ROBUST RESOURCE ALLOCATION TO SECURE PHYSICAL LAYER USING UAV-ASSISTED MOBILE RELAY COMMUNICATIONS IN 5G TECHNOLOGY

by

Shakil Ahmed

A thesis submitted in partial fulfillment
of the requirements for the degree

of

MASTER OF SCIENCE

in

Electrical Engineering

Approved:

Rose Qingyang Hu, Ph.D. Major Professor	Bedri Cetiner, Ph.D. Committee Member
Ziqi Song, Ph.D. Committee Member	Richard S. Inouye, Ph.D. Vice Provost for Graduate Studies

UTAH STATE UNIVERSITY
Logan, Utah

2019

ABSTRACT

Robust Resource Allocation to Secure Physical Layer using UAV-assisted Mobile Relay Communications in 5G Technology

by

Shakil Ahmed, Master of Science

Utah State University, 2019

Major Professor: Rose Qingyang Hu, Ph.D.
Department: Electrical and Computer Engineering

Due to the diverse applications of the internet of things (IoT), the unmanned aerial vehicles (UAVs) can be a viable solution to provide reliable connectivity for the next generation wireless networks. The UAVs have numerous advantages to serve next generation users, such as higher mobility, adaptive flight altitude, quick, easy, and cost-effective deployment, etc. Moreover, the UAVs have the line of sight (LOS) communication link, which improves the quality of service (QoS) of the 5G cellular users. Thus, the UAVs can be a good standing to support different potential applications, such as emergency smart health users, continuous border patrol, the social unrest monitoring, and military surveillance, etc. On the other hand, the UAVs have the security risk due to its air to ground broadcast nature. Although the UAVs have these salient features, insignificant research on the UAV physical layer security analysis has been conducted. This thesis investigates the UAV performance for the next generation of wireless networks while improving the physical layer security. The proposed model considers the UAV-assisted mobile relay (UAV-MR), which serves as a mobile relay. The model also considers the base station (BS), which serves as the source. Moreover, the active presence of multiple eavesdroppers and one ground user are also considered in the proposed system. However, the actual locations of the eavesdroppers are unknown to the UAV-MR while the UAV-MR knows the exact locations of the ground user and the BS. Moreover, the three-dimensional flying direction of the UAV-MR is also analyzed in the thesis, which becomes an essential parameter to design the UAV-MR trajectory. Thus, the UAV-MR performance analysis, the physical layer security, and the UAV-MR robust resource allocation, etc., are investigated. The improved performance is achieved by developing the framework for maximizing the achievable secrecy rate under the UAV-MR flight time constraint while the multiple eavesdroppers are present in the network. A mathematical structure, which solves the maximization problem sub-optimally, is also formulated to support the proposed efficient algorithm. Significantly improved performance of the proposed algorithm is illustrated via the simulation results, where the results are compared with the backbench method.

(75 pages)

PUBLIC ABSTRACT

Robust Resource Allocation to Secure Physical Layer using UAV-assisted Mobile Relay Communications in 5G Technology

Shakil Ahmed

The unmanned aerial vehicles (UAVs) are also known as drones. Recently, UAVs have attracted the next generation researchers due to their flexible, dynamic, and cost-effective deployment, etc. Moreover, the UAVs have a wide range of application domains, such as rescue operation in the remote area, military surveillance, emergency application, etc. Given the UAVs are appropriately deployed, the UAVs provide continuous and reliable connectivity, on-demand, and cost-effective features to the desired destination in the wireless communication system. Thus, the UAVs can be a great choice to deploy as a mobile relay in co-existence with the base stations (BSs) on the ground to serve the 5G wireless users. In this thesis, the UAV-assisted mobile relay (UAV-MR) in the next generation wireless networks has been studied, which also considers the UAV-MR physical layer security. The proposed system also considers one ground user, one BS on the ground, and active presence of multiple eavesdroppers, situated nearby the ground user. The locations of these nodes (i.e., the ground user, the BS, and the evesdroppers) are considered fixed on the ground. Moreover, the locations of the eavesdroppers are not precisely known to the UAV-MR. Thus, this thesis aims to maximize the achievable secrecy rate, while the BS sends the secure information to the ground user via the UAV-MR. However, the UAV-MR has some challenges to deploy in wireless networks, such as 3D deployment, robust resource allocation, secure UAV-MR to ground communication, the channel modeling, the UAV-MR flight duration, and the UAV-MR robust trajectory design, etc. Thus, this project investigates the UAV-MR assisted wireless networks, which addresses those technical challenges to guarantee efficient UAV-MR communication. Moreover, the mathematical frameworks are formulated to support the proposed model. An efficient algorithm is proposed to maximize the UAV-MR achievable secrecy rate. Finally, the simulation results show the improved performance for the UAV-MR assisted next-generation networks.

To all the good people.

ACKNOWLEDGMENTS

I owe my sincere gratitude to my major professor, Dr. Rose Qingyang Hu, who not only continuously supports me to gain the required research-related knowledge but also motivates me to be steadfast in achieving the goal. Thus, the continuous support from my major professor never makes me feel lonely or depressed. Eventually, her support makes me motivated during the stressful time of graduate studies. Moreover, I would also like to express my sincere gratitude to my committee members Dr. Bedri Cetiner, and Dr. Ziqi Song, who have extended their support while pursuing the MS degree. I would also like to thank Dr. Fuhui Zhou, the School of Information Engineering, Nanchang University, China, who helped me with the problem formulation of the project.

I also thank my parents, wife, brother, sisters, and all my friends for having taken care of me during my graduate studies. Without their mental support and inspiration, it would be impossible for me to fulfill my dream.

I would also like to thank Dr. Reyhan Baktur, Dr. Koushik Chakraborty, Dr. Jacob Gunther, Dr. Todd Moon, and Dr. Zhen Zhang, who guided me in various course works. I want to acknowledge help from my colleagues at the Communications Network Innovation Lab. Especially, Haijian Sun and Qun Wang helped a lot, which makes me successful in accomplishing the project. Finally, my sincere gratitude is towards the school of Research and Graduate Studies, Utah State University, for awarding me Presidential Doctoral Research Fellowship (PDRF). I also thank the National Science Foundation (NSF grant no. ECCS-1308006, NeTS- 1423348, and EARS- 1547312) for providing me the necessary funding support.

Shakil Ahmed

CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure Page

ACRONYMS

AWGN	additive white Gaussian noise
BS	base station
DC	difference of concave
HAP	high altitude platform
IoT	internet of things
IPM	interior point method
LAP	low altitude platform
LOS	line of sight
MIMO	multiple input multiple output
OFDMA	orthogonal frequency-division multiple access
QoS	quality of service
SINR	signal to interference plus noise ratio
SWIPT	simultaneous wireless information and power transfer
UAV	unmanned aerial vehicle
UAV-MR	UAV-assisted mobile relay
UAV-SR	UAV-assisted static relay

CHAPTER 1
INTRODUCTION

1.1 Motivation

As billions of wireless devices are being connected each year in 5G wireless networks, the massive number of users require reliable connectivity and low latency. Fortunately, the unmanned aerial vehicles (UAVs) can meet those demands with a low cost and flexibility. As the ground base stations (BS) cannot always guarantee the quality of service (QoS) in various geographical regions, for example, mountain areas, impoverished wireless coverage region, etc., UAVs can reach those areas to provide reliable connectivity with better QoS and flexibility. However, UAVs have considerable physical layer security concerns due to the air to ground wireless broadcast nature but still lack significant research efforts in this area. Improving the UAV-MR physical layer security might be a research hotspot so that the UAV relay can fly in the sky without the physical layer security concern. Moreover, the UAV can serve next-generation cellular users without the legitimate information being intercepted by the unknown eavesdroppers. In the next several sections, different types of UAVs and related literature are studied to address the limitations and research scope of the UAV physical layer security.

