynamic environment. Similarly, the adaptive particle swarm optimization algorithm (APSO) designed for introduction to APF has been introduced in [79] where authors combine the global virtual navigation path (VNP) calculated by the particle swarm optimization algorithm (PSO) with the artificial potential field method for UAV path planning. In [80], the authors propose two algorithms, one is an obstacle avoidance control algorithm for a distributed multi-UAV formation system, and the other is the velocity-based artificial potential field (VAPF) algorithm which helps a UAV to avoid dynamic obstacles and overcome the APF problems of local minimum. The key idea behind the APF algorithm is to calculate the distance between the moving object and the obstacle.

6.1.1 UAV and Cyber-Physical System (CPS)

Cyber-physical systems (CPS) are intelligent computer systems that are engineered in a way combining algorithmic computation and communication processes while sensing and interacting with the physical world. The rapid development of CPS technology encourages the development of key technologies and products in autonomous systems such as UAVs and self-driving cars. The mutual interaction between the physical world and information technology puts CPS at risk and makes it vulnerable to malicious attacks that are beyond traditional cyber attacks [81], [82], [83]. This is becoming a real threat to many technologies sometimes resulting in potential breaches of sensitive information about individuals and entities. Therefore, UAVs are one of the most targeted elements by the attackers to take advantage of and wreak havoc by taking control of the UAVs' movement and position. However, since it is difficult to ensure the safe movement of UAVs with the autopilot system against various cyber security attacks, many new studies have proposed new approaches to discovering the attackers and providing a recovery procedure for the system. The authors in [22] discuss the security threat coming from cyber attacks and how it will affect the safety performance of the UAVs, and they analyze the Cross-domain security risk mechanism of UAVs. Furthermore, in [62], the authors propose a new GPS spoofing attack detection method based on a machine learning algorithm that allows UAVs to detect GPS spoofing attacks. An attacker implementing GPS spoofing sends fake information either by generating new signals or by altering legitimately received signals, leading to an inaccurate display of GPS positions of the targeted device [84]. By the same token, a detection attack using the Bayesian network model has been proposed in [85], authors use their proposed model to analyze and detect the fake GPS signal data which is injected by the attackers. In the same direction, the authors in [86] carry out three studies involving GPS attacks in UAVs detecting GPS fraud, counterfeiting GPS on real UAVs, and implementing security measurements to avoid the attack. In [87], the authors propose an effective real-time cyber attack detection method using modified sliding innovation sequences (MSIS) detector. Also,

in [88] the authors develop a Gaussian process GP-based approach to estimate the unknown disturbance and propose an approach to adapt the system performance (i.e., speed) along the planned trajectory based on environmental constraints and the GP-based estimation and to dynamically update the GP model.

These results have motivated further research efforts on studying problems of adversarial attacks on UAVs. The adversarial training and defensive distillation methods are evaluated and discussed in [89]. The authors in [90] propose two adversarial attack methods based on forward derivative and optimization to conduct adversarial attacks against DL-based navigation systems of UAVs. To the best of our knowledge, prior work has not taken into account the impact of the cyber-physical attack on the path planning of the UAV and how it affects the entire flight mission of the UAV by sending wrong information to the GBS on the location of the UAV. Furthermore, in many cases, it can cause a real danger to the entire mechanism and the components of the autopilot system, which controls the movement of the UAV.

To address this challenge, we propose an efficient approach to detect and recover the UAV path planning under cyber-physical attacks on the GPS, knowing that the UAV is equipped with a detector. Attack detection occurs when the UAV loses connectivity with the nearest ground base station (GBS). By injecting false data, the attack diverts the UAV from following its planned path and dictates it to follow a different path. In addition, the GBS loses track of the UAV information such as the coordinates at a certain time and location. We design a new detection and estimation architecture based on two steps. Firstly, we estimate the UAV location under GPS attack using received signal strength (RSS) based trilateration. Secondly, we have developed a cyber-attack resilience procedure utilizing the Artificial Potential Field (APF) algorithm, known as the Resilience to Cyber-Attacks APF (RCA-APF) algorithm.

In essence, the RCA-APF algorithm is a specific method that handles both GPS permanent fault detection and estimated UAV path planning. Such an algorithm can be developed

based on feeding the system with the coordinates of the UAV during its flight from an initial to a final location. To be specific, our method is applicable to deal with compromised sensor measurements caused by faults and false data injection. In this sense, detection, and estimation are presented as cause and effect. Finally, we evaluate our design by conducting simulation-based experiments which demonstrate the performance of the proposed approach.

Particularly, the RCA-APF algorithm, while indeed serving as an obstacle avoidance mechanism, is intrinsically designed to complement our system's resilience to GPS permanent fault. In scenarios where GPS fault might mislead the UAV path into hazardous zones, the RCA-APF algorithm serves as a critical layer of defense. It enables the UAV to make context-aware decisions, avoiding obstacles that might not be evident through compromised GPS data. In addition, the RCA-APF algorithm works in collaboration with our RSS trilateration technique. While RSS trilateration provides accurate localization in the absence of reliable GPS data, RCA-APF ensures safe navigation through potential threats, forming a comprehensive solution to GPS faults.

Regarding the advantages of RCA-APF over traditional APF algorithms, we have identified several key improvements:

- Unlike traditional APF algorithms [20], which have static response behaviors, our RCA-APF algorithm adapts its response based on the context, such as the proximity and size of obstacles and the severity of GPS fault.

- Our algorithm demonstrates superior robustness in dynamic and unpredictable environments, a common challenge for the UAV, especially in GPS-compromised scenarios.

The rest of this chapter is organized as follows. Section 6.2 presents the design overview and the system model. Section 6.3 introduces the UAV cyber-physical system and the threat model. Section 6.4 describes the UAV cyber-physical system approach. Section 6.5 demonstrates the simulation results. Finally, Section 6.6 concludes the chapter.

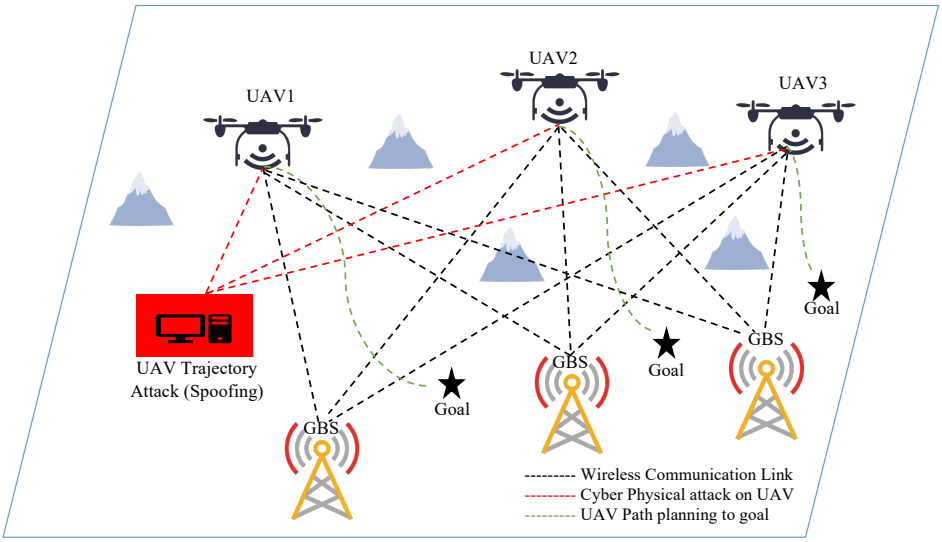


Figure 6.1: UAVs attack system model.

6.2 Preliminaries and Design Overview

In this section, we delineate the system model, illustrating the trajectory of each UAV as it navigates from a starting point to its destination. We detail the communication channel model between UAVs and Ground-Based Stations (GBSs).

6.2.1 System Model

In this work, we consider a graphical area with a $3D$ Cartesian coordinate system, where the horizontal coordinate of a ground base station (GBS) k is fixed at $W_k = [x_k, y_k]$. The UAV communicates with each of the ground base stations with time length T. All UAVs are assumed to fly at an altitude of H_u above the ground, and the time-varying horizontal coordinate of the UAV at time instant t is denoted by $\mathbf{L_u} = [x_u(t), y_u(t)]$. In this model, potential permanent faults on the UAV path planning can be introduced, as shown in Figure 6.1. Also, we assume that each UAV starts from a fixed initial location $\mathbf{L_s} = [x_s, y_s]$, and aims to reach the destination/goal $\mathbf{L_g} = [x_g, y_g]$. Also, we assume that the fixed obstacles are randomly distributed and the location of the obstacle j is denoted by $\mathbf{L_o} = [x_j, y_j]$.

6.2.2 Channel Model between UAV and GBS

The communication link between a UAV and the k^{th} GBS is typically dominated by line-of-sight (LOS) [10]. The LOS probability is given by

$$P_{LOS} = \frac{1}{1 + a\exp(-b(\arctan\frac{h}{d_i} - a))}. \tag{6.1}$$

where a and b are constant values depending on the environment. The relative Non-line-of-sight (NLOS) probability is $P_{NLOS} = 1 - P_{LOS}$. The UAV exchanges data packets with the GBS, assuming that all GBS locations are known. The distance from the i^{th} UAV to the k^{th} GBS at time t is given by

$$d_k(t) = \sqrt{H_u^2 + (x_i(t) - x_k)^2 + (y_i(t) - y_k)^2}. \tag{6.2}$$

Similarly, the distance from the i^{th} UAV to the j^{th} obstacle at time t is given by

$$d_j(t) = \sqrt{H_u^2 + (x_i(t) - x_j)^2 + (y_i(t) - y_j)^2}. \tag{6.3}$$

6.3 UAV CPS and Threat Model

6.3.1 System Model of UAVs Wireless Networks

UAVs are drones or aircraft that can fly without the need for a pilot on board. Also, UAVs are equipped with many essential components such as the flight control unit, sensor payloads, and wireless communications module. In addition, reliable and very high-speed wireless communication networks are required for the UAV to execute its flying mission successfully. The payload sensors are equipped with onboard sensors and GPS modules for position and navigation purposes. The communication module includes a high-speed wireless interface and antennas to transmit and receive control signals and data. There are mainly

two types of radio communications that occur in a typical UAV-assisted communication network; UAV-to-UAV and the communication between UAV to the nearest GBS. Moreover, network communication plays an important role to ensure smooth wireless networking and uninterrupted services. The integrated system of the UAV works by collecting data, exchanging information, making decisions, and eventually executing those decisions [91].

6.3.2 CPS Architecture of UAV

We consider that a single UAV is used to execute complex missions. During these missions, the UAV communicates with the GBS through the uplink and downlink channels. Moreover, the onboard GPS sensor in the cyber-physical system architecture plays an essential role in cooperating and achieving efficient coordination. In addition, the GPS sensor helps the UAV with mission allocation and monitors path planning in addition to exchanging the data between the UAV and the nearest GBS.

In this work, we focus on the GPS permanent faults in cyber-physical systems. It is important to have an attack detector deployed on the UAV to maintain the safety of the system [92], [93], [94]. Additionally, the attack detector should be computing-efficient due to the limited resources on the UAV in real-time scenarios. Usually, the attack detector monitors the data streams from the sensors to check whether there is a statistically abnormal signal [92], [95]. For example, Cumulative Sum CUSUM-based methods can be applied onboard at the UAV to monitor the residuals between the sensor measurements and estimation over a time window [95]. Figure 6.2 depicts the UAV hardware components within the cyber-physical system architecture. Notably, the GPS sensor of the UAV emerges as an appealing target for potential attackers, posing a significant risk of system damage. The errors in the GPS readings affect the movements of the UAV. These errors instruct the UAV to follow a specific path. In other words, the GPS permanent faults divert the UAV to an arbitrary location of the attacker's choosing. It is worth noting that the UAV is equipped with an onboard detector. This onboard attack detector is further used to estimate the UAV position

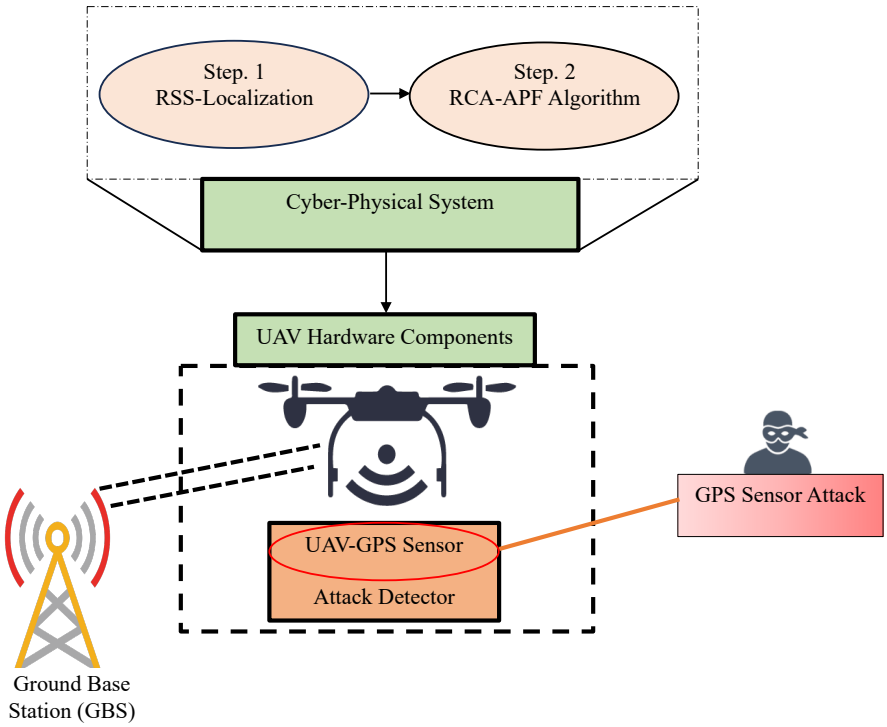


Figure 6.2: Cyber-physical system architecture.

when the attacker caused the permanent fault for the UAV-GPS sensor.

Figure 6.3 illustrates the primary sensors mounted on the UAV, which include the onboard attack detection system, the GPS sensor, and the camera sensor.

6.3.3 Cyber-Physical Attack to UAV and Threat Model

In general, a cyber-physical attack can target each of the components of any cyber-physical system. Indeed, UAV security threats should be analyzed from the perspective of a new type of attack, which dismantles the physical operation of the UAV. Moreover, sensors are critical components for the UAV to receive data about itself and the surrounding environment. Essentially, UAVs rely on the collaboration of various sensors, including GPS. With this crucial sensor, UAV can obtain the obstacle's location, altitude, and other important information related to the flight mission, for the safe and successful completion of a task.