1.2 UAV Classification

Fig. 1.1 describes the UAV classification based size, wing, and altitude.

UAV size and altitude: Different sizes of the UAV [1] are described as follows: The maximum weight of a small size UAV is $0 - 20$ lbs, which can normally fly less than 12000 ft above the ground level. Its size can vary from a giant insect to 50 cm long. It can be used for spying or military surveillance due to its lightweight.

A medium size UAV has a weight $21 - 55$ lbs, which can fly more than 3500 ft above

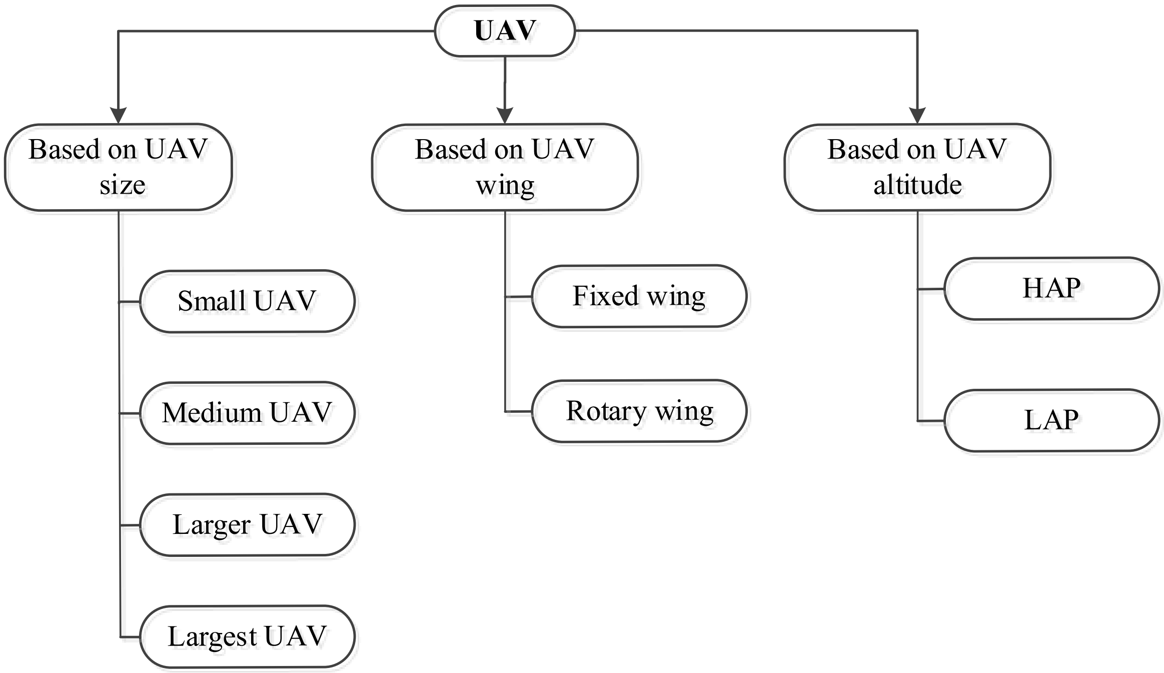

Fig. 1.1: The UAV classification.

the sea level. A large size UAV can fly up to 18000 ft mean sea level with a weight less than 1320 lbs. A giant UAV can fly more than 18000 ft mean sea level with weight more than 1320 lbs. Ultimately a high altitude platform (HAP) UAV maintains a $65000-164000$ ft altitude from the earth In recent days, HAP UAVs are commonly used in the wireless communication servers [3]. On the other hand, the LAP UAV can be used near the ground, for example, border surveillance, and social unrest monitoring, etc.

UAV wing: There are two types of UAVs based on the wing, namely the fixed wing and the rotary wing [2]. As the name implies, the fixed-wing UAV has a stationary wing, which uses UAV's forward speed to keep it aloft during the flight time. On the other hand, the rotary UAV has multiple rotating blades, which help the UAV to be aloft on the sky. However, the operation principle of both the fixed and the rotary wings are pretty much the same. The only difference is that the rotary wing UAV does not require the forward movement to keep the UAV aloft. Instead, the rotary blade makes the forward movement, which keeps the UAV aloft during the flight time.

1.3 Literature Review

UAVs have a bunch of salient features, which are essential towards the successful future wireless communication system, for example, unmanned and remote operation, cost-effectiveness, flexible deployment, high mobility, and reliable connectivity, etc. UAVs can make a significant contribution to the various applications of wireless communication domain [4,5], such as social unrest surveillance, rescuing operation to unreachable and remote areas, military and border transportation, and search operation, etc. Moreover, UAVs can also be a good fit to support the next generation wireless networks, such as sending the smart health-related real-time information to the destination/users, especially where it is difficult to reach in a short time in the event of the emergency scenario. Thus, UAV applications in the future wireless communication can meet the excessive demand of different types of users.

Due to various potential opportunities of UAVs, many telecommunications companies, such as Qualcomm, Ericsson, Verizon, AT&T, and China Mobile, have started the UAV related research projects for the next generation wireless communications [6,7]. In practice, UAVs can be applied in two paradigms, namely

1. Using UAV as an aerial base station: The UAV works as a mobile base station in the air, which can be flexibly deployed. It is also dynamic and can serve an on-demand basis to the ground users. Moreover, UAV can be used as the aerial base station to support the emergency wireless communication service if there is terrestrial BS hardware malfunction, provides offloading in a highly crowded environment, or unreachable and unprivileged areas, where the ground wireless network is not supported [8] - [12].

2. Using UAV as a relay: The UAV can also be used as a relay in the air. If users are far away from the BS on the ground, the BS serves the remote users via using the UAV relay.

UAV has better line of sight (LOS) communication links, which can better provide reliable air to the ground communications and also ensure the legitimate communication link over a long distance, especially in the outdoor environment. Moreover, the UAV enabled applications can gather the required information/data in real time and send to the ground user.

However, UAVs can be quite vulnerable to the communication link interception due to the openness of the transmission medium and broadcast nature of the communication links [13]. Though the UAV-assisted mobile relay (UAV-MR) has the LOS air to ground communication nature, the LOS type communication between air to the ground can be considered as prone to the eavesdroppers, which leads to the physical layer security challenge for UAV-MR communication. The security research has been focused mainly in the upper layer protocol stack design using the cartographic methods. The UAV-MR physical layer security has become an emerging research hotspot nowadays.

Very insignificant amount of research has been performed on the UAV-MR robust resource allocation to secure the physical layer. To secure the physical layer, the UAV-MR trajectory optimization is critical due to the active presence of multiple eavesdroppers in the geographical environment. Moreover, such as the UAV-MR flight duration, location of the ground user, locations of eavesdroppers, and energy consumed by the UAV-MR, etc., during the UAV-MR flight play a significant role to design the UAV-MR trajectory [14] - [17]. The authors in [17] studied the UAV trajectory optimization to maximize the sum-rate uplink communication. The UAVs are equipped with multiple antennas. However, the presence of eavesdroppers is not considered in their proposed system. Authors in [18] considered a photo sensing method to optimize the UAV trajectory. They proposed an algorithm to optimize the UAV energy consumption while the UAV is flying over the area of interest. In the end, the authors investigated an optimal waypoint and an optimal UAV velocity while the UAV is flying over the waypoints. In [19], a swarm of UAVs is considered to optimize the trajectory, the UAVs energy consumption, given that the proposed system is free from the UAV-UAV collisions. In [20], a joint UAV-users scheduling and UAV trajectory is optimized, which aims to optimize the average rate.

Another widely accepted UAV physical layer security design parameter is the achievable secrecy rate [21] - [35]. The UAV sends secure information to the destination reliably while the eavesdroppers are unable to intercept the secure information. Comparing the UAV-to-user and the UAV-to-eavesdropper communication links, if the communication links of the UAV-MR to the eavesdroppers are weaker than the legitimate air to the ground communication link, the achieved secrecy rate is non-zero secrecy rate. On the other hand, if the legitimate air to the ground communication link is stronger than the communication link of the eavesdroppers, the achieved secrecy rate is not non-zero secrecy rate.

In the UAV physical layer security research, each of the active communication nodes is considered as static on their locations in the recent research. Due to this assumption, both the average channel gain of the legitimate UAV to the user communication link and the UAV to the eavesdropper communication link mostly depend on the LOS communication link based path loss and source or ground shadowing. In this scenario, the channel gain can be achieved if the locations of the source, destination, and eavesdropper are known to the UAV. If the channel gain of the eavesdropper is more significant than channel gain of the legitimate source, various techniques can be investigated so that the positive achievable secrecy rate can be achieved. The example of those techniques can be fading, resource allocation, and power control, etc. However, if there is long enough distance between the source and the legitimate destination, possibly the channel gain of the legitimate link is smaller compared to the channel gain of the UAV to the eavesdroppers.

The authors in [24] considered the fading channel while their proposed system model aims to maximize the achievable secrecy rate. They also considered the power control for maximizing the secrecy rate. In [25], the authors proposed the power control over the frequency sub-carriers to maximize the achievable the secrecy rate. They considered the orthogonal frequency-division multiple access (OFDMA). The authors in [26] investigated the physical layer security via designing the beamforming with channel coding. Their investigation is based on multiple input multiple output (MIMO) communication system.

Moreover, the artificial noise is produced to deceive the eavesdroppers on the ground with the help of multiple UAV relays. Thus, their proposed system model improves the overall achievable secrecy rate performance.

The authors in [27] compared the performance of the static and mobile destination. It is proved that the mobile destination has better performance based on the point-point system. In [28, 29], the authors considered the joint power control on the legitimate source-destination and the artificial noise based on simultaneous wireless information and power transfer (SWIPT) system. They maximized the secrecy rate based on joint power control and SWIPT technique. The source sends the artificial noise and uses the beamforming technique to the locations of the eavesdroppers. These procedures are done via jointly the beamforming technique and the artificial noise employment in the MIMO system. Thus, the legitimate link between the source and the destination is enhanced while the communication link of the UAV to the eavesdroppers degraded. Eventually, the secrecy rate performance is enhanced.

The authors in [30] proposed an efficient approach to maximize the achievable secrecy rate via a transmission scheduling in a multiuser cognitive radio system network. The authors investigated the point to point and source to the legitimate destination link to maximize the achievable secrecy rate in [31]. Moreover, the co-operative jamming using the relay for single antenna node is considered to maximize the secrecy rate.

Very initial theoretical research about the UAV physical layer security while maximizing the achievable secrecy rate is studied in [32]. M. Cui *et. al.* investigated the joint optimization of the UAV trajectory; the UAV transmit power to optimize the achievable secrecy rate [33]. The system considers the active presence of the eavesdroppers. In their investigation, the UAV is considered as the mobile relay, and BS is regarded as the source. On the contrary, Q. Wang *et. al.* also analyzed the secure physical layer communication considering four nodes such as the UAV relay, the BS, the ground user, and the eavesdropper [34]. In their proposed system, the location of the eavesdropper is perfectly known to the UAV, which is unrealistic in the real implementation. Moreover, the authors did not consider robust USV resource allocation.

None of the above literature addressed the physical layer security issue. This thesis addresses those unresolved issues, which are not reflected in the above literature.

1.4 Summary the Chapter

This chapter discusses the prospect and challenges of UAV in next-generation wireless networks. The classification of the UAVs is described. The motivation of the proposed system model in the project is elaborated. The chapter further presents recent research in the area of the UAV physical layer security. In the end, several limitations on the UAV physical layer security are pointed, which are addressed in the later chapters of the thesis.

CHAPTER 2
UAV-MR PHYSICAL LAYER SECURITY

In this chapter, the proposed physical layer security for UAV-MR communication is presented in details. Moreover, the chapter provides the proposed system model overview, for example, the explanation of different parameters and assumptions, etc. The UAV-assisted mobile relay (UAV-MR) has a big challenge of transmitting secure information to the ground user due to the broadcast nature of the air-to-ground line of sight (LOS) channels. This challenge is tackled via jointly designing robust UAV-MR trajectory, and transmit power of the UAV-MR and the BS optimization in next-generation wireless networks. The thesis aims to maximize the achievable secrecy rate considering the presence of one base station (BS), one UAV-MR, one user on the ground, and multiple eavesdroppers on the ground. The locations of the eavesdroppers are unknown to the UAV-MR when it transmits secure information to the ground user. Moreover, the proposed model also considers the information casualty constraint, which guarantees the UAV-MR forwards the decoded secure information from the BS to the ground user.

2.1 Background and Contributions

Recently, UAV is a new communication entity that has attracted considerable interest to the 5G researchers [36] - [42] due to the enormous potential applications. Moreover, UAVs have salient features, such as higher connectivity, LOS channel advantage, a better quality of service (QoS), and spectral efficiency, etc., which make UAVs a desirable choice to support the next generation wireless networks in various situations. While UAV can be used a relay, there area two possible scenarios.

1. UAV-assisted mobile relay (UAV-MR)

2. UAV-assisted static relay (UAV-SR)

In general the UAV-MR has more advantages over the UAV-SR [43, 44] in terms of cost-effectiveness, fast deployment, and coverage, etc. The UAV-MR is moving all the time while the UAV-SR has a fixed location [45]. UAV-MR can be deployed in various environments, for example, a remote area or areas with nature disasters. UAV-MR communication has the physical layer security concern due to its air to ground broadcast nature. In this investigation, the legitimate and secure UAV-MR communications in the presence of multiple eavesdroppers on the ground are studied. We make a realistic assumption that the locations of the eavesdroppers are considered unknown to the UAV-MR. The goal of the thesis is to maximize the achievable secrecy rate, subject to the robust resource allocation, the mobility constraint, and the information-causality constraints, etc., under given UAV-MR flight time. The formulated achievable secrecy rate maximization problem is not a convex problem and difficult to solve. As such the key contributions of this investigation are summarized as follows:

- Securing the physical layer based on joint optimization of the robust UAV-MR trajectory, and transmit power of the UAV-MR and the BS is studied for the next generation wireless networks. The locations of the BS and the ground user are known to the UAV-MR in advance. However, the actual locations of the eavesdroppers are unknown to the UAV-MR. The UAV-MR knows the approximate locations of the eavesdroppers by combining the information of the known regions of the locations of the eavesdroppers and possible errors of the eavesdroppers for their actual positions.

- There are no direct communication links between the BS and the ground user, between the BS and the eavesdroppers, and between the ground user and the eavesdroppers in the proposed system model to blockages and shadowing. Moreover, the proposed model optimizes jointly the robust UAV-MR trajectory (in x and y direction) and the transmit powers of the UAV-MR and the BS. The study considers the average and the peak transmit power of the UAV-MR and the BS to optimize the achievable secrecy rate. The proposed model is more realistic by assuming the unknown presence of the eavesdroppers.

- The information-causality constraint is considered in the system, which allows the UAV-MR to send only the decoded information from the BS to the ground user [46].

- Jointly designing robust UAV-MR trajectory, and transmit power of the UAV-MR, and the BS can tackle the unknown locations of the eavesdroppers effectively.