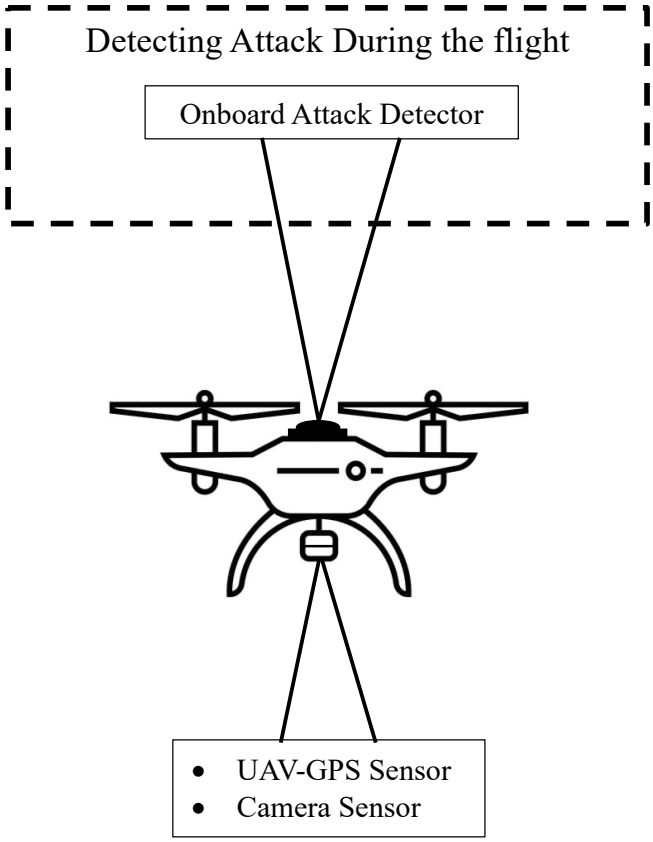


Figure 6.3: The hardware components of the UAV.

Additionally, the GPS sensor provides the necessary data to make sure the UAV reaches its final destination. However, false data leads the UAV to make the wrong decision, affecting flight safety and reliability. It can further cause a catastrophic crash. Therefore, sensor attacks have been categorized as one of the most critical threats in cyber-physical attacks.

6.3.3.1 Threat Model

In this work, our attention is centered on the physical mechanisms of Unmanned Aerial Vehicles (UAVs). Specifically, we explore the strategies for path planning in scenarios where UAVs encounter persistent GPS sensor malfunctions. In addition, false GPS data alters the real data by compromising the integrity and availability of the GPS sensor measurements.

The wrong readings modify the GPS sensor data and feed it into the system, making it unreliable, and thus the estimated state based on the sensor measurements becomes corrupted and untrustworthy.

For example, the value $\mathbf{r(t)}$ can be set to be $\tilde{\mathbf{r}}(\mathbf{t}) \pm \mathbf{e}$ by an attack, where $\mathbf{e}$ is the perturbation/modification value. Another attack scenario can be realized by the attacker through delay of the data sent to the GPS sensor, i.e., $\mathbf{r(t)} = \tilde{\mathbf{r}}(\mathbf{t_0})$ for a time period of $\mathbf{T}$ where $\mathbf{t_0}$ is the start time of the attack, and then $\mathbf{r(t)} = \tilde{\mathbf{r}}(\mathbf{t} - \mathbf{T})$ for $\mathbf{t} \geq \mathbf{t_0} + \mathbf{T}$.

6.3.3.2 GPS Sensor Spoofing/Jamming

The UAV depends on the GPS signals received and processed by the onboard GPS receiver. GPS spoofing attack is the most common attack form where the attackers take control of the UAV by transmitting signals from the satellites to the target UAV. Compared with the spoofing attacks, GPS jamming is more implemented GPS sensor spoofing attacks are directed toward onboard sensors that depend on the outside environment. The goal of this attack is to destabilize UAVs by compromising the sensor by injecting false data. Some attacks try to steal information through security holes of communication links in the system while others aim to spoof sensors, such as GPS spoofing. Therefore, successful attacks will lead to serious consequences [96]. Another example that can be related to the spoofing attack, is to develop acoustic injection attacks on Microelectromechanical Systems (MEMS) accelerometers [97].

6.3.3.3 False GPS Sensor Data Injection

The UAV can be forced to respond to false signals as a result of the GPS sensor attack, and it can completely disrupt its navigation system and mislead the UAV from achieving its goal [98]. Fake GPS sensor data injection targets onboard GPS sensing components such as accelerometers and actuators that are dependent on sensing external environment conditions. Authors in [99] took the UAVs navigation as the example and modeled it as a

stochastic liner CPS system with the Gaussian noise. The purpose of these permanent faults is to destabilize UAVs by compromising a collection of sensors such as GPS and introducing falsified readings into the flight controller, hence jeopardizing the control system and the flight mission of the UAV [100].

6.3.3.4 UAV Authentication and Cybersecurity Measures for GBS Communications

In this chapter, we explore how attackers can significantly impair network performance by disrupting routing mechanisms, leading to packet loss and congestion, which adversely impacts UAV missions. To counter these threats, researchers are developing comprehensive solutions that include both prevention and detection strategies. The primary line of defense, prevention, aims to thwart attacks before they penetrate the system. This involves traditional security practices such as authentication, encryption, and secure routing protocols. However, these measures can sometimes compromise system availability, and the risk of insider threats persists [101].

Detection serves as a secondary but vital line of defense. It focuses on continuous system monitoring to identify any anomalies or ongoing attacks, ensuring timely response to security breaches. This layered approach to security is crucial for maintaining the operational integrity of UAV systems.

One notable advancement in UAV security is the development of a lightweight mutual authentication mechanism, as discussed in [102]. This protocol is pivotal in distributed systems for ensuring the integrity and trustworthiness of communication nodes. It employs a unique challenge-response strategy that leverages a physical unclonable function and chaotic system dynamics to obscure messages and generate a secret session key. The main objective is to ensure the integrity of each packet transmitted along the communication path, thereby facilitating key agreement and mutual authentication between UAVs and between UAVs and their ground stations [103]. This system completes the access control process with

just two message exchanges and is designed to withstand various security threats, including MITM attacks, physical attacks, forgery, insider threats, replay attacks, and threats related to session-specific temporary information. This robust mechanism enhances the security framework, significantly bolstering the defense against sophisticated cyber threats.

6.4 UAV CPS

The physical state of the UAV path planning under GPS permanent faults is addressed in this section. It contains physical and cyber components including computation, communication, and on-board sensors. Figure 6.2 depicts the data flows that begin with the UAV-GPS sensor, which communicates the original data from the UAV to the nearest GBS. Computation modules, analyze and make decisions based on all the acquired information. In our case, the onboard UAV-GPS sensor records all the decisions that the UAV makes. For example, the UAV flies from an initial location following the path plan and at a specific time, the GPS sensor starts being disabled and compromised due to faults. After a short delay, as shown in Figure 6.4.

The system architecture of the UAV includes the GPS procedure based on two main steps. Firstly, the UAV localization method was introduced using the received signal strength trilateration approach, and then we implemented the resilience to cyber-attack artificial potential field algorithm (RCA-APF). In other words, the UAV generates the path plan in the environment with randomly distributed obstacles, where the UAV flies from an initial position to the final destination while it communicates with the GBSs. Due to the GPS false readings, the UAV loses its connectivity with the GBSs. Therefore, location estimation for the UAV is obtained using the received signal strength trilateration.

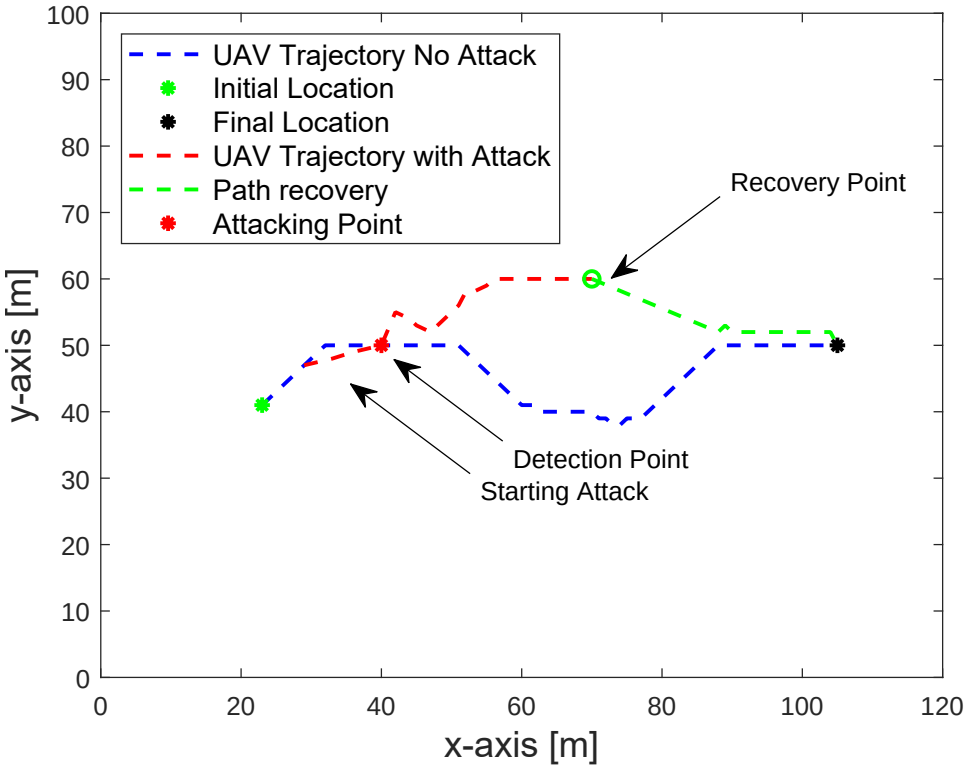


Figure 6.4: The Path planning framework of the UAV at different scenarios.

6.4.1 Received Signal Strength Based Trilateration

To estimate the location of the UAV under the GPS attack, we use a geolocation approach based on the received signal strength (RSS). Essentially, the UAV flies along a trajectory and receives signals from the surrounding ground base stations (GBSs). The RSS traditional model [104] has been implemented to collect those measurements. Using the long-distance path loss propagation model [105], [106], the location-related information measurements are obtained from the RSS, which is generally affected by multi-path effects and NLoS propagation. Furthermore, the location of the UAV can be ideally determined in 2D space with the use of the three GBSs. In general, the average received power P_k associated with the kth GBS can be modeled in dB form as

$$P_k = P_0 - 10\alpha_k \log_{10} d_k + e_{RSS,k}, k = 1, 2, ..., N, \tag{6.4}$$

where P_0 is the reference received average power at a reference distance of 1 meter, α_n denotes the path loss exponent, and $e_{RSS,n}$ represents the error of the RSS measurements. Assuming that P_0 and $\alpha_k, k = 1, 2, ..., K$ are given, the distance between the UAV and each of the GBSs can be estimated. Therefore, the RSS measurement model that comes from the kth GBS and received by the UAV can be derived as follows

$$r_{RSS,k} = P_k - P_0, \tag{6.5}$$

$$q_{RSS}(\mathbf{p}_k, \mathbf{w}) = -10\alpha_k \log_{10} d_k, \tag{6.6}$$

$$r_{RSS,k} = q_{RSS}(\mathbf{p}_k, \mathbf{w}) + e_{RSS,k}, k = 1, 2, ..., N. \tag{6.7}$$

where $r_{RSS,k}$ denotes the RSS measurement associated with the k^{th} GBS, $q_{RSS}(\mathbf{p}_k, \mathbf{w})$ is a nonlinear function which contains all necessary information to calculate the location of the UAV, and $e_{RSS,k}$ represents the measurement error. The main task of RSS-localization is to estimate $\mathbf{w}$ based on the obtained $\{r_{RSS,k}\}_{k=1}^{K}$ in (6.7).

In Figure 6.5, we show the RSS measurements from K GBSs at different locations received by the UAV. Typically, solving nonlinear equations requires the application of nonlinear estimators, which include the nonlinear least squares (NLS), weighted nonlinear least squares (WNLS), and maximum likelihood (ML) estimators [107]. Based on the RSS model (6.7), the cost function of the NLS estimator can be expressed as [108]

$$\begin{aligned} Q_{NLS}(\mathbf{w}) &= \sum_{k=1}^{K} (r_{RSS,k} - q_{RSS}(\mathbf{p}_k, \mathbf{w}))^2 \\ &= (\mathbf{r} - \mathbf{q}(\mathbf{w}))^T (\mathbf{r} - \mathbf{q}(\mathbf{w})), \end{aligned} \tag{6.8}$$

where $\mathbf{r} = [r_{RSS,1}, ..., r_{RSS,K}]^T$ and $\mathbf{q}(\mathbf{w}) = [q(\mathbf{p_1}, \mathbf{w}), ..., q(\mathbf{p_K}, \mathbf{w})]^T$. The solution of NLS

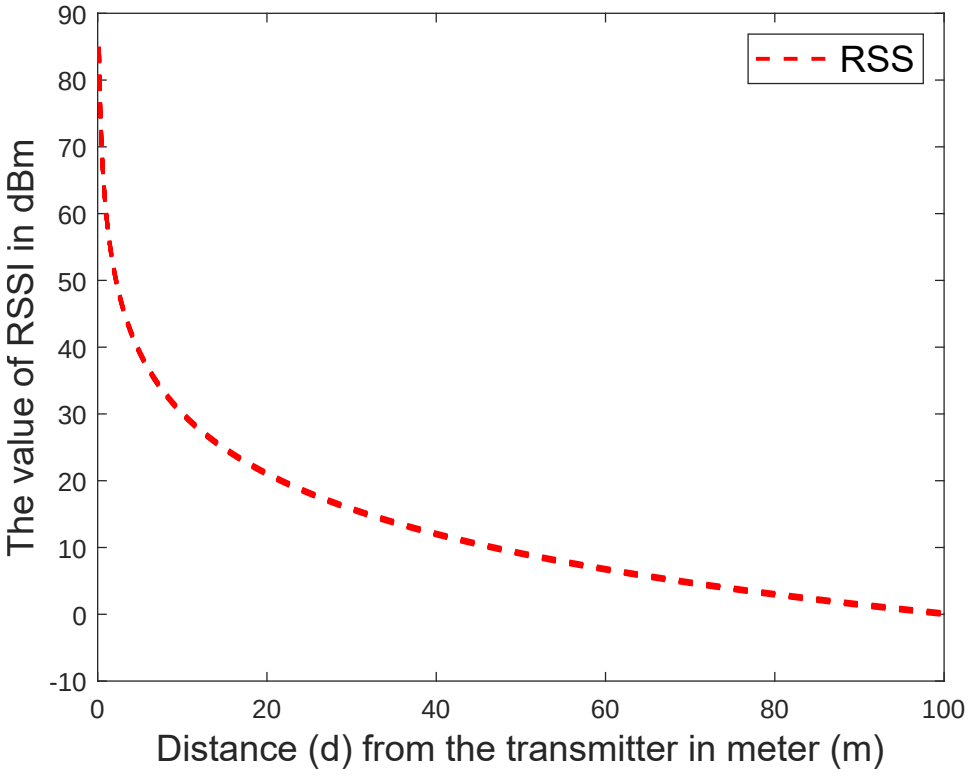


Figure 6.5: RSS values from UAV to GBS.

estimator corresponds to the estimated location $\widehat{\mathbf{w}}$ that minimizes the cost function (6.8), i.e.,

$$\widehat{\mathbf{w}} = \arg\min_{w} Q_{NLS}(\mathbf{w}). \tag{6.9}$$

The NLS estimator does not rely on any assumption about the error statistics. However, when the covariance of the error vector $\mathbf{w} = [e_1, ..., e_K]^T$ is available, we can obtain the WNLS estimator, which can be expressed as [109]

$$\begin{aligned} \widehat{\mathbf{w}} &= \arg\min_{w} Q_{WNLS}(\mathbf{w}) \\ &= \arg\min_{w} (\mathbf{r} - \mathbf{q}(\mathbf{w}))^T \mathbf{C}^{-1}(\mathbf{e})(\mathbf{r} - \mathbf{q}(\mathbf{w})), \end{aligned} \tag{6.10}$$

where $\mathbf{C}(\mathbf{e}) = \mathbb{E}[\mathbf{e}\mathbf{e}^{\mathbf{T}}]$ represents the covariance of $\mathbf{e}$, and $\mathbb{E}[.]$ denotes the expectation opera-

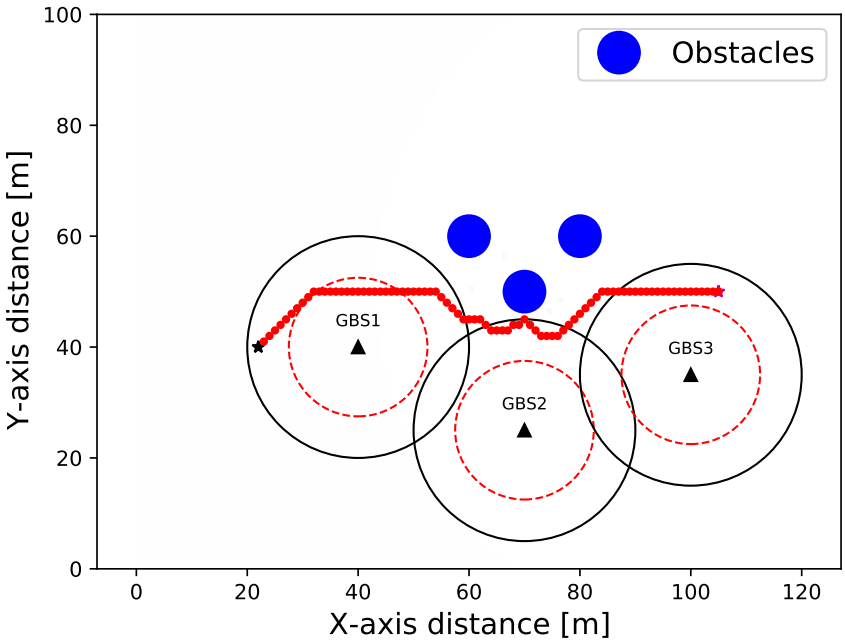


Figure 6.6: The map elements of the system.

tion. In addition, when error probability distribution $P_e(\mathbf{e})$ is known, the ML estimator can be used for location estimation [110],[111]

$$\begin{aligned} \widehat{\mathbf{w}} &= \arg\min_{w} Q_{ML}(\mathbf{w}) \\ &= \arg\min_{w} \log P_e(\mathbf{e})(\mathbf{r} - \mathbf{q}(\mathbf{w})). \end{aligned} \tag{6.11}$$

The errors follow the zero-mean Gaussian distribution, and the WNLS and ML estimators have the same performance. To solve the optimization problems in (6.9), (6.10), (6.11), several approaches exist. For instance, grid search is a reliable method to find the point $\widehat{\mathbf{w}}$ that minimizes the objective function Q.

Moreover, the main advantage of RSS-based localization lies in that time synchronization among different GBSs is not required and RSS measurements are readily available in almost all practical wireless systems. On the other hand, the main drawback of RSS-based approaches is the poor localization accuracy. Also, RSS-based distance estimation can be

challenged due to the unpredictable variations of the channel behavior. However, due to inaccuracy in the RSS localization, we consider a larger obstacle to covering the issue, as shown in Figure 6.6.

6.4.1.1 UAV Localization Using Time of Arrival (TOA)

The primary advantage of RSS-based localization is that it does not require time synchronization among different agents (UAV and GBSs), and RSS measurements are readily available in almost all practical wireless systems. Unlike alternative schemes such as TOA, TDOA, or AOA-based approaches, RSS measurements do not rely on Line-of-Sight (LoS) signal propagation. However, the major drawback of RSS-based methods is their poor localization accuracy, especially in cluttered environments. In these settings, signal attenuation is weakly correlated with distance, resulting in inaccurate distance estimation [112]. Additionally, an accurate signal propagation model is essential for reliable RSS-based distance estimation, which is challenging due to the unpredictable variations in channel behavior.

Another approach for location estimation is the Time of Arrival TOA-based approaches which initially estimate the distances between the UAV and each of the Ground Base Stations (GBSs) by measuring the signal propagation delay or time of flight (TOF), denoted as t_f. Using these distance estimates, they then construct a trilateration model to determine the location of the UAV. TOA-based methods can be further categorized into one-way TOA (OW-TOA) and two-way TOA (TW-TOA), depending on how t_f is defined [113], [114].

For OW-TOA localization, the UAV transmits a packet to the GBS that includes a timestamp, t_s, recording the transmission time. GBS then measures the Time of Arrival (TOA) of the received signal, denoted as t_r. The TOA is commonly measured using matched filtering or correlation techniques, where the TOA measurement is derived from the time shift of the reference signal that produces the highest correlation with the received signals. In OW-TOA localization, if the clocks of the GBSs and the UAV are perfectly synchronized, GBS can determine the time of flight t_f as $t_f = t_r - t_s$, and the distance between UAV and GBS

can be calculated as $d = t_f.c$, where c is the signal propagation speed, typically the speed of light. However, OW-TOA methods have two main drawbacks. First, even a small time synchronization error between the UAV and the GBSs can significantly compromise distance estimation. Second, the transmitted signal must be labeled with a timestamp, increasing the complexity of the signal structure and potentially introducing additional estimation errors.

In contrast, TW-TOA localization involves UAV transmitting a packet to GBS, which responds by sending an acknowledgment packet back to the UAV after a response delay, t_d. If t_d is known, UAV can calculate its distance to GBS based on the signal's round-trip time of flight (RTOF), i.e., $t_{RT} = 2t_f + t_d$. TW-TOA addresses the primary drawback of OW-TOA by eliminating the need for time synchronization between the UAV and GBS. However, in practice, it is challenging for UAV to know the exact response delay t_d. Although t_d can be ignored if it is relatively small compared to t_f in long-range signal propagation, it critically affects performance in short-range scenarios. Moreover, while TW-TOA eliminates clock synchronization errors between the two agents, relative clock drift can still compromise distance estimation accuracy. Additionally, a timestamp is still required for TW-TOA to compute the RTOF of the transmitted signal.

A general TOA-based measurement model can be mathematically expressed as follows [115], [108]:

$$c.t_{f,n} = d_n + e_{TOA}, n = 1, 2, ..., N. \tag{6.12}$$

In this model, $t_{f,n}$ represents the measured Time of Flight (TOF) of signal propagation between the Ground Base Station (GBS) and the UAV. This measurement is typically affected by a positive bias error introduced during the signal measurement process, which is captured by the additional measurement error e_{TOA}. Using similar notations as in (6.7), let $r_{TOA,n} = c \cdot t_{f,n}$ and $h_{TOA}(\mathbf{p_n}, \mathbf{w}) = d_n = \|\mathbf{p_n} - \mathbf{w}\|$. The general model for TOA-based

localization can be expressed as

$$r_{TOA,n} = h_{TOA}(\mathbf{p_n}, \mathbf{w}) + e_{TOA,n}, \quad n = 1, 2, \ldots, N. \tag{6.13}$$

By solving the system of nonlinear equations in (6.13), the location of the UAV can be estimated.

6.4.1.2 Error Analysis in UAV RSS Tolerance Range Measurements

In this chapter, we acknowledge that relying on Received Signal Strength (RSS) measurements for UAV localization is susceptible to environmental factors and communication challenges such as interference, signal attenuation, multipath propagation, and other wireless communication complexities. These factors can indeed affect the accuracy of RSS-based localization methods. As described in Section 2.2, line-of-sight (LOS) propagation is the dominant communication mode between the UAV and each Ground Base Station (GBS). Additionally, we assume that the UAV is flying at a moderate altitude of 60 meters. According to the 3rd Generation Partnership Project (3GPP) technical report TR 36.777 [116], at moderate to high altitudes, UAVs are more likely to maintain a Line of Sight (LoS) with the Ground Base Stations (GBS). LoS conditions are favorable for communication as they typically result in lower path loss and better signal quality. Hence, in the presence of a relatively strong LoS link, the impact of interference and multipath propagation diminishes, and RSS measurements are not substantially affected by these factors.

Regarding the assumption of fixed altitudes for the UAV, we acknowledge that this may limit the applicability of our approach in diverse and complex environments. This assumption was made to simplify the initial model and focus on the core aspects of our algorithm. However, we recognize the importance of addressing the dynamic nature of UAV operations.

Concerning the acceptable error range for our system, it is primarily influenced by the

performance of the RSS-trilateration estimation method, which can exhibit considerable variation depending on the specific application and deployment environment. In this work, we have focused on a relatively straightforward environment characterized by moderate-altitude UAV flight. Under ideal circumstances, RSS trilateration achieves sufficient accuracy within a few meters. However, when operating in more challenging environments with significant interference and multipath effects, the error margin may expand to tens of meters. A relevant study conducted in [18] the error associated with localization estimation, particularly focusing on the analysis of RSS errors. This study formulated an analytical expression for the RSS localization error, demonstrating that the precision of range-based RSS localization is contingent upon crucial environmental factors.

6.4.1.3 RSS-based Trilateration

Trilateration determines the location of the UAV under attack using distance-related signal measurements for multiple GBSs. In other words, the UAV would be located at the intersection of the three circles with the centers being the locations of the GBSs and radii equal to the distances from the UAV to each of the GBSs. The locations of the GBSs are known and their distances to the UAV can be determined based on the RSS measurements [117], [118], [119], [112]. Furthermore, the RSS measurements from all GBSs are calculated and then converted into distances. Based on this distance, the system trilaterates the UAV location as illustrated in Figure 6.7. The trilateration method uses RSS measurement values to calculate the distance between the UAV and GBSs. The location of the UAV $[x_u, y_u]$ needs to be computed, then the formulated circles are calculated using mathematical computations. Assuming $z = 0$ and to simplify the calculations, the equations are formulated so that the intersection of circles occurs at the Cartesian plane. The equation for each circle can be expressed as [120]

$$(x_u - x_k)^2 + (y_u - y_k)^2 = d_k^2. \tag{6.14}$$

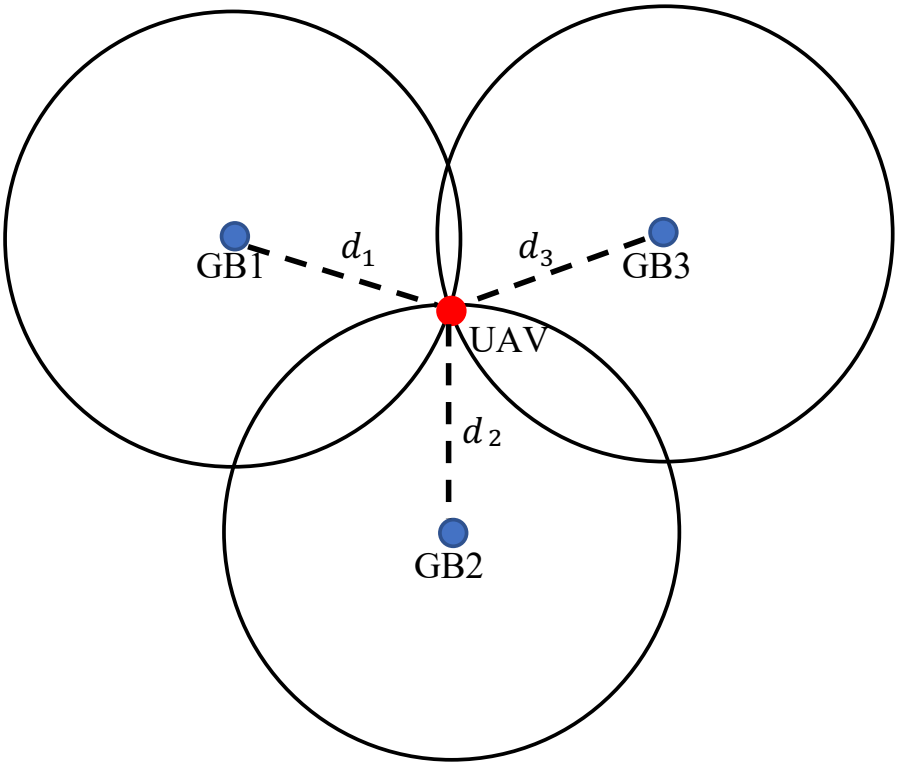


Figure 6.7: RSS-based localization, where d_k, $k = 1, 2, 3$, denote the actual distances from the UAV to each of the GBS.

where (x_k, y_k) denotes the location of the kth GBS.

The intersection of three circles is obtained by solving systems of linear equations for two variables simultaneously. Hence, by solving the linear systems, the location of $[x_u, y_u]$ can be determined. The accuracy of coordinate $[x_u, y_u]$ depends on the measurement of RSS values.