- The formulated secrecy rate maximization problem is a non-convex problem. The achievable secrecy rate non-convex optimization problem is solved sub-optimally in the proposed system. The UAV-MR and the BS transmit power is optimized for the given UAV-MR trajectory location. On the other hand, the UAV-MR trajectory location is optimized for the optimal UAV-MR, and the BS transmit power. For the UAV-MR trajectory optimization, $\mathcal{S}$-*Procedure*, the difference of concave (DC), successive convex approximation (SCA), and interior point method (IPM) are applied altogether to deal with the non-convexity of the UAV-MR trajectory optimization. Based on the $\mathcal{S}$-*Procedure*, IPM, SCA, and DC, an efficient overall algorithm is proposed to maximize the achievable secrecy rate, which solves the optimization iteratively and alternatively.

- Finally, the simulation is performed, which shows the improved achievable secrecy rate performance and the efficient UAV-MR trajectory.

The rest of the thesis studies the proposed system model and the problem formulation, the sub-optimal solution, and the proposed algorithm.

2.2 Proposed System Model Overview

As shown in Fig. 2.1, a UAV based communications system covering geographical area is considered. The environment consists of a UAV-MR, a BS on the ground, one user on the ground, and multiple eavesdroppers on the ground while this investigation aims to maximize the UAV-MR achievable secrecy rate. In the proposed system, the UAV-MR can move horizontally and dynamically during UAV-MR flight time. Unlike the UAV-SR with fixed relay location, it is considered the UAV-MR has sufficiently higher mobility. Moreover, the

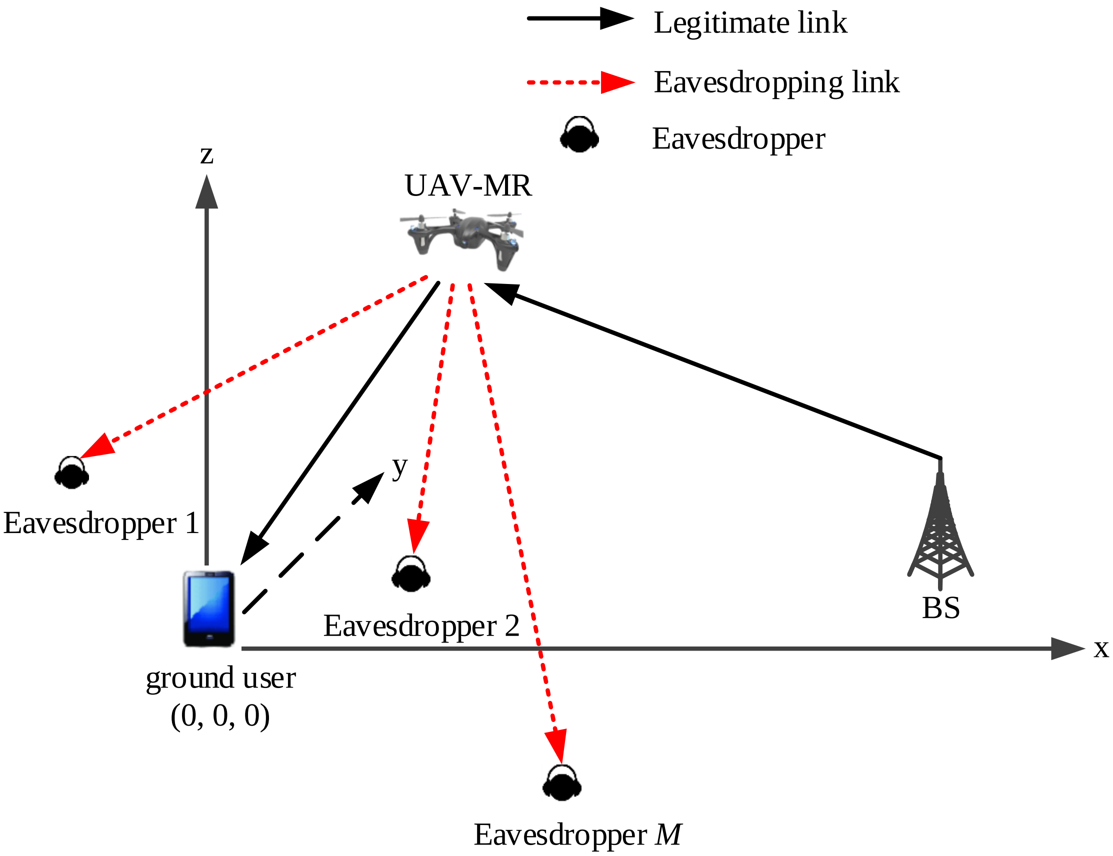

Fig. 2.1: Communications from the BS to the UAV-MR and from the UAV-MR to the ground user while M potential eavesdroppers intercept on the ground.

ground user has a fixed location. The ground user locates far from the BS, making the BS not able to reach the ground user directly. Thus, the proposed system considers that the BS serves the ground user using the UAV-MR in order to attain the required QoS. The active presence of multiple eavesdroppers is also considered in the proposed UAV-MR to ground user communication system. The UAV-MR does not know the exact locations of the eavesdroppers while approximated regions of the locations of the eavesdroppers can be estimated by the UAV-MR. These eavesdroppers try to intercept the legitimate communication links between the UAV-MR and the ground user. The locations of the eavesdroppers are considered far from the BS and near to the ground user, as shown in Fig. 2.1.

Each of the nodes, i.e., the UAV-MR, the BS, the ground user, and the eavesdroppers, is equipped with a single antenna. The proposed system does not consider any direct link between the BS to the ground user, between the ground user to the eavesdroppers, and between the BS to the eavesdroppers due to long distance, or severe blockage and shadowing, which may happen in the mega-cities due to the tall buildings and other obstacles or remote areas, for example, the high mountains. The BS and the UAV-MR establish the legitimate communication link to the UAV-MR and the ground user during the UAV-MR flight time. During the UAV-MR flight time, the UAV-MR flies over the ground user at a fixed altitude. Moreover, the proposed wireless system is developed in three-dimensional coordinate systems.

The UAV-MR flies at a finite time horizon $0 \leq t \leq T$, where T is in second, due to its limited power resource, for the reasons such as coming back to the original location for charging. This finite time horizon plays a significant role to design the UAV-MR trajectory location. The UAV-MR flies at a fixed altitude h_f while it changes its (x, y) locations serving as a mobile relay during the $0 \leq t \leq T$ flight time. Moreover, h_f has a minimum altitude so as to avoid the tall buildings and other obstacles during the UAV-MR flight duration. Thus, the UAV-MR does not require ascending or descending while the UAV-MR is flying over the ground user.

In this thesis, two of the UAV-MR operation phases, i.e., the takeoff phase and the landing phase, are ignored. Thus, this investigation only focuses on the UAV-MR flight operation period during $0 \leq t \leq T$ flight time. The channel gains for all the possible communication links, such as the BS to the UAV-MR, the UAV-MR to the ground user, and the UAV-MR to the eavesdroppers are calculated based on finite time horizon $0 \leq t \leq T$.

Moreover, the presence of a set of active eavesdroppers in the system is denoted as $\mathcal{M}$, where $\mathcal{M}$=$\{1, 2, 3, ..., M\}$ and M represents the total number of eavesdroppers. The UAV-MR establishes the legitimate link to the ground user and transmits secure information to the ground user. $\mathcal{M}$ set of eavesdroppers attempt to intercept the legitimate communication link from the UAV-MR to the ground user. The UAV-MR knows the perfect locations of the BS and the ground user while only estimated locations with errors of the eavesdroppers are known to the UAV-MR.