6.4.2 UAV Estimated Location Based On Three GBSs

Given the three GBSs coordinates $W_1 = [x_1, y_1]$, $W_2 = [x_2, y_2]$, $W_3 = [x_3, y_3]$ and the distance measurements d_1, d_2, and d_3 as shown in Figure 6.7. The UAV coordinates $L_u = [x_u, y_u]$ can be calculated by finding the solution to the following system of quadratic equations: [121]

$$(x_u - x_1)^2 + (y_u - y_1)^2 = d_1^2 \tag{6.15}$$

$$(x_u - x_2)^2 + (y_u - y_2)^2 = d_2^2 \tag{6.16}$$

$$(x_u - x_3)^2 + (y_u - y_3)^2 = d_3^2 \tag{6.17}$$

Equations (6.15), (6.16), and (6.17) can be rearranged and represented in matrix as:

$$\begin{bmatrix} 1 & -2x_1 & -2y_1 \\ 1 & -2x_2 & -2y_2 \\ 1 & -2x_3 & -2y_3 \end{bmatrix} \begin{bmatrix} x^2 + y^2 \\ x \\ y \end{bmatrix} = \begin{bmatrix} d_1^2 - x_1^2 - y_1^2 \\ d_2^2 - x_2^2 - y_2^2 \\ d_3^2 - x_3^2 - y_3^2 \end{bmatrix} \tag{6.18}$$

Thus, (6.18) is the matrix equation and which can be written as:

$$\mathbf{A_0}.\mathbf{x} = \mathbf{b_0}; \quad \mathbf{x} \in E = \{(x_0, x_1, x_2, x_3)^T \in \mathbb{R}^4 : x_0 = x_1^2 + x_2^2 + x_3^2\} \tag{6.19}$$

The UAV flies each time step updating its coordinate at different locations. Therefore, equation (6.19) does not lie on a straight line and the solution can be given by:

$$\mathbf{x_1} = \mathbf{x_k} + t_1\mathbf{x_i} \tag{6.20}$$

$$\mathbf{x_2} = \mathbf{x_k} + t_2\mathbf{x_i} \tag{6.21}$$

where t_1 and t_2 are real parameters that can be calculated using a quadratic equation $t_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. x_k and x_i are the particular and homogeneous solutions, respectively. The solution for the trilateration estimation values for the UAV based on three GBSs locations is given by

$$UAV_1 = \mathbf{x}_1\mathbf{I}, \quad UAV_2 = \mathbf{x}_2\mathbf{I},$$
$$\text{where } \mathbf{I} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{6.22}$$

6.4.3 RCA-APF Algorithm

6.4.3.1 Artificial Potential Field Algorithm

The Artificial Potential Field (APF) method offers a straightforward yet efficient technique for the motion planning of unmanned vehicles. The APF algorithm is capable of encapsulating comprehensive environmental data, including obstacles, the destination, and other entities within the vicinity. Our focus is on a solitary UAV navigating towards a target point within a three-dimensional space, assuming a relatively uncomplicated setting characterized by a singular objective and several obstacles. To address the issue of local minima, we employ the strategy outlined in [59], incorporating extra terms for the attractive potential field and adjusting the potential field configuration to ensure the UAV circumvents any halt between obstacles and the target. The UAV navigates along the horizontal plane, maintaining a 2D position denoted as $\mathbf{L}_u = [x_u(t), y_u(t)]^T$ at any time t. The destination is stationary, located at $\mathbf{L}_g = [x_g, y_g]^T$. Consequently, the attractive potential function for a single UAV is defined as per [122].

$$J_{att}(\mathbf{L}_u) = q_{att}\frac{(\mathbf{L}_u - \mathbf{L_g})^2}{2}. \tag{6.23}$$

The single UAV case is similar to the attractive potential function of the traditional APF. The attractive force of the UAV $F_{att}(\mathbf{L}_u)$ is the negative gradient of the attractive potential

function given as

$$F_{att}(\mathbf{L}_u) = -\nabla J_{att}(\mathbf{L}_u) = -q_{att}(\mathbf{L}_u - \mathbf{L_g}). \tag{6.24}$$

The additional field function helps the UAV to avoid the local minimum point by pulling it toward the target. The additional field force $J_{add}(\mathbf{L}_u)$ is given by [59]

$$J_{add}(\mathbf{L}_u) = \begin{cases} \frac{q_{add}}{2}\left[(\mathbf{L_u} - \mathbf{L_g}) - \mathbf{p_{add}}\right]^2 & , \parallel \mathbf{L_u} - \mathbf{L_g} \parallel \leq \mathbf{p_{add}}\,, \\ 0 & , \parallel \mathbf{L_u} - \mathbf{L_g} \parallel > \mathbf{p_{add}}\,. \end{cases} \tag{6.25}$$

where q_{add} is the additional field coefficient, $\parallel \mathbf{L_u} - \mathbf{L_g} \parallel$ is the distance between the UAV and the goal, $\mathbf{p_{add}}$ is the impact of the field on the distance between the UAV and the goal.

The additional field force $F_{add}(\mathbf{L}_u)$ is represented as follows:

$$F_{add}(\mathbf{L_u}) = -\nabla[J_{add}(\mathbf{L_u})] = \begin{cases} q_{add}\left[(\mathbf{L_u} - \mathbf{L_g}) - \mathbf{p_{add}}\right] & , \parallel \mathbf{L_u} - \mathbf{L_g} \parallel \leq \mathbf{p_{add}}\,, \\ 0 & , \parallel \mathbf{L_u} - \mathbf{L_g} \parallel > \mathbf{p_{add}}\,. \end{cases} \tag{6.26}$$

The modified repulsive potential function, which takes the relative distance between the UAV and the target into consideration is given as

$$J_{rep}(\mathbf{L_u}) = \begin{cases} \frac{q_{rep}}{2}\left(\frac{1}{\mathbf{L_u} - \mathbf{L_0}} - \frac{1}{\mathbf{p_0}}\right)^2 & , \parallel \mathbf{L_u} - \mathbf{L_0} \parallel \leq \mathbf{p_0}\,, \\ 0 & , \parallel \mathbf{L_u} - \mathbf{L_0} \parallel > \mathbf{p_0}\,. \end{cases} \tag{6.27}$$

The repulsion force function $F_{rep}(\mathbf{L_u})$ for the single UAV is given by

$$F_{rep}(\mathbf{L_u}) = -\nabla[J_{rep}(\mathbf{L_u})] = \begin{cases} q_{rep}(\frac{1}{\mathbf{L_u} - \mathbf{L_0}} - \frac{1}{\mathbf{p_0}})\frac{1}{(\mathbf{L_u} - \mathbf{L_0})^2} & , \parallel \mathbf{L_u} - \mathbf{L_0} \parallel \leq \mathbf{p_0}\,, \\ 0 & , \parallel \mathbf{L_u} - \mathbf{L_0} \parallel > \mathbf{p_0}\,. \end{cases} \tag{6.28}$$

As demonstrated in equations (6.27) and (6.28), the formulations closely mirror the original APF. The pivotal modification lies in the introduction of an extra force, ensuring the UAV's evasion of local minimum points. The complete potential field encountered by the UAV at each step can be expressed as follows:

$$J_{\mathbf{L_u}} = \sum_{r=1}^{i} J_{rep}(r) + \sum_{l=1}^{t}[J_{att}(l) + J_{add}(l)] \tag{6.29}$$

where i is the number of obstacles, and t is the number of the goals. Similarly, the total force that affects the UAV and applies to multiple targets and obstacles is given as follows:

$$F_{\mathbf{L_u}} = \sum_{r=1}^{i} F_{rep}(r) + \sum_{l=1}^{t}[F_{att}(l) + F_{add}(l)]. \tag{6.30}$$

There are other factors that can affect the performance of the RCA-APF algorithm.

Drawing from the equations outlined in the preceding section, we have devised an iterative algorithm to determine the optimal UAV trajectory using the RCA-APF method. At each iteration, the UAV computes the attractive and repulsive potential field functions, thereby gathering essential data regarding the location of the target, obstacles, and Ground-Based Stations (GBS). Within a compact grid of size $[s \times s]$, the UAV deliberates its subsequent maneuver. The operational geographic expanse of our system is demarcated as $[M \times Z]$.

The UAV is equipped with a repertoire of eight possible movements to navigate from its starting point to the intended target. The matrix's rows and columns correspond to the

Algorithm 3 RCA-APF Algorithm for Single UAV Path Planning

Input:Initial location $\mathbf{L_s}$, final location $\mathbf{L_g}$, position of GBS W_k, position of obstacles $\mathbf{L_o}$, attraction gain coefficient q_{att}, repulsive gain coefficient q_{rep}, additional field coefficient q_{add}, UAV height H_u, RSS-based Trilateration measurement values
Output:path planning of the UAV $\boldsymbol{P}$
for j = 1 : J **do**
  for s = 1 : S **do**
    calculate equation (6.23), (6.25) and (6.27) for given input
    calculate the total force potential field (6.30)
    while $d_k(t)$, $d_j(t) \geq [q \times q]$ **do**
      for each UAV step **do**
        Update $x_u(t)$ and $y_u(t)$
        if $x_u(t)$, $y_u(t) < 0$ or $x_u(t)$, $y_u(t) > [M \times Z]$ **then**
          Break;
        end if
        Update UAV coordinate $x_u(t)$ and $y_u(t)$
      end for
    end while
    if the UAV have reached the final location $\mathbf{Z_g}$ **then**
      Break;
    end if
  end for
  return $\boldsymbol{x_u, y_u}$;
  for i = 1 : I **do**
    each UAV $\boldsymbol{(x_u, y_u)}$ step; calculate distances using equations (6.15), (6.16), and (6.17), calculate the RSS values (6.7)
    for each UAV RSS value **do**
      calculate UAV estimated value $\boldsymbol{(x_{ues}, y_{ues})}$ equation (6.11)
    end for
  end for
  return $\boldsymbol{x_{ues}, y_{ues}}$;
  for calculated inputs $\boldsymbol{(x_u, y_u)}$ and $\boldsymbol{(x_{ues}, y_{ues})}$ start to implement the path planning using an open-source simulator
end for
return $\boldsymbol{P}$;

UAV's x_u and y_u coordinates, respectively. The intricacies of the algorithm are encapsulated in Algorithm 1. It is important to note that this algorithm evolves from the conventional APF algorithm.

6.4.3.2 RCA-APF Algorithm Description

Based on the equations in the previous sections, we construct an iterative RCA-APF algorithm for the best UAV path planning. Initially, we calculate the UAV path planning using a modified version of the traditional artificial potential field algorithm. Specifically, at every move of its journey, the UAV actively computes the attractive and repulsive potential field

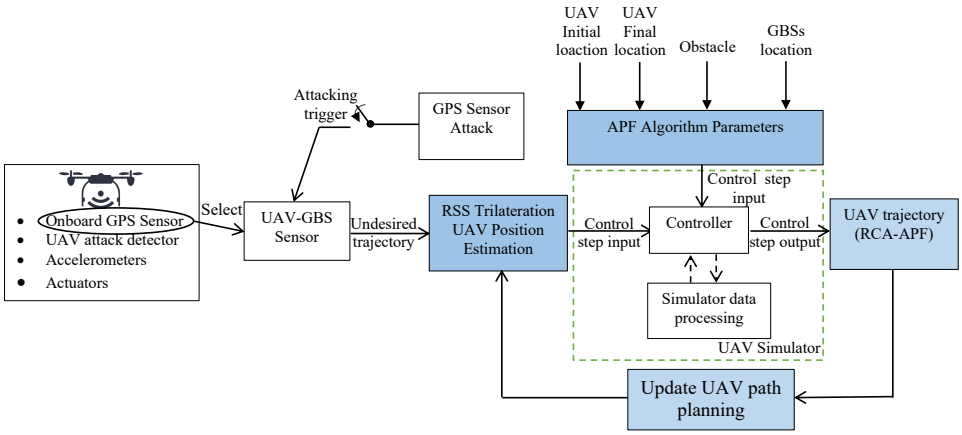


Figure 6.8: Architecture of the proposed approach.

functions. This process enables the UAV to assimilate critical data regarding the positions of the target, any obstacles in the vicinity, and Ground-Based Stations (GBSs). Operating within a confined grid space measured at $[q \times q]$, the UAV assesses and selects its forthcoming course of action. The system's operational terrain is designated as $[M \times Z]$. From the onset of its mission, the UAV is presented with a selection of eight directional choices to navigate towards its ultimate goal. At this point of the RCA-APF algorithm, the UAV coordinates (x_u, y_u) will get calculated and updated for the next iterative loop. The UAV coordinates will be constructed as a matrix representing x_u values for the rows and y_u values for the column, respectively. We calculat the UAV positions at each time step and we use the trilateration estimation localization technique to estimate the location of the UAV. The implementation of the trilateration algorithm is combined with the RCA-APF algorithm. For the fixed coordinate values of each of the GBSs, we calculated the distances from the UAV at each time step to the GBSs. In addition, we computed the received signal strength between UAV and GBSs. From the measured distances for each GBS, the algorithm finds the coordinates that minimize the error function and returns the most optimal solution of the estimated location coordinates (x_{ues}, y_{ues}) of the UAV. The specifics of the algorithm are concisely explained in Algorithm 1. It is noteworthy to mention that this algorithm evolves from the conventional Artificial Potential Field (APF) algorithm. The path planning is computed to be used as

a reference to the UAV simulator. In the final iteration of the RCA-APF algorithm, we applied both calculated and estimated coordinates of the UAV as input to an open-source UAV simulator implementing UAV path planning scenarios. The UAV simulator is based on Python Dynamics, which is a toolkit made to enable the study of multibody dynamics. The simulator is built on multiple packages. The main functionality of the UAV simulator is to initialize the UAV with various parameters and conditions. Also, the simulator includes a control algorithm that is strongly inspired by the PX4 multicopter control algorithm. It is a cascade controller, where the position error (difference between the desired position and the current position) generates a velocity setpoint, the velocity error then creates a desired thrust magnitude and orientation, which is then interpreted as a desired rotation (expressed as a quaternion). Figure 6.8, depicts the workflow of the proposed RCA-APF algorithm.

6.5 Simulation Results and Analysis

In this section, we show the UAV's behavior with GPS permanent faults and the effectiveness of the proposed algorithm by conducting experiments and simulations on different path planning of the UVA at different environment setups. Also, we consider the UAV communicates with the nearest GBS to receive all the information about the current location of the UAV at each time step.

To illustrate the concepts and the algorithm discussed in this chapter, we present and show simulation results to demonstrate how the RCA-APF algorithm operates. We conduct multiple experiments and set up the appropriate values for the parameters. To facilitate the simulation, the UAV is set to fly at a known altitude, which is fixed throughout the entire simulation. We run the simulation using an open-source UAV simulator. Also, we provide 2D plan implementation of the UAV path planning. In the simulations, the UAV path is generated based on an input to the UAV simulator, $\mathbf{v} \leq 5m/s$, and flight altitude is $60m$. In addition, the time flying off the UAV varies based on the path planning time delay.

We have further explained the robustness of our UAV path-planning algorithm, particularly focusing on its obstacle avoidance capabilities, which, alongside permanent fault detection and recovery, stands as one of its primary functionalities. To this end, we have designed and executed several additional experiments under a variety of environmental conditions. The outcomes of these experiments are comprehensively detailed in Table 6.1.

Table 6.1 shows the success rates of UAV missions conducted across various scenarios, each uniquely characterized by a varying number of obstacles while maintaining a constant configuration of three Ground Base Stations (GBSs). The presence of three GBSs across all scenarios is a strategic choice, reflecting a realistic density of navigational aids that a UAV might typically have access to. Moreover, we define the success rate as the proportion of missions in which the UAV successfully navigates to its intended destination without incurring collisions or deviating significantly from its planned trajectory. To ensure the reliability and accuracy of our success rate, we ran our algorithm to a rigorous testing protocol, executing the experiment a total of 100 times for each obstacle scenario. Upon analyzing the data, we observed a clear trend: as the number of obstacles increased, the success rate tended to decrease. This was expected, as more obstacles present a greater navigational challenge.

Number of obstacles	Number of GBSs	Number of Iteration	Success Rate (%)
10	3	100	98
25	3	100	85
50	3	100	74.5
75	3	100	60
100	3	100	50

Table 6.1: Success/Failure Rates of the UAV.

In Figure 6.9, we demonstrate a 2D path planning design of a single UAV. The UAV flies from an initial location to its final destination with obstacle collision avoidance integrated into the system. The obstacles are generated in a way that fits with the setup framework. Furthermore, the framework includes the GBSs located at fixed positions to maintain con-

nectivity with the UAV during the mission. The figures show a different number of obstacles. Indeed, the obstacles are randomly distributed with mean and variance. We run the experiment with 25 and 75 obstacles. In an environment with more obstacles, the UAV has failed to reach the final location. Indeed, the obstacles are randomly distributed with mean $\mu = 0$and variance $\sigma = 0.01$.

In Figure 6.10, we illustrate two distinct scenarios of UAV path-planning. These scenarios compare the actual UAV path planning with a trajectory estimated using the RSS-trilateration method. Specifically, Figure 6.10 (a) depicts the intended UAV trajectory in blue, while the estimated trajectory derived from RSS-trilateration is shown in red. The comparison demonstrates the efficacy of the RSS-trilateration estimation algorithm, as it closely mirrors the desired trajectory.

Extending this analysis to Figure 6.10 (b), we observe a scenario where, despite the UAV's inability to reach its final destination, the RSS-trilateration estimation remains accurate and reliable. This is evidenced by the red trajectory, which is based on RSS-trilateration, closely following the actual path taken by the UAV until its early termination. The consistency of the RSS-trilateration algorithm's performance in both scenarios underscores its robustness and potential applicability in real-world UAV navigation systems.

6.5.1 UAV Simulator

To validate our results, we used an open-source Quadcopter simulator. In that simulator, we implemented a simple scenario with a single UAV flying from the initial location to the final destination. The Quadcopter simulator provides a simple working simulation of the quadcopter's dynamics and a simple controller that can handle position control and supports minimum snap (but also minimum velocity, acceleration, and jerk) trajectory generation. The UAV's orientation is based on two frames: the first one is the X direction North, Y East, and Z Down. The second frame is the X direction East, Y North, and Z Up. Also, the simulator uses the quaternion for the UAV's rotation. Different trajectories can be selected,

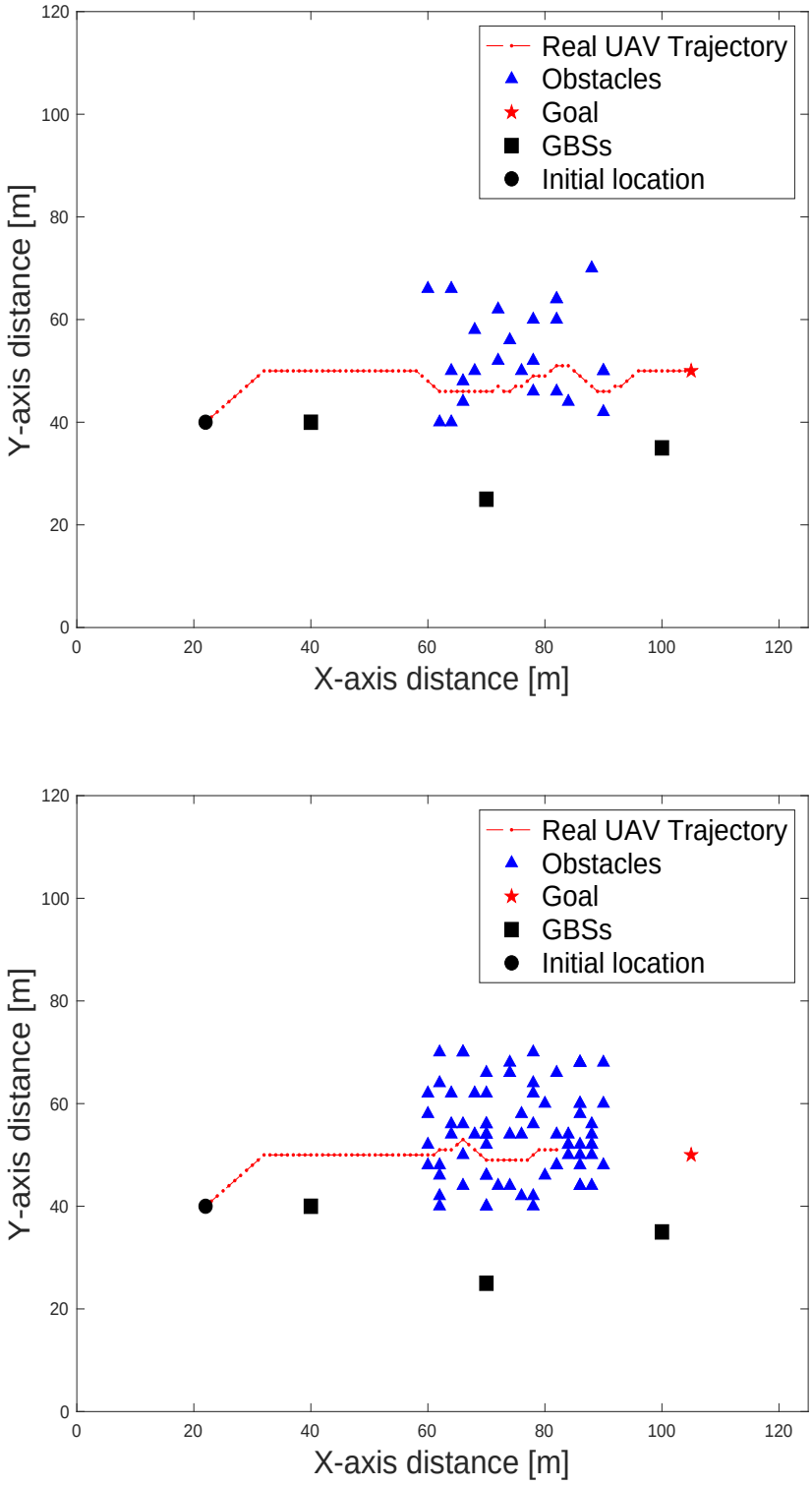
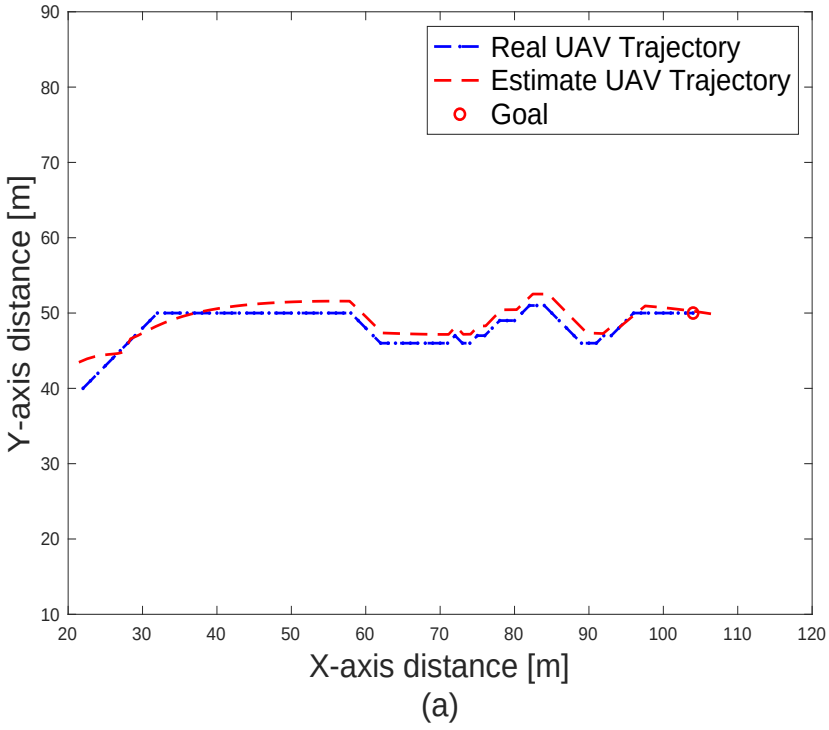


Figure 6.9: The path planning of the UAV with a different number of obstacles.



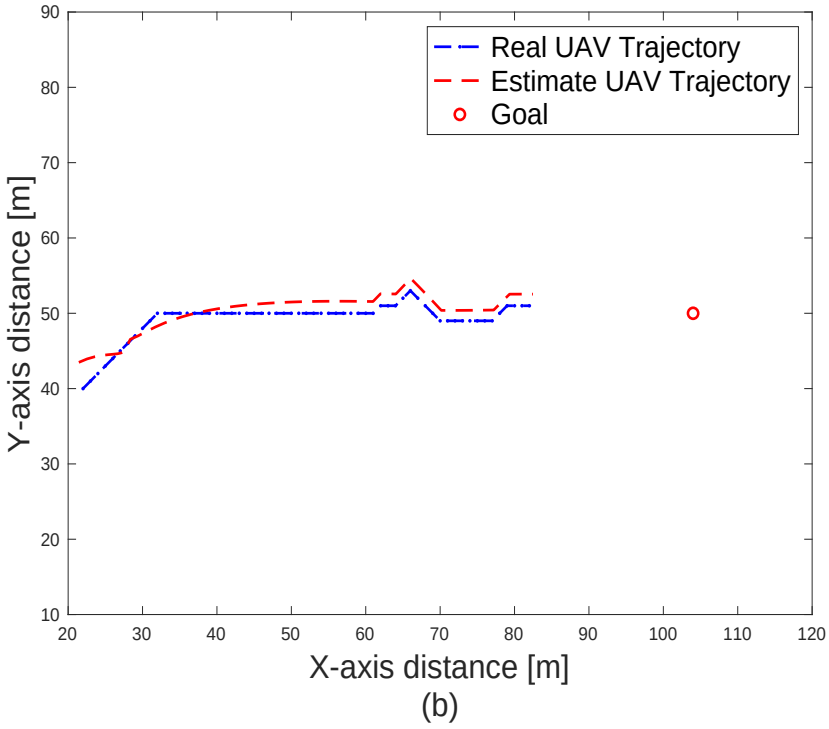


Figure 6.10: The path planning of the UAV with the estimated path planning.

for both position and heading. Using the simulator, we can set the desired position and heading waypoints, and the time for each waypoint. We can select to use each waypoint as a step, interpolate between waypoints, or generate a minimum velocity, acceleration, jerk, or snap trajectory. The controller of the Quadcopter simulator is the most critical part. There are three controllers: one to control XYZ positions, one to control XY velocities and Z position, and one to control XYZ velocities. In all 3 current controllers, it is also possible to set a Yaw angle (heading) setpoint. The control algorithm is strongly inspired by the PX4 multicopter control algorithm. It is a cascade controller, where the position error (difference between the desired position and the current position) generates a velocity setpoint, the velocity error then creates a desired thrust magnitude and orientation, which is then interpreted as a desired rotation (expressed as a quaternion). The source code is available at `https://github.com/bobzwik/Quadcopter_SimCon`.

It should be noted that the UAV encounters a certain delay in detecting attacks, a critical metric that is essential for assessing the effectiveness of our system. We have conducted additional experiments to measure this delay, which is the time duration from the initial data point of an attack being observed to the point where our system successfully identifies the attack. Particularly, we utilized an open-source simulation tool to implement and test the attack/recovery scenario. It is important to note that the delay in attack detection observed in these simulations is influenced by the performance capabilities of the computing device, particularly the GPU and CPU specifications. To provide a more thorough insight into this aspect, for each system, we executed the simulation 10 times to ensure statistical reliability and to mitigate any anomalies or outliers in the data. After each run, we meticulously recorded the time taken by the attack detection mechanism to identify the breach. This process involved measuring the interval from the initial indication of an attack to the point where our system successfully recognized and flagged the anomaly. Below, Table 6.2 summarizes the results of these experiments:

The modeling of our attack detector is intricately designed around the RCA-APF algo-

Processor	**GPU Specs**	**CPU Specs**	**Average Attack Detection Delay**
Intel Core i9	Intel UHD Graphics 630	2.4 GHz 8-core	16.32 sec
Apple M1 Max	Integrated Apple GPU	10-core CPU	10.45 sec

Table 6.2: Attack delay table.

rithm. This setup encompasses a comprehensive environment configuration, precise parameter tuning, and a realistic representation of potential obstacles. Utilizing an open-source simulator, we have meticulously adapted and fine-tuned various parameters to accurately replicate scenarios where a UAV deviates from its intended flight path due to an external attack. In these simulated scenarios, the attack detector is integrated into the UAV's system. Its primary role is to promptly identify any form of attack that causes trajectory deviation. The moment an attack-induced diversion is detected, our RCA-APF algorithm is triggered to initiate an immediate recovery process. This process is designed to swiftly reorient the UAV back to its original course, thereby mitigating the impact of the attack. Our modifications to the simulator parameters include adjustments to the UAV's response sensitivity to external disruptions, the threshold levels for attack detection, and the dynamic recalibration of the UAV's pathfinding algorithms post-attack detection. These enhancements enable us to simulate with high fidelity the UAV's behavior under attack conditions and to rigorously test the efficacy of our attack detection and recovery mechanism. This comprehensive setup not only demonstrates the robustness of our attack detector in identifying and responding to trajectory deviations but also underscores the effectiveness of the RCA-APF algorithm in ensuring the UAV's swift return to its intended path post-attack.