Table 2.1: List of mathematical symbols used in Chapter 2

Symbol	Description
$\mathcal{M}$	Set of the eavesdroppers
M	Total number of eavesdroppers
T	The UAV-MR flight time period
h_f	The fixed altitude of the UAV-MR
(x_u, y_u, h_f)	3D location of the UAV-MR
$(x_b, y_b, 0)$	3D location of the BS
$(x_m, y_m, 0)$	Actual 3D location of the eavesdropper, m
$(x_m^a, y_m^a, 0)$	Estimated 3D location of the eavesdropper, m
$(\triangle x_m, \triangle y_m, 0)$	Set of possible errors of the eavesdropper, m
l_m	Radius of the circular region of the eavesdropper, m

2.3 3D Locations of the UAV-MR, the ground user, and the BS

Without the loss of generality, the proposed system is developed in the 3D coordinate system. The time varying UAV-MR location during $0 \leq t \leq T$ is defined as $(x_u(t), y_u(t), h_f)$, where $x_u(t)$ denotes the time varying x-coordinate and $y_u(t)$ defines the time varying y-coordinate. The fixed location of the BS on the ground is $(x_b, y_b, 0)$, where x_b and y_b define the BS in x and y coordinates, respectively. The UAV-MR knows the exact location of the BS. Without the loss of generality, the ground user location is considered as $(0, 0, 0)$, which is correctly known by the UAV-MR. The BS allows the UAV-MR to store the secure information so that the UAV-MR can send the decoded secure information to the ground user. The list of the mathematical symbols used in this chapter is described in Table 2.1.

2.4 Location of Eavesdroppers

It is almost impossible for the UAV-MR to find out the exact locations of the eavesdroppers as most of the eavesdroppers tend to hide themselves well. For eavesdropper m on the ground, its exact location is defined as $(x_m, y_m, 0)$, which is unknown to the UAV-MR. Nevertheless, it is assumed that the UAV-MR knows the regions where the eavesdroppers are located. In order to estimate the locations of the eavesdroppers, a circular region of eavesdropper m, $m \in \mathcal{M}$, is assumed, as shown in Fig. 2.1. The UAV-MR can estimate the region of eavesdroppers locations and calculate the possible errors from the actual locations of the eavesdroppers.

The actual location of the eavesdropper m is calculated as follows.

$$x_m^a = x_m + \triangle x_m, \tag{2.1}$$

$$y_m^a = y_m + \triangle y_m, \tag{2.2}$$

$$z_a = 0, \tag{2.3}$$

where $(x_m^a, y_m^a, 0)$ defines the actual location of the eavesdropper m. $(x_m, y_m, 0)$ is the estimated location of the eavesdropper m.

l_m is the radius of the circular region, where the eavesdropper m is located. $(\triangle x_m, \triangle y_m, 0) \in \varepsilon_m$, where $(\triangle x_m, \triangle y_m, 0)$ defines the possible error in the location of the eavesdropper m. Moreover, ε_m describes the set of possible errors of the eavesdropper m, which is the approximated possible errors from the actual location of the eavesdropper m. The estimated location of the eavesdropper m is the center of the circular region, which is $(x_m, y_m, 0)$. If the eavesdropper m lies on the uncertain circular region [33], the following condition must be satisfied.

$$\sqrt{\triangle x_m^2 + \triangle y_m^2} \leq l_m, \tag{2.4}$$

where l_m is the radius of the uncertain circle with the center $(x_m, y_m, 0)$. In practice, the UAV-MR has a higher chance of LOS air-to-ground communication links due to the higher altitude of the UAV-MR during flight. Thus, the air-to-ground communication link is used

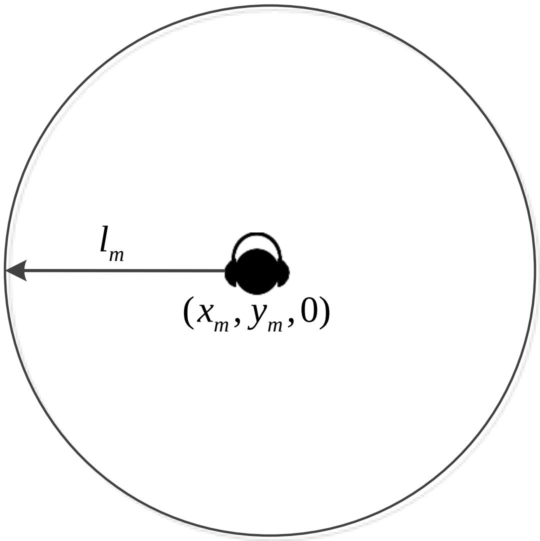

Fig. 2.2: Circular region of the eavesdropper, m, where l_m is the radius and $(x_m, y_m, 0)$ is the center of the circular region.

to send secure information from the UAV-MR to the ground user.

2.5 Summary of the Chapter

This Chapter 2 describes the proposed system model. Moreover, the chapter summarizes the contribution of the thesis. Different scenarios are also addressed using several figures to define the system model accurately and clearly. The locations of all the nodes, i.e., the BS, the UAV-MR, the eavesdroppers, and the ground user, are also explained in detail. The locations of the eavesdroppers, calculated by the UAV-MR, are also addressed in the chapter. The Chapter 3 will discuss the BS to UAV-MR, the UAV-MR to ground user, and the UAV-MR to eavesdroppers channel gains and data rate, which eventually formulate the achievable secrecy rate problem discussed in Chapter 4.

CHAPTER 3
THE ACHIEVABLE SECRECY RATE

This chapter discusses the achievable secrecy rate, including the BS to the UAV-MR, the UAV-MR to the ground user, and the UAV-MR to the eavesdropper data rate. The achievable secrecy rate is then formulated, considering the unknown active presence of multiple eavesdroppers while the UAV-MR transmits secure information from the BS to ground user using the UAV-MR.

The location of the UAV-MR changes with time while the UAV-MR is flying. Thus, the distance between the UAV-MR and the ground user also changes with time. The channel condition is also changed accordingly. A dynamic channel model, reflecting those changes with the UAV-MR trajectory location, is formulated based on the LOS communication links. Before designing the UAV-MR trajectory location, the flight duration of UAV-MR is defined as $0 \leq t \leq T$, where T is a time in second. Moreover, h_f defines the UAV-MR fixed altitude, which can correspond to the minimum UAV-MR altitude required for buildings or mountains avoidance without frequent ascending and descending. However, the time varying location for UAV-MR over $0 \leq t \leq T$ is $(x_u(t), y_u(t), h_f)$. The list of mathematical symbols used in this chapter is listed in Table 3.1.

3.1 The BS to the UAV-MR Data Rate

The BS to the UAV-MR channel gain is based on LOS communication links. This investigation does not consider the Doppler effect [47] due to the mobility of the UAV-MR over $0 \leq t \leq T$ flight time. The channel gain from the BS to the UAV-MR over $0 \leq t \leq T$ flight time based on free space path loss can be calculated as

$$c_{bu}(t) = \frac{\beta_0}{(x_u(t) - x_b)^2 + (y_u[(t) - y_b)^2 + h_f^2}, \tag{3.1}$$

Table 3.1: List of mathematical symbols in Chapter 3

Symbol	Description
r_s	The UAV-MR achievable secrecy rate
c_{bu}	The BS to the UAV-MR channel gain
c_{ug}	The UAV-MR to the ground user channel gain
c_{ue}	The UAV-MR to the eavesdropper, m channel gain
r_{bu}	The BS to the UAV-MR achievable data rate
r_{ug}	The UAV-MR to the ground user achievable data rate
r_{ue}	The UAV-MR to the eavesdropper, m achievable data rate
p_u	The UAV-MR transmit power
p_b	The BS transmit power
β_0	The channel power at reference distance $d_0 = 1$ m
p_u^a	The UAV-MR average power
p_u^m	The UAV-MR peak power
p_b^a	The BS average power
p_b^m	The BS peak power

where β_0 is the channel power gain [48] having reference distance $d_0 = 1$ m, $(x_u(t), y_u(t), h_f)$ is the location of the UAV-MR on the air, and $(x_b, y_b, 0)$ is the location of the BS on the ground. The BS transmit power also needs to be considered for calculating the BS to the UAV-MR data rate.