In our experiments, the implementation of the attack detector, based on the RCA-APF algorithm, was conducted in a controlled simulation environment designed to mimic real-world UAV operational scenarios. We utilized a sophisticated open-source UAV simulator that allowed us to create the attack scenario. This includes a GPS attack, which could

potentially divert the UAV from its intended path. In addition, the attack detector was integrated into the UAV's onboard system within the simulator. This integration was crucial to ensure that the detector had access to real-time flight data, including the UAV coordinates, flight speed, and trajectory information. Also, we configured specific parameters within the simulator to define the attack detection threshold. This involved setting up conditions under which the UAV would be considered under attack, such as sudden deviations from the planned path. Following the detection of an attack, our RCA-APF algorithm was automatically activated. This algorithm then recalculated the optimal path to ensure the UAV returned to its original trajectory. Throughout the experiments, data was collected on the response time of the attack detector, the accuracy of attack detection, and the effectiveness of the recovery path. This data was crucial for evaluating the performance of our system under various parameters. The experiments were conducted iteratively, allowing us to refine the attack detection parameters and recovery algorithms based on the outcomes of each test. This iterative process was key to enhancing the robustness and reliability of our system.

In Figure 6.11, we present an overhead view of a 3D path planning simulation for a UAV navigating in an environment with obstacles. This simulation is derived from an enhanced version of the original Quadcopter Simulation and Control program, to which we have integrated a reference UAV path planning algorithm with no attack. The modifications enable the simulator to generate a realistic depiction of the UAV's trajectory based on the provided input parameters.

Specifically, Figure 6.11 demonstrates the UAV's path planning capabilities in an attack-free scenario. This allows us to observe the UAV's trajectory as it smoothly progresses from its initial location to the intended destination, strictly adhering to the pre-calculated trajectory determined by our algorithm. The simulation, conducted in such an idealized setting, serves as a benchmark for evaluating the UAV's navigational proficiency and the path planning algorithm's efficacy under optimal conditions. In addition, the simulation results depicted in Figure 6.11 not only demonstrate the UAV's adherence to the predefined

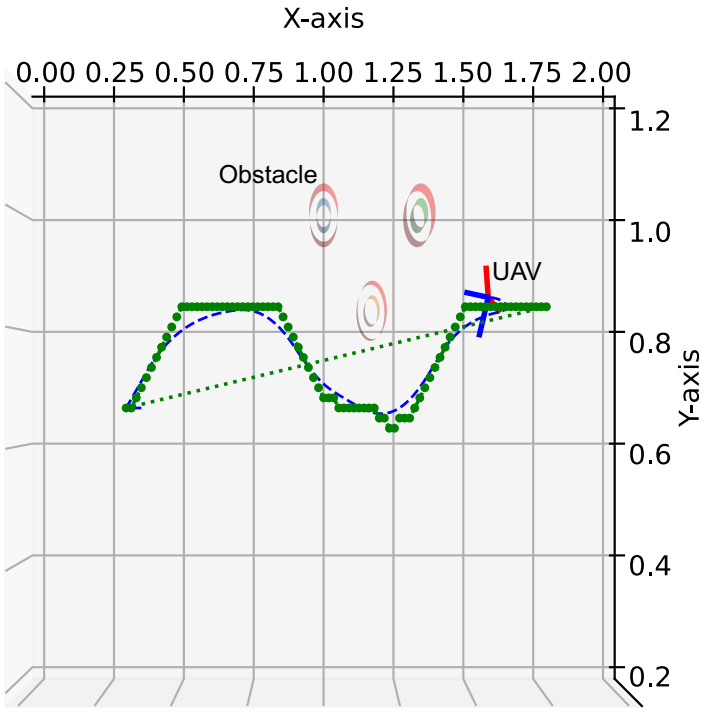
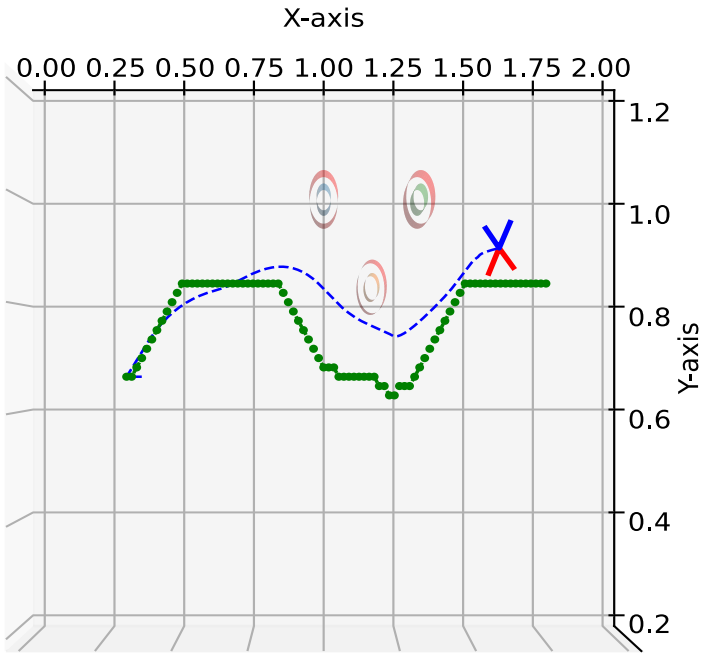


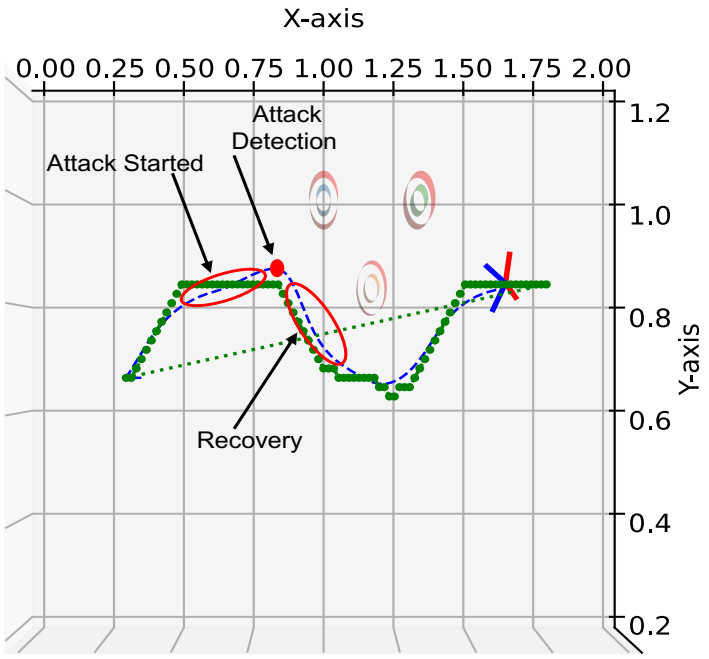
Figure 6.11: UAV Path planning simulation with no attack.

trajectory but also underscore the precision and robustness of our path planning algorithm. It is evident from the UAV's flight pattern that the trajectory is followed with remarkable accuracy, highlighting the algorithm's capability to navigate with minimal deviation from the set course. This fidelity to the planned route is indicative of the algorithm's sophisticated design, which accounts for various flight dynamics and environmental factors to ensure a seamless navigation experience.

In Figure 6.12, we show a comparative visual analysis of two scenarios that highlight the resilience and adaptability of our algorithm in UAV path planning simulations. Figure 6.12 (a) depicts the UAV's path when it encounters a hostile attack and lacks any recovery protocols. This particular depiction serves to illustrate the vulnerability of the UAV's trajectory to external disruptions, which can lead to significant deviations from the intended path or, in some cases, result in the failure to complete the mission. The trajectory shown reveals the



(a)



(b)

Figure 6.12: UAV Path planning simulation with (a) attack and no recovery, (b) attack and recovery.

extent to which adversarial interference can compromise the UAV's operational integrity and underscores the necessity for robust countermeasures within the path planning framework. In contrast, Figure 6.12 (b) illustrates the UAV's trajectory under the condition of an external attack, which is initiated at a specific time and location during the flight. The system is designed to detect such an attack within a brief time frame, triggering the activation of the recovery protocol embedded within our algorithm. This sequence of events sets the stage for a critical evaluation of the recovery mechanism's robustness. The subsequent path of the UAV, as shown in Figure 6.12 (b), serves as a testament to the resilience of the recovery protocol. Despite the initial disruption, the UAV is not only able to detect and respond to the attack but also to recalibrate its course effectively. This realignment with the pre-planned route is a crucial demonstration of the algorithm's dynamic response capabilities. The UAV's successful navigation back to its intended trajectory and ultimate arrival at the target destination.

Moreover, the UAV's successful completion of its mission, as shown in the simulation, is proof of the algorithm's operational effectiveness. The algorithm's ability to guide the UAV through its journey with or without interference showcases its potential for real-world applications where reliability and precision are paramount. The UAV's performance, in this case, reflects a well-synchronized harmony between the algorithm's theoretical underpinnings and practical execution, paving the way for its deployment in more complex and dynamic environments.

6.6 Conclusions

As shown in this work, the cyber-physical nature of UAVs demands an extension to the scope of ordinary vulnerability analysis for such systems. In addition to threats in the computational components such as the GPS sensor and detectors, a largely overlooked class of vulnerabilities is fostered by the interactions between the computational systems and

electrical and mechanical components. Pondering the list of UAV attacks, we started to investigate some of these computational threats where we have determined strategies and policies for path planning of the UAV under GPS performant faults. In the considered setting, we have developed a path planning procedure based on three stages: firstly, we use the modified artificial potential field algorithm to find the best path planning of the UAV, which flies in a complex environment with obstacles and GBSs. Secondly, we used the RSS trilateration localization approach to estimate the location of the UAV under GPS permanent faults. The RSS trilateration localization measurements helped us to estimate the location of the UAV at every step. Finally, combining the first two steps, we implemented the RCA-APF algorithm considering a single UAV. Simulation and experiment results have demonstrated the path-planning conditions under which the UAV can reach its final destination. Finally, we validate the feasibility of our design using a path-planning UAV simulator. Future work will show more complex environments including multiple path planning for several UAVs.

Chapter 7

Conclusion

7.1 Dissertation Summary & Conclusion

7.1.1 Antenna Pattern Aware UAV Trajectory Planning Using Artificial Potential Field

In this study, we have presented and implemented a sophisticated variant of the Artificial Potential Field (APF) algorithm, specifically designed for the navigation of both individual and grouped UAVs. This enhanced algorithm enables the generation of optimal flight paths that enhance both operational efficiency and safety. Our method comprehensively addresses the challenges associated with obstacle avoidance and the prevention of in-flight collisions among UAVs—key factors for effective swarm operations. Additionally, we have explored the subtle impacts of antenna radiation patterns on the optimization of flight paths, demonstrating how these technical elements crucially affect trajectory planning to maintain strong communication links.

The simulation results have been enlightening, demonstrating the algorithm's effectiveness in directing UAVs accurately to their intended destinations. These findings highlight the algorithm's proficiency in sustaining vital communication links with ground stations and other UAVs, while adeptly maneuvering around obstacles and mitigating potential aerial

conflicts. This equilibrium is essential for the successful real-world application of UAVs in complex scenarios, emphasizing the importance of operational reliability and safety.

7.1.2 Cyber-Physical Attack on UAV Systems

Historically, security assessments for Unmanned Aerial Vehicles (UAVs) have been categorized into two distinct areas: flight safety and information security. However, with the increasing complexity of cyber-physical system (CPS) integration within UAVs, cyber-attacks that target these systems not only threaten data integrity but also lead to incorrect control commands. Such incursions critically compromise both the safety and operational reliability of UAVs. It is therefore crucial to explore the ripple effects of security threats from the informational to the physical realm, understanding how cyber vulnerabilities can translate into real-world risks.

In this study, we have provided a comprehensive overview of the evolving security landscape for UAVs, emphasizing the intertwined nature of cyber and physical threats. Our holistic examination of how cyber-attacks impact physical operations is central to this research, providing key insights for the security assessment of broader CPS frameworks. This approach underscores the need for an integrated security strategy that addresses both cyber and physical vulnerabilities.

7.1.3 Path Planning for UAVs Under GPS Permanent Faults

As demonstrated in this study, the cyber-physical integration of Unmanned Aerial Vehicles (UAVs) necessitates a broader approach to vulnerability analysis than traditionally applied. Beyond the computational risks inherent to components like GPS sensors and detectors, a significant yet often neglected set of vulnerabilities arises from the interplay between computational, electrical, and mechanical systems. In response to a catalog of UAV attacks, we have initiated investigations into several computational threats, devising strategies and policies for UAV path planning in scenarios of GPS malfunctions.

Our developed path planning process consists of three phases: initially, we employ a modified artificial potential field algorithm to navigate the UAV through complex environments filled with obstacles and Ground-Based Stations (GBSs). Next, we utilize the Received Signal Strength (RSS) trilateration technique to ascertain the UAV's location in the event of persistent GPS failures, providing location estimates at each stage. Subsequently, by integrating these methods, we implemented the Robust Control Algorithm-Artificial Potential Field (RCA-APF) algorithm tailored for a single UAV scenario.

Simulation and experimental results have affirmed the operational conditions under which the UAV successfully reaches its target. The effectiveness of our approach is further validated through a path-planning UAV simulator. Future research will explore more intricate scenarios, including multi-UAV path planning in diverse environments.

7.2 Future Research Directions

This section outlines the principal domains for future research, which aim to significantly enhance UAV cyber-resilience using the Advanced RCA-APF (Resilient Cyber-attack Artificial Potential Field) algorithm in complex environments:

- One future goal is to enhance UAV Cyber-Resilience with Advanced RCA-APF Algorithms in Complex Environments. Furthermore, we aim to deploy the Resilient Cyber-attack Artificial Potential Field (RCA-APF) algorithm in more intricate environments involving multiple UAVs. This will test the algorithm's efficacy in scenarios where several UAVs concurrently navigate from an initial location to a designated final destination. The primary challenge addressed will be the coordination and real-time path adjustment among UAVs to maintain optimal flight paths while responding dynamically to potential threats.
  - The initial step is to evaluate the RCA-APF algorithm's scalability by increasing the number of UAVs in simulation environments to mirror real-world operational

complexities.

  - Next step is to develop mechanisms for effective inter-UAV communication and coordination, ensuring that the fleet can respond as a unified entity to navigational adjustments or threats.

- Another future direction is to enhance attack detection and recovery mechanisms by significantly improving the process of detecting attacks. The main goal is to reduce the response time to nearly instantaneous recovery, targeting intervention speeds close to fractions of a second. This enhancement will be achieved by optimizing the existing RCA-APF algorithm parameters and integrating more responsive sensor data processing techniques.