Thus, this project considers the BS average and peak transmit power constraints as follows.

$$\frac{1}{T-1}\int_{t=1}^{T-1} p_b(t)dt \leq p_b^a, \ \forall t, \tag{3.2}$$

$$0 \leq p_b(t) \leq p_b^m, \ \forall t, \tag{3.3}$$

$$p_b^a \leq p_b^m, \tag{3.4}$$

where $p_b(t) \in \mathbb{R}_+$ is the BS transmitted power. p_b^a and p_b^m are the average and peak power of BS, respectively.

Thus, the achievable data rate from the BS to the UAV-MR can be written as

$$\begin{aligned} r_{bu}(t) &= \log_2\left(1 + \frac{p_b(t)c_{bu}(t)}{\sigma^2}\right), \\ &= \log_2\left(1 + \frac{p_b(t)\gamma}{(x_u(t) - x_b)^2 + (y_u(t) - y_b)^2 + h_f^2}\right), \end{aligned} \tag{3.5}$$

where

$$\gamma = \frac{\beta_0}{\sigma^2}. \tag{3.6}$$

σ^2 is the power of the additive white Gaussian noise (AWGN) at the receiver. Eqn. 3.5 describes the achievable data rate for the BS to UAV-MR.

3.2 The UAV-MR to the Ground User Data Rate

Like the BS to UAV-MR communication links, the channel gain between the UAV-MR and the ground user is also based on LOS communication links. The channel gain between the UAV-MR and the ground user over $0 \leq t \leq T$ flight time based on LOS communication links can be calculated as follows.

$$c_{ug}(t) = \frac{\beta_0}{(x_u(t) - 0)^2 + (y_u(t) - 0)^2 + h_f^2}, \tag{3.7}$$

where $(0, 0, 0)$ is the exact location of the ground user. Similar to sub-section 3.1, the UAV-MR transmit power is also considered. The UAV-MR average and peak transmit power constraints as follows.

$$\frac{1}{T-1}\int_{t=2}^{T} p_u(t)dt \leq p_u^a, \ \forall t, \tag{3.8}$$

$$0 \leq p_u(t) \leq p_u^m, \ \forall t, \tag{3.9}$$

$$p_u^a \leq p_u^m, \tag{3.10}$$

where $p_u(t) \in \mathbb{R}_+$ is the UAV-MR transmitted power. p_u^a and p_u^m are the average and peak powers of the UAV-MR, respectively.

The UAV-MR to the ground user data rate can be calculated as follows.

$$\begin{aligned} r_{ug}(t) &= \log_2\left(1 + \frac{p_u(t)c_{ug}(t)}{\sigma^2}\right), \\ &= \log_2\left(1 + \frac{p_u(t)\gamma}{x_u^2(t) + y_u^2(t) + h_f^2}\right). \end{aligned} \tag{3.11}$$

Eqn. 3.11 describes the achievable data rate for the UAV-MR to ground user.

3.3 The UAV-MR to the Eavesdropper Data Rate

In the proposed system, as there is no direct communication link between the BS and the eavesdroppers, the eavesdroppers attempt to intercept the legitimate UAV-MR to ground user communication links. Moreover, while intercepting the legitimate communication link, the UAV-MR to the eavesdropper communication link is also based on LOS. The channel gain between the UAV-MR and the eavesdropper m, where $m \in M$, can be expressed as follows.

$$c_{ue}(t) = \frac{\beta_0}{(x_u(t) - x_m^a)^2 + (y_u(t) - y_m^a)^2 + h_f^2}, \tag{3.12}$$

where $(x_m^a, y_m^a, 0)$ is the eavesdropper m location. The achievable data rate from the UAV-MR to the eavesdropper m can be written as

$$\begin{aligned} r_{ue}(t) &= \log_2\left(1 + \frac{p_u(t)c_{ue}(t)}{\sigma^2}\right) \\ &= \log_2\left(1 + \frac{p_u(t)\gamma}{(x_u(t) - x_m^a)^2 + (y_u(t) - y_m^a)^2 + h_f^2}\right). \end{aligned} \tag{3.13}$$

3.4 Information Causality Constraint

The information causality constraint [49] is stated as follows. *The secure information of the BS, which is sent to the UAV-MR and the UAV-MR has no clue to know secure information before sending to the UAV-MR, can be gained by the UAV-MR using its local resource. On the other hand, if secure o bits are sent from the BS to the UAV-MR, the complete secure information received by the UAV-MR must not higher be greater than the* *secure* 0 *bits.*

The secure information of the BS is allowed to be stored in the UAV-MR, while the UAV-MR forwards the secure information to the ground user in any of the remaining slots. Now, the information-causality constraint [34, 35] is imposed and it can be expressed as

$$r_{ug}(1) = 0, \tag{3.14}$$

$$\int_{j=2}^{t} r_{ug}(j)dj \leq \int_{j=1}^{t-1} r_{bu}(j)dj. \tag{3.15}$$

Eqs. 3.14 - 3.15 make sure that the UAV-MR forwards only the secure information received from the BS.

3.5 The Achievable Secrecy Rate

To achieve the maximum secrecy rate with the secure UAV-MR and the ground user communication, joint robust UAV-MR trajectory, and transmit power of the UAV-MR and the BS can maximize the achievable secrecy rate. The achievable secrecy rate in bps/Hz can be expressed as

$$r_s(t) = \int_{t=2}^{T} \left(r_{ug}(t) - \max_{m \in \mathcal{M}} \max_{(\triangle x_m, \triangle y_m) \in \varepsilon_m} r_{ue}(t) \right) dt, \tag{3.16}$$

where $r_{ug}(t)$ and $r_{ue}(t)$ are expressed in eq. 3.11 and eq. 3.13, respectively. Eq. 3.16 cannot guarantee the maximized achievable secrecy rate of the proposed system, unless the relevant constraints are added and the maximization problem is formulated. In the next chapter, the achievable secrecy rate optimization problem is formulated and solved sub-optimally. We propose an efficient algorithm aiming to optimize the UAV-MR trajectory location, and transmit power of the UAV-MR and the BS under a number of constraints.

3.6 Summary of the Chapter

The achievable secrecy rate problem is formulated in this chapter, considering the presence of the UAV-MR, the BS, the ground user, and multiple unknown eavesdroppers on the ground for the given UAV-MR flight time. While formulating the problem, UAV-MR trajectory, and the transmit powers of the UAV-MR and the BS design are jointly considered. The BS and the UAV-MR average and peak transmit power constraints are also discussed. Moreover, the information casualty constraint is also introduced so that the UAV-MR can only forward the received secure information to the ground user. In the next Chapter 4, the achievable secrecy rate optimization problem with the relevant constraints is formulated. Several tractable approaches are also proposed to solve the formulated optimization problem sub-optimally.

CHAPTER 4
ACHIEVABLE SECRECY RATE MAXIMIZATION

In this chapter, the achievable secrecy rate maximization problem is formulated. Due to the non-convexity, the formulated achievable secrecy rate maximization cannot be solved just in a single step because of various factors, such as continuous time, nature of eq. 3.16, and the infinite number errors of the locations of the eavesdroppers, etc. A tractable approach is proposed to solve the optimization problem, which is summarized as follows.

- Firstly, due to the UAV-MR continuous time flight duration, time t is discretized into a number of equal time slots using the state space representation in Section 4.1.
- Secondly, the achievable secrecy rate maximization problem is formulated in Section 4.2.
- Thirdly, the achievable formulated problem is non-smooth due to its objective function (i.e., eq. 4.13a). Thus, the non-smoothness of the objective function is tackled in Section 4.3.
- The maximization problem is solved sub-optimally. The sub-optimal solution of the UAV-MR transmit power, and the BS transmit power is achieved for a given UAV-MR trajectory location in Section 4.4. Further the sub-optimal solution of the UAV-MR trajectory location is achieved using the sub-optimal transmit power of the UAV-MR and BS in Section 4.5.
- An efficient algorithm is proposed in Section 4.6, which can guarantee the improved achievable secrecy rate performance.

Moreover, the list of mathematical symbols used in this Chapter 4 is described in Table 4.1.

Table 4.1: List of mathematical symbols in Chapter 4

Symbol	Description
N	Total number of discrete time slots
T	The UAV-MR flight time
ρ_t	The size of a time slot
v_m	The UAV-MR flying speed
$\flat$, η	Non-negative parameters
λ	Lagrange variable
Γ	Variable
z, u, t	Slack variables

4.1 Discrete Linear State Space Representation

In the proposed system, the UAV-MR has the flight duration $0 \leq t \leq T$, where T is in second. The UAV-flight time horizon T is divided into N equal time slots, indexed by $n = 1, 2, 3, ..., N$. The slot size is ρ_t, so we have

$$\rho_t = \frac{T}{N}. \tag{4.1}$$

Moreover, ρ_t is small, static, and equal size time slot. The value of ρ_t is chosen in such a way that the location of the UAV-MR is considered static within each time slot. Thus, the discrete-time UAV-MR location can be represented as $(x_u[n], y_u[n], h_f)$. From eq. 3.5, the achievable data rate between the BS and the UAV-MR can be reformulated as follows.

$$r_{bu}[n] = \log_2\left(1 + \frac{p_b[n]\gamma}{(x_u[n] - x_b)^2 + (y_u[n] - y_b)^2 + h_f^2}\right),\ n = 1, 2, ..., N-1, \tag{4.2}$$

where n is time slot. Similarly, using eq. 3.11, the achievable data rate between the UAV-MR and the ground user can be reformulated as follows.

$$r_{ug}[n] = \log_2\left(1 + \frac{p_u[n]\gamma}{x_u^2[n] + y_u^2[n] + h_f^2}\right),\ n = 2, 3, ..., N. \tag{4.3}$$

The achievable data rate between the UAV-MR and the eavesdropper m from eq. 3.13 can be reformulated as follows.

$$r_{ue}[n] = \log_2\left(1 + \frac{p_u[n]\gamma}{(x_u[n] - x_m^a)^2 + (y_u[n] - y_m^a)^2 + h_f^2}\right),\ n = 2, 3, ..., N. \tag{4.4}$$

The BS transmit power constraints from eqs. 3.2 - 3.3 can be reformulated as follows.

$$\frac{1}{N-1}\sum_{n=1}^{N-1} p_b[n] \leq p_b^a,\ \forall n, \tag{4.5}$$

$$0 \leq p_b[n] \leq p_b^m,\ \forall n. \tag{4.6}$$

Similarly, using eqs. 3.8 - 3.9, the UAV-MR transmit power constraints can be reformulated as follows.

$$\frac{1}{N-1}\sum_{n=2}^{N} p_u[n] \leq p_u^a,\ \forall n, \tag{4.7}$$

$$0 \leq p_u[n] \leq p_u^m,\ \forall n. \tag{4.8}$$

The information-causality constraint is also represented using eqs. 3.14 - 3.15 in terms of state space representation as follows

$$r_{ug}[1] = 0, \tag{4.9}$$

$$\sum_{j=2}^{n} r_{ug}[j] \leq \sum_{j=1}^{n-1} r_{bu}[j],\ n = 2, 3, ..., N. \tag{4.10}$$

Let the initial and final locations of the UAV-MR are $(x_u[1], y_u[1], h_f)$ and $(x_u[N], y_u[N], h_f)$, respectively. Thus, the UAV-MR mobility constraint can be written as

$$(x_u[n] - x_u[n-1])^2 + (y_u[n] - y_u[n-1])^2 \leq (v_m\rho_t)^2, \tag{4.11}$$

where v_m defines the UAV-MR speed. Finally, the achievable secrecy rate in terms of discrete time representation can be expressed as

$$r_s[n] = \sum_{n=2}^{N} \Bigg[r_{ug}[n] - \max_{m \in \mathcal{M}} \max_{(\triangle x_m, \triangle y_m) \in \varepsilon_m} r_{ue}[n] \Bigg]. \tag{4.12}$$

4.2 The Achievable Secrecy Rate Maximization Problem Formulation

Now, using eq. 4.12 and relevant constraints, the achievable secrecy rate maximization can be formulated as follows.

$$\max_{x_u[n], y_u[n], p_u[n], p_b[n]} \sum_{n=2}^{N} \Bigg[r_{ug}[n] - \max_{m \in \mathcal{M}} \max_{(\triangle x_m, \triangle y_m) \in \varepsilon_m} r_{ue}[n] \Bigg]^{+}, \tag{4.13a}$$

$$\text{s.t.} \sum_{j=2}^{n} \log_2 \left(1 + \frac{p_u[j] c_{ug}[j]}{\sigma^2} \right) \leq \sum_{j=1}^{n-1} \log_2 \left(1 + \frac{p_b[j] c_{bu}[j]}{\sigma^2} \right), \; n = 2, 3, ..., N, \tag{4.13b}$$

$$(x_u[n] - x_u[n-1])^2 + (y_u[n] - y_u[n-1])^2 \leq (v_m \rho_t)^2, \tag{4.13c}$$

$$\frac{1}{N-1} \sum_{n=1}^{N-1} p_b[n] \leq p_b^a, \tag{4.13d}$$

$$0 \leq p_b[n] \leq p_b^m, \tag{4.13e}$$

$$\frac{1}{N-1} \sum_{n=2}^{N} p_u[n] \leq p_u^a, \tag{4.13f}$$

$$0 \leq p_u[n] \leq p_u^m, \tag{4.13g}$$

where, in eq. 4.13a, $[.]^{+} \triangleq \max(., 0)$. Eq. 4.13b implies the information causality constraint. Eq. 4.13c defines the mobility constraint of the UAV-MR during the UAV-MR flight time. Moreover, eqs. 4.13d - 4.13e define the average and peak power constraints of the BS, respectively. On the other hand, eqs. 4.13f - 4.13g describe the average and peak power constraints of the UAV-MR, respectively. However, eq. 4.13 is too challenging to solve using the conventional optimization technique due to the following reasons.

1. The non-convexity nature of eq. 4.13a and eq. 4.13b.

2. The non-smoothness of the objective function due to $[.]^{+}$ operator.

3. Infinite number of possible errors of finding the actual locations of the eavesdroppers.

Thus, a tractable approach to solving eq. 4.13 is proposed in the Section 4.3 - Section 4.6.

4.3 Tackling Non-smoothness of Objective Function

The non-smoothness of eq. 4.13a can be tackled as follows.

$$\max_{x_u[n],y_u[n],p_u[n],p_b[n]} \sum_{n=2}^{N} \left[r_{ug}[n] - \max_{m\in\mathcal{M}} \max_{(\triangle x_m,\triangle y_m)\in\varepsilon_m} r_{ue}[n] \right], \tag{4.14a}$$

$$\text{s.t. } (4.13b) \;-\; (4.13g).$$

Proposition: Eq. 4.13 and eq. 4.14 are equivalent and share the same optimal solution. The proof is given in Appendix A. However, a detailed explanation can be found in [50].