  - Refine algorithmic efficiency to detect and initiate recovery processes quicker, minimizing the potential impact of attacks.

  - Utilize a broader array of sensor inputs to enhance detection capabilities, employing faster data processing frameworks to support rapid response functionalities.

  - New approaches depend on advanced technologies in wireless communication systems, such as 5G and beyond, utilizing more sophisticated signal processing methods and control systems.

- A promising future direction is to explore predictive analytics for preemptive attack mitigation. In this scenario, another branch of our research will concentrate on developing predictive capabilities within the RCA-APF framework, employing artificial intelligence (AI) and machine learning techniques. The goal is not only to react to attacks but also to anticipate them before they occur, thereby enhancing preemptive countermeasures. Implementation can involve the following:

  - Leverage machine learning models to analyze historical attack data and UAV behavior, developing predictive models that can accurately forecast potential cyber-

attacks.

  - Integrate these predictive models with the RCA-APF algorithm, allowing UAVs to adjust their flight paths in anticipation of potential threats, rather than merely reacting to them.

- Each of these areas can be pursued through a combination of theoretical development, simulation testing, and controlled field experiments. In particular, advanced simulation tools can be employed to model UAV fleet operations in high-risk environments, algorithms can be validated through extensive testing, and approaches can be refined based on feedback from these simulations.

- The proposed enhancements and expansions to the RCA-APF algorithm hold the promise of significantly advancing the state of UAV cybersecurity, making these systems more robust against increasingly sophisticated cyber-physical attacks.

- This research will not only improve the safety and reliability of UAV operations but also contribute to the broader field of autonomous vehicle security and wireless connectivity.

Bibliography

[1] K. P. Valavanis and G. J. Vachtsevanos, *Handbook of Unmanned Aerial Vehicles*. Springer Publishing Company, Incorporated, 2014.

[2] Q. Wu, Y. Zeng, and R. Zhang, "Joint trajectory and communication design for multi-UAV enabled wireless networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 2109–2121, mar 2018.

[3] I. Bekmezci, O. K. Sahingoz, and Temel, "Flying Ad-Hoc Networks (FANETs): A survey," pp. 1254–1270, may 2013.

[4] E. Yanmaz, R. Kuschnig, M. Quaritsch, C. Bettstetter, and B. Rinner, "On path planning strategies for networked unmanned aerial vehicles," *2011 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2011*, pp. 212–216, 2011.

[5] H. Wang, G. Ren, J. Chen, G. Ding, and Y. Yang, "Unmanned Aerial Vehicle-Aided Communications: Joint Transmit Power and Trajectory Optimization," *IEEE Wireless Communications Letters*, vol. 7, no. 4, pp. 522–525, 2018.

[6] H. Wang, J. Chen, G. Ding, and J. Sun, "Trajectory Planning in UAV Communication with Jamming," in *2018 10th International Conference on Wireless Communications and Signal Processing, WCSP 2018*. Institute of Electrical and Electronics Engineers Inc., nov 2018.

[7] J. Tisdale, Z. W. Kim, and J. K. Hedrick, "Autonomous UAV path planning and estimation: An online path planning framework for cooperative search and localization," *IEEE Robotics and Automation Magazine*, vol. 16, no. 2, pp. 35–42, 2009.

[8] M. Mozaffari, W. Saad, M. Bennis, Y. H. Nam, and M. Debbah, "A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2334–2360, 2019.

[9] S. H. Yeh, Y. S. Wang, T. D. Perera, Y. W. Peter Hong, and D. N. K. Jayakody, "UAV Trajectory optimization for Data-Gathering from Backscattering Sensor Networks," in *IEEE International Conference on Communications*, vol. 2020-June. Institute of Electrical and Electronics Engineers Inc., jun 2020.

[10] Y. Zeng and R. Zhang, "Energy-Efficient UAV Communication with Trajectory Optimization," *IEEE Transactions on Wireless Communications*, vol. 16, no. 6, pp. 3747–3760, jun 2017.

[11] S. R. Ganti and Y. Kim, "Design of Low-Cost On-board Auto-Tracking Antenna for Small UAS," in *Proceedings - 12th International Conference on Information Technology: New Generations, ITNG 2015*. Institute of Electrical and Electronics Engineers Inc., may 2015, pp. 273–279.

[12] N. M. Boev, "Design and implementation antenna for small UAV," *2011 International Siberian Conference on Control and Communications, SIBCON 2011 - Proceedings*, vol. 201, pp. 152–154, 2011.

[13] F. Paonessa, G. Virone, A. M. Lingua, M. Piras, I. Aicardi, P. Maschio, O. A. Peverini, G. Addamo, R. Orta, R. Tascone, and P. Bolli, "Effect of the uav orientation in antenna pattern measurements," in *2015 9th European Conference on Antennas and Propagation (EuCAP)*, 2015, pp. 1–2.

[14] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," *2012 IEEE International Conference on Technologies for Homeland Security, HST 2012*, pp. 585–590, 2012.

[15] G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, "Security Threats and Mitigation Techniques in UAV Communications: A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 112 858–112 897, 2022.

[16] C. G. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," *SSRR 2017 - 15th IEEE International Symposium on Safety, Security and Rescue Robotics, Conference*, pp. 194–199, oct 2017.

[17] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," https://cvxr.com/cvx, Mar. 2014.

[18] J. Holis and P. Pechac, "Elevation dependent shadowing model for mobile communications via high altitude platforms in built-up areas," *IEEE Transactions on Antennas and Propagation*, vol. 56, no. 4, pp. 1078–1084, 2008.

[19] S. J. Maeng, H. Kwon, O. Ozdemir, and Güvenç, "Impact of 3-d antenna radiation pattern in uav air-to-ground path loss modeling and rsrp-based localization in rural area," *IEEE Open Journal of Antennas and Propagation*, vol. 4, pp. 1029–1043, 2023.

[20] O. Khatib, "Real-time obstacle avoidance for manipulators and mobile robots," in *Proceedings - IEEE International Conference on Robotics and Automation*, 1985, pp. 500–505.

[21] M. H. Sulieman, M. C. Gursoy, and F. Kong, "Antenna pattern aware uav trajectory planning using artificial potential field," in *2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)*, 2021, pp. 1–7.

[22] G. Rong-xiao, T. Ji-wei, W. Bu-hong, and S. Fu-te, "Cyber-physical attack threats analysis for uavs from cps perspective," in *2020 International Conference on Computer Engineering and Application (ICCEA)*, 2020, pp. 259–263.

[23] M. H. Sulieman, M. Liu, M. C. Gursoy, and F. Kong, "Path planning for uavs under gps permanent faults," *ACM Trans. Cyber-Phys. Syst.*, mar 2024, just Accepted. [Online]. Available: https://doi.org/10.1145/3653074

[24] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 36–42, may 2016.

[25] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Efficient Deployment of Multiple Unmanned Aerial Vehicles for Optimal Wireless Coverage," *IEEE Communications Letters*, vol. 20, no. 8, pp. 1647–1650, Aug. 2016.

[26] D. Orfanus, E. P. De Freitas, and F. Eliassen, "Self-Organization as a Supporting Paradigm for Military UAV Relay Networks," *IEEE Communications Letters*, vol. 20, no. 4, pp. 804–807, apr 2016.

[27] J. Kosmerl and A. Vilhar, "Base stations placement optimization in wireless networks for emergency communications," in *2014 IEEE International Conference on Communications Workshops, ICC 2014*. IEEE Computer Society, 2014, pp. 200–205.

[28] Y. Zeng, R. Zhang, and T. J. Lim, "Throughput Maximization for UAV-Enabled Mobile Relaying Systems," *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 4983–4996, dec 2016.

[29] J. Lyu, Y. Zeng, and R. Zhang, "Cyclical Multiple Access in UAV-Aided Communications: A Throughput-Delay Tradeoff," *IEEE Wireless Communications Letters*, vol. 5, no. 6, pp. 600–603, dec 2016.

[30] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[31] Y. Zeng, R. Zhang, and T. J. Lim, "Throughput Maximization for UAV-Enabled Mobile Relaying Systems," *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 4983–4996, dec 2016.

[32] K. G. Nguyen, Q. D. Vu, M. Juntti, and L. N. Tran, "Distributed Solutions for Energy Efficiency Fairness in Multicell MISO Downlink," *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 6232–6247, sep 2017.

[33] S. Wang, F. Huang, and Z. H. Zhou, "Fast power allocation algorithm for cognitive radio networks," *IEEE Communications Letters*, vol. 15, no. 8, pp. 845–847, aug 2011.

[34] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control*, ser. Lecture Notes in Control and Information Sciences, V. Blondel, S. Boyd, and H. Kimura, Eds. Springer-Verlag Limited, 2008, pp. 95–110, http://stanford.edu/~boyd/graph_dcp.html.

[35] K. Namuduri, U. C. Fiebig, D. W. Matolak, I. Guvenc, K. V. Hari, and H. L. Maattanen, "Advanced Air Mobility: Research Directions for Communications, Navigation, and Surveillance," *IEEE Vehicular Technology Magazine*, vol. 17, no. 4, pp. 65–73, dec 2022.

[36] D. Erdos, A. Erdos, and S. E. Watkins, "An experimental uav system for search and rescue challenge," *IEEE Aerospace and Electronic Systems Magazine*, vol. 28, no. 5, pp. 32–37, 2013.

[37] Y. Zeng, J. Lyu, and R. Zhang, "Cellular-connected uav: Potential, challenges, and promising technologies," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 120–127, 2019.

[38] M. Atif, R. Ahmad, W. Ahmad, L. Zhao, and J. J. P. C. Rodrigues, "Uav-assisted wireless localization for search and rescue," *IEEE Systems Journal*, vol. 15, no. 3, pp. 3261–3272, 2021.

[39] D. W. Matolak and R. Sun, "Unmanned aircraft systems: Air-ground channel characterization for future applications," *IEEE Vehicular Technology Magazine*, vol. 10, no. 2, pp. 79–85, 2015.

[40] W. Khawaja, O. Ozdemir, F. Erden, I. Guvenc, and D. W. Matolak, "Ultra-wideband air-to-ground propagation channel characterization in an open area," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 6, pp. 4533–4555, 2020.

[41] A. Al-Hourani and K. Gomez, "Modeling cellular-to-uav path-loss for suburban environments," *IEEE Wireless Communications Letters*, vol. 7, no. 1, pp. 82–85, 2018.

[42] M. Badi, J. Wensowitch, D. Rajan, and J. Camp, "Experimentally analyzing diverse antenna placements and orientations for uav communications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14 989–15 004, 2020.

[43] P. Sinha and I. Guvenc, "Impact of antenna pattern on toa based 3d uav localization using a terrestrial sensor network," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 7, pp. 7703–7718, 2022.

[44] "Propagation data required for the design of earth-space land mobile telecommunication systems," International Telecommunication Union, Geneva, Switzerland, Tech. Rep. ITU-R P.681-6, 2003, recommendation.

[45] W. C. Jakes, *Microwave Mobile Communications*. Wiley-IEEE Press, 1994.

[46] C. A. Balanis, *Antenna Theory: Analysis and Design*. Wiley-IEEE Press, 2016.

[47] P. Chandhar, D. Danev, and E. G. Larsson, "Massive mimo as enabler for communications with drone swarms," in *2016 International Conference on Unmanned Aircraft Systems (ICUAS)*, 2016, pp. 347–354.

[48] S. J. Maeng, M. A. Deshmukh, Güvenç, A. Bhuyan, and H. Dai, "Interference analysis and mitigation for aerial iot considering 3d antenna patterns," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 490–503, 2021.

[49] E. Frachtenberg, "Practical Drone Delivery," *Computer*, vol. 52, no. 12, pp. 53–57, 2019.

[50] L. Zhang, H. Zhao, S. Hou, Z. Zhao, H. Xu, X. Wu, Q. Wu, and R. Zhang, "A Survey on 5G Millimeter Wave Communications for UAV-Assisted Wireless Networks," *IEEE Access*, vol. 7, pp. 117 460–117 504, Jul. 2019.

[51] I. Bucaille, S. Héthuin, A. Munari, R. Hermenier, T. Rasheed, and S. Allsopp, "Rapidly deployable network for tactical applications: Aerial base station with opportunistic links for unattended and temporary events ABSOLUTE example," in *Proceedings - IEEE Military Communications Conference MILCOM*, 2013, pp. 1116–1120.

[52] S. Rahman and Y. Z. Cho, "UAV positioning for throughput maximization," *Eurasip Journal on Wireless Communications and Networking*, vol. 2018, no. 1, pp. 1–15, Dec. 2018.

[53] M. Alzenad, A. El-Keyi, F. Lagum, and H. Yanikomeroglu, "3-D Placement of an Unmanned Aerial Vehicle Base Station (UAV-BS) for Energy-Efficient Maximal Coverage," *IEEE Wireless Communications Letters*, vol. 6, no. 4, pp. 434–437, Aug. 2017.

[54] S. Zhang, Y. Zeng, and R. Zhang, "Cellular-enabled UAV communication: A connectivity-constrained trajectory optimization perspective," in *IEEE Transactions on Communications*, vol. 67, no. 3, Mar. 2019, pp. 2580–2604.

[55] H. M. Jayaweera and S. Hanoun, "A dynamic artificial potential field (D-APF) UAV path planning technique for following ground moving targets," *IEEE Access*, vol. 8, pp. 192 760–192 776, 2020.

[56] J. Sun, J. Tang, and S. Lao, "Collision avoidance for cooperative uavs with optimized artificial potential field algorithm," *IEEE Access*, vol. 5, pp. 18 382–18 390, 2017.

[57] Q. Zhu, Y. Yan, and Z. Xing, "Robot path planning based on artificial potential field approach with simulated annealing," in *Proceedings - ISDA 2006: Sixth International Conference on Intelligent Systems Design and Applications*, vol. 2, 2006, pp. 622–627.

[58] J. Chen, D. Raye, W. Khawaja, P. Sinha, and I. Guvenc, "Impact of 3d uwb antenna radiation pattern on air-to-ground drone connectivity," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 2018, pp. 1–5.

[59] Q. Yao, Z. Zheng, L. Qi, H. Yuan, X. Guo, M. Zhao, Z. Liu, and T. Yang, "Path Planning Method With Improved Artificial Potential Field—A Reinforcement Learning Perspective," *IEEE Access*, vol. 8, pp. 135 513–135 523, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9146273/

[60] L. Dongcheng and D. Jiyang, "Research on Multi-UAV Path Planning and Obstacle Avoidance Based on Improved Artificial Potential Field Method," in *2020 3rd International Conference on Mechatronics, Robotics and Automation (ICMRA)*, Oct. 2020, pp. 84–88.