Eq. 4.14 is still non-convex and challenging to solve. To make it tractable, the optimization variables, i.e., the UAV-MR trajectory (x_u, y_u), and the BS transmit power, p_b, and the UAV-MR transmit power, p_u, are solved sub-optimally. The division facilitates the designing of the algorithm to solve eq. 4.13. Firstly, the BS transmit power, p_b, and the UAV-MR transmit power, p_u, are optimized under a given UAV-MR trajectory location (x_u, y_u). Secondly, the UAV-MR trajectory location (x_u, y_u) is optimized under the optimal p_u and p_b. The iteration continues till the process converges.

4.4 Sub-optimal Solution of the UAV-MR and the BS Transmit Power

The UAV-MR and the BS transmit power optimization for a given trajectory is practicably feasible if the UAV-MR is required to serve in a fixed location, such as military, border surveillance, and smart health networks, etc. For a given UAV-MR trajectory location (x_u, y_u), the optimal solution of the UAV-MR transmit power, p_u and the BS transmit power, p_b can be written from eq. 4.13 as

$$\max_{p_u[n],p_b[n]} \sum_{n=2}^{N} \left[r_{ug}[n] - \max_{m\in\mathcal{M}} \max_{(\triangle x_m,\triangle y_m)\in\varepsilon_m} r_{ue}[n] \right], \tag{4.15a}$$

$$\text{s.t. } (4.13b),\ (4.13d)\ -\ (4.13g).$$

The optimal solution of eq. 4.15 needs to satisfy all the constraints. However, eq. 4.15a (i.e. the objective function) and eq. 4.13b are not a convex function yet. Thus, in order to tackle eq. 4.15a, the following expression can be written as

$$r_s^{new}[n] = \sum_{n=2}^{N} \left[\log_2\left(1 + \frac{p_u[n]}{\sigma^2} c_{ug}[n]\right) - \log_2\left(1 + \frac{p_u[n]}{\sigma^2} c_{ue}^{new_1}[n]\right)\right]. \tag{4.16}$$

Moreover, using eqs. 2.1 - 2.2, $c_{ue}^{new_1}$ can be defined as follows.

$$c_{ue}^{new_1}[n] = \frac{\beta_0}{\min\limits_{(\triangle x_m,\triangle y_m)\in\varepsilon_m} (x_u[n] - x_m - \triangle x_m)^2 + (y_u[n] - y_m - \triangle y_m)^2 + h_f^2}. \tag{4.17}$$

However, eq. 4.17 is still not tractable due to the presence of $(\triangle x_m, \triangle y_m) \in \varepsilon_m$. Thus, substituting eq. 2.4 in eq. 4.17, the following expression can be found.

$$\begin{aligned} c_{ue}^{new}[n] &= \frac{\beta_0}{\min\limits_{(\triangle x_m,\triangle y_m)\in\varepsilon_m} (x_u[n] - x_m)^2 + (y_u[n] - y_m)^2 + h_f^2 + l_m^2 + b} \\ &\approx \frac{\beta_0}{\min\limits_{(\triangle x_m,\triangle y_m)\in\varepsilon_m} (x_u[n] - x_m)^2 + (y_u[n] - y_m)^2 + h_f^2 + l_m^2}, \end{aligned} \tag{4.18}$$

where $b = -2(x_u[n] - x_m) \triangle x_m - 2(y_u[n] - y_m) \triangle y_m$, which is negligible as $(\triangle x_m, \triangle y_m)$ is significantly small. However, from eq. 4.18, it can be said that the distance between the actual eavesdropper m, which is (x_m, y_m) and the UAV-MR location, which is (x_u, y_u) is greater than the eavesdropper circular region l_m (the detail information can be found in [33]). The distance between the UAV-MR and the actual location of the eavesdropper m

can be expressed as

$$d_{u,e}[n] = \sqrt{(x_u[n] - x_m)^2 + (y_u[n] - y_m)^2}. \tag{4.19}$$

If $d_{u,e}[n] > l_m$, then c_{ue}^{new} is

$$c_{ue}^{new}[n] = \frac{\beta_0}{(\sqrt{(x_u[n] - x_m)^2 + (y_u[n] - y_m)^2} - l_m^2)^2 + h_f^2}. \tag{4.20}$$

If $d_{u,e}[n] \leq l_m$, then c_{ue}^{new} is

$$c_{ue}^{new}[n] = \frac{\beta_0}{h_f^2}. \tag{4.21}$$

Moreover, eq. 4.13b is not a convex. It can be tackled to make it convex by introducing variable, Γ as follows.

$$\sum_{j=2}^{n} \Gamma[j] \leq \sum_{j=1}^{n-1} \log_2 \left(1 + \frac{p_b[j]c_{bu}[j]}{\sigma^2}\right), \; n = 2, ..., N, \tag{4.22}$$

$$\Gamma[n] \leq \log_2 \left(1 + \frac{p_u[n]c_{ug}[n]}{\sigma^2}\right), \; n = 1, 2, ..., N-1. \tag{4.23}$$

Eq. 4.22 - 4.23 are equivalent to eq. 4.13b, which are also convex. Eq. 4.15 can be reformulated as follows.

$$\max_{p_u[n], p_b[n], \Gamma[n]} \sum_{n=2}^{N} \left[\Gamma[n] - \log_2 \left(1 + \frac{p_u[n]c_{ue}^{new}[n]}{\sigma^2}\right)\right], \tag{4.24a}$$

$$\text{s.t. } (4.22) \; - \; (4.23), \; (4.13d) \; - \; (4.13g).$$

Comparing eq. 4.15 and eq. 4.24, it is obvious that the optimal solution of eq. 4.24 satisfies all the constraints in eq. 4.15. The theory of contradiction can prove it. Thus it can be said that eq. 4.15 and eq. 4.24 are equivalent as eqs. 4.22 - 4.23 are equivalent to eq. 4.13b. However, eq. 4.24 is not a convex function due to its objective function i.e., eq. 4.24a. Fortunately, eq. 4.24 is solvable at some $p_u^f[n]$ feasible points using the difference of the concave (DC) method. The main idea of the DC method is that it linearizes the objective function at some feasible points.

Thus, using first-order Taylor series expansion and $f(g^f) + f'(g)(g - g^f) \leq f(g)$, eq. 4.24a can be expressed as

$$r_s^{new}[n] = \sum_{n=2}^{N} \left[\Gamma[n] - \frac{c_{ue}^{new}[n](p_u[n] - p_u^f[n])}{1 + p_u^f[n] c_{ue}^{new}[n]} - \log_2 \left(1 + \frac{p_u^f[n] c_{ue}^{new}[n]}{\sigma^2} \right) \right]. \tag{4.25}$$

Thus, the reformulated optimization problem can be written as

$$\max_{p_u[n], p_b[n], \Gamma[n]} \sum_{n=2}^{N} \left[\Gamma[n] - \frac{c_{ue}^{new}[n](p_u[n] - p_u^f[n])}{1 + p_u^f[n] c_{ue}^{new}[n]} - \log_2 \left(1 + \frac{p_u^f[n] c_{ue}^{new}[n]}{\sigma^2} \right) \right], \tag{4.26a}$$

s.t. (4.22) − (4.23), (4.13d) − (4.13g).

Lemma 1 *The semi-closed and sub-optimal solution of p_b and p_u are as follows.*

$$p_u^*[n] = \left[\frac{\left(1 - \sum_{i=n}^{N} \lambda_i \right) p_u^f[n] c_{ue}^{new}[n]}{\eta + c_{ue}^{new}[n](\eta p_u^f[n] + 1)} - \frac{1}{c_{ug}[n]} \right]^+, \ \forall n, \tag{4.27}$$

$$p_b^*[n] = \left[\flat \left(\sum_{j=n+1}^{N} \lambda_j \right) - \frac{1}{c_{bu}[n]} \