[61] G. Chmaj and H. Selvaraj, "Distributed processing applications for uav/drones: A survey," in *Progress in Systems Engineering*. Springer International Publishing, 2015, pp. 449–454.

[62] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei, "Survey on Unmanned Aerial Vehicle Networks: A Cyber Physical System Perspective," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 1027–1070, apr 2020.

[63] R. Dhakal and L. N. Kandel, "A Survey of Physical Layer-Aided UAV Security," in *Integrated Communications, Navigation and Surveillance Conference, ICNS*, vol. 2023-April. Institute of Electrical and Electronics Engineers Inc., 2023.

[64] Y. Peng, Y. Wang, C. Xiang, X. Liu, Z. Wen, D. Chen, and C. Zhang, "Cyber-physical attack-oriented industrial control systems (ics) modeling, analysis and experiment environment," in *2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, 2015, pp. 322–326.

[65] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: A new frontier," in *2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008)*, 2008, pp. 1–9.

[66] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei, "Survey on unmanned aerial vehicle networks: A cyber physical system perspective," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1027–1070, 2020.

[67] K.-D. Kim and P. R. Kumar, "Cyber–physical systems: A perspective at the centennial," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287–1308, 2012.

[68] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Trans. Cyber-Phys. Syst.*, vol. 1, no. 2, nov 2016. [Online]. Available: https://doi.org/10.1145/3001836

[69] V. Behzadan, "Cyber-physical attacks on uas networks- challenges and open research problems," 2017.

[70] L. Petnga and H. Xu, "Security of unmanned aerial vehicles: Dynamic state estimation under cyber-physical attacks," in *2016 International Conference on Unmanned Aircraft Systems (ICUAS)*, 2016, pp. 811–819.

[71] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[72] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in *2013 American Control Conference*, 2013, pp. 3344–3349.

[73] W. Chen, Y. Dong, and Z. Duan, "Attacking altitude estimation in drone navigation," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2018, pp. 888–893.

[74] A. Al-Hourani, S. Kandeepan, and A. Jamalipour, "Modeling air-to-ground path loss for low altitude platforms in urban environments," in *2014 IEEE Global Communications Conference, GLOBECOM 2014*. Institute of Electrical and Electronics Engineers Inc., feb 2014, pp. 2898–2904.

[75] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Unmanned Aerial Vehicle with Underlaid Device-to-Device Communications: Performance and Tradeoffs," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3949–3963, jun 2016.

[76] Q. Wu, Y. Zeng, and R. Zhang, "Joint trajectory and communication design for multi-UAV enabled wireless networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 2109–2121, mar 2018.

[77] X. Wang and M. C. Gursoy, "Resilient UAV Path Planning for Data Collection under Adversarial Attacks," in *IEEE International Conference on Communications*, vol. 2022-May. Institute of Electrical and Electronics Engineers Inc., 2022, pp. 625–630.

[78] B. Song, H. Chen, J. Suo, and W. Zhou, "Low-power Robustness Learning Framework for Adversarial Attack on Edges," *2022 18th International Conference on Mobility, Sensing and Networking (MSN)*, pp. 821–828, dec 2022. [Online]. Available: https://ieeexplore.ieee.org/document/10076784/

[79] H. Zhang and F. Luo, "An improved UAV path planning method based on APSOvnp-APF algorithm," in *Proceedings of the 34th Chinese Control and Decision Conference, CCDC 2022*. Institute of Electrical and Electronics Engineers Inc., 2022, pp. 5458–5463.

[80] C. Ma, J. Li, Y. Shang, S. Zhang, and Q. Yang, "A Dynamic Obstacle Avoidance Control Algorithm for Distributed Multi-UAV Formation System," in *2022 IEEE International Conference on Mechatronics and Automation, ICMA 2022*. Institute of Electrical and Electronics Engineers Inc., 2022, pp. 876–881.

[81] A. A. Cárdenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," *Proceedings - International Conference on Distributed Computing Systems*, pp. 495–500, 2008.

[82] N. Adam, "Workshop on future directions in cyber-physical systems security," *U.S. Department of Homeland Security*, no. October 2014, pp. 1–61, 2010. [Online]. Available: https://feihu.eng.ua.edu/NSF_CPS/year1/w2_read.pdf

[83] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, "Robustness of attack-resilient state estimators," *2014 ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS 2014*, pp. 163–174, 2014.

[84] D. Mendes, N. Ivaki, and H. Madeira, "Effects of GPS spoofing on unmanned aerial vehicles," in *Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC*, vol. 2018-Decem. IEEE Computer Society, feb 2019, pp. 155–160.

[85] C. Titouna and F. Naït-Abdesselam, "A Lightweight Security Technique For Unmanned Aerial Vehicles Against GPS Spoofing Attack," in *2021 International Wireless Communications and Mobile Computing, IWCMC 2021*. Institute of Electrical and Electronics Engineers Inc., 2021, pp. 819–824.

[86] I. G. Ferrao, S. A. Da Silva, D. F. Pigatto, and K. R. Branco, "GPS Spoofing: Detecting GPS Fraud in Unmanned Aerial Vehicles," *2020 Latin American Robotics Symposium, 2020 Brazilian Symposium on Robotics and 2020 Workshop on Robotics in Education, LARS-SBR-WRE 2020*, nov 2020.

[87] J. Xiao and M. Feroskhan, "Cyber Attack Detection and Isolation for a Quadrotor UAV With Modified Sliding Innovation Sequences," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 7, pp. 7202–7214, jul 2022.

[88] E. Yel and N. Bezzo, "GP-based Runtime Planning, Learning, and Recovery for Safe UAV Operations under Unforeseen Disturbances," in *IEEE International Conference on Intelligent Robots and Systems*. Institute of Electrical and Electronics Engineers Inc., oct 2020, pp. 2173–2180.

[89] J. Tian, B. Wang, R. Guo, Z. Wang, K. Cao, and X. Wang, "Adversarial Attacks and Defenses for Deep Learning-based Unmanned Aerial Vehicles," *IEEE Internet of Things Journal*, 2021.

[90] ——, "Adversarial Attacks and Defenses for Deep-Learning-Based Unmanned Aerial Vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22 399–22 409, nov 2022.

[91] M. Haider, I. Ahmed, and D. B. Rawat, "Cyber Threats and Cybersecurity Reassessed in UAV-assisted Cyber Physical Systems," in *International Conference on Ubiquitous and Future Networks, ICUFN*, vol. 2022-July. IEEE Computer Society, 2022, pp. 222–227.

[92] L. Zhang, Z. Wang, M. Liu, and F. Kong, "Adaptive window-based sensor attack detection for cyber-physical systems," in *59th ACM/IEEE Design Automation Conference, DAC 2022*. Institute of Electrical and Electronics Engineers Inc., 2022, pp. 919–924.

[93] Y. Harada, Y. Yamagata, O. Mizuno, and E.-H. Choi, "Log-based anomaly detection of cps using a statistical method," in *2017 8th International Workshop on Empirical Software Engineering in Practice (IWESEP)*. IEEE, 2017, pp. 1–6.

[94] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," *ACM Computing Surveys (CSUR)*, vol. 54, no. 5, pp. 1–36, 2021.

[95] M. Liu, L. Zhang, P. Lu, K. Sridhar, F. Kong, O. Sokolsky, and I. Lee, "Fail-safe: Securing cyber-physical systems against hidden sensor attacks," in *2022 IEEE Real-Time Systems Symposium (RTSS)*. IEEE, 2022, pp. 240–252.

[96] R. X. Guo, J. W. Tian, B. H. Wang, and F. T. Shang, "Cyber-Physical Attack Threats Analysis for UAVs from CPS Perspective," in *Proceedings - 2020 International Conference on Computer Engineering and Application, ICCEA 2020*. Institute of Electrical and Electronics Engineers Inc., mar 2020, pp. 259–263.

[97] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks," in *Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017*. Institute of Electrical and Electronics Engineers Inc., jun 2017, pp. 3–18.

[98] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[99] C. Kwon, W. Liu, and I. Hwang, "Security analysis for Cyber-Physical Systems against stealthy deception attacks," in *Proceedings of the American Control Conference*, 2013, pp. 3344–3349.

[100] J. Park, R. Ivanov, J. Weimer, M. Pajic, S. H. Son, and I. Lee, "Security of cyber-physical systems in the presence of transient sensor faults," *ACM Trans. Cyber-Phys. Syst.*, vol. 1, no. 3, may 2017. [Online]. Available: https://doi.org/10.1145/3064809

[101] O. Ceviz, P. Sadioglu, and S. Sen, "A Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions," jun 2023. [Online]. Available: https://arxiv.org/abs/2306.14281v3

[102] C. Pu and Y. Li, "Lightweight Authentication Protocol for Unmanned Aerial Vehicles Using Physical Unclonable Function and Chaotic System," *IEEE Workshop on Local and Metropolitan Area Networks*, vol. 2020-July, jul 2020.

[103] A. K. Das, B. Bera, M. Wazid, S. S. Jamal, and Y. Park, "IGCACS-IoD: An Improved Certificate-Enabled Generic Access Control Scheme for Internet of Drones Deployment," *IEEE Access*, vol. 9, pp. 87 024–87 048, 2021.

[104] A. J. Weiss, "On the Accuracy of a Cellular Location System Based on RSS Measurements," *IEEE Transactions on Vehicular Technology*, vol. 52, no. 6, pp. 1508–1518, nov 2003.

[105] R. K. Martin, A. S. King, J. R. Pennington, R. W. Thomas, R. Lenahan, and C. Lawyer, "Modeling and mitigating noise and nuisance parameters in received signal strength positioning," *IEEE Transactions on Signal Processing*, vol. 60, no. 10, pp. 5451–5463, 2012.

[106] D. Jin, F. Yin, C. Fritsche, F. Gustafsson, and A. M. Zoubir, "Bayesian cooperative localization using received signal strength with unknown path loss exponent: Message passing approaches," *IEEE Transactions on Signal Processing*, vol. 68, pp. 1120–1135, 2020.

[107] S. A. Zekavat and M. Buehrer, *Handbook of Position Location: Theory, Practice, and Advances*, 2011. [Online]. Available: https://ieeexplore.ieee.org/book/8633728

[108] I. Güvenç and C. C. Chong, "A survey on TOA based wireless localization and NLOS mitigation techniques," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 3, pp. 107–124, 2009.

[109] F. Seco, A. R. Jiménez, C. Prieto, J. Roa, and K. Koutsou, "A survey of mathematical methods for indoor localization," in *WISP 2009 - 6th IEEE International Symposium on Intelligent Signal Processing - Proceedings*, 2009, pp. 9–14.

[110] Y. T. Chan, H. Y. C. Hang, and P. C. Ching, "Exact and approximate maximum likelihood localization algorithms," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 1, pp. 10–16, jan 2006.

[111] C. Chang and A. Sahai, "Estimation bounds for localization," in *2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, IEEE SECON 2004*, 2004, pp. 415–424.

[112] Z. Xiao and Y. Zeng, "An overview on integrated localization and communication towards 6G," jun 2022. [Online]. Available: https://arxiv.org/abs/2006.01535v1

[113] A. Ledergerber, M. Hamer, and R. D'Andrea, "A robot self-localization system using one-way ultra-wideband communication," *IEEE International Conference on Intelligent Robots and Systems*, vol. 2015-December, pp. 3131–3137, dec 2015.

[114] A. A. Wahab, A. Khattab, and Y. A. Fahmy, "Two-way TOA with limited dead reckoning for GPS-free vehicle localization using single RSU," *2013 13th International Conference on ITS Telecommunications, ITST 2013*, pp. 244–249, 2013.

[115] Y. T. Chan, W. Y. Tsui, H. C. So, and P. C. Ching, "Time-of-arrival based localization under NLOS conditions," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 1, pp. 17–24, jan 2006.

[116] 3GPP TR 36.777, "Enhanced LTE support for aerial vehicles," Online, 2019, accessed on May 17, 2019. [Online]. Available: https://www.3gpp.org/specs/archive/36_series/36.777

[117] Z. Yang, Z. Zhou, and Y. Liu, "From RSSI to CSI: Indoor localization via channel response," *ACM Computing Surveys*, vol. 46, no. 2, dec 2013. [Online]. Available: https://dl.acm.org/doi/10.1145/2543581.2543592

[118] P. Kumar, L. Reddy, and S. Varma, "Distance measurement and error estimation scheme for RSSI based localization in wireless sensor networks," in *5th International Conference on Wireless Communication and Sensor Networks, WCSN-2009*, 2009, pp. 80–83.

[119] J. Yang and Y. Chen, "Indoor localization using improved rss-based lateration methods," in *GLOBECOM - IEEE Global Telecommunications Conference*, 2009.

[120] M. E. Rusli, M. Ali, N. Jamil, and M. M. Din, "An Improved Indoor Positioning Algorithm Based on RSSI-Trilateration Technique for Internet of Things (IOT)," in *Proceedings - 6th International Conference on Computer and Communication Engineering: Innovative Technologies to Serve Humanity, ICCCE 2016*. Institute of Electrical and Electronics Engineers Inc., dec 2016, pp. 12–77.

[121] A. Norrdine, "An algebraic solution to the multilateration problem," in *Proceedings of the 15th international conference on indoor positioning and indoor navigation, Sydney, Australia*, vol. 1315, 2012.

[122] M. H. Sulieman, M. C. Gursoy, and F. Kong, "Antenna Pattern Aware UAV Trajectory Planning Using Artificial Potential Field," in *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, vol. 2021-Octob. Institute of Electrical and Electronics Engineers Inc., 2021.

Vita

Name: *Mohamad Hani Sulieman*

Education:

- B.S., Electrical Engineering, Syracuse University, 2016
- M.S., Electrical Engineering, Syracuse University, 2022
- Ph.D., Electrical & Computer Engineering, Syracuse University, 2024

Professional Experience:

- Senrio Electrical Engineer, INFICON, USA, 2023
- Lead Engineer, Baker Hughes, USA, 2021
- Research and Development Engineer, ICM Controls Inc., USA, 2021
- Part-time Teaching Professor, John Carroll University, USA, 2023

Recent Publications:

1. Path Planning for UAVs under GPS Permanent Faults, ACM Transactions on Cyber-Physical Systems (TCPS), 2024
2. Antenna Pattern Aware UAV Trajectory Planning Using Artificial Potential Field, 2021 IEEE/AIAA 40th Digital Avionics Systems Conference, 2021

Awards and Honors:

- La Page Fellowship Award Fall 2020- Spring 2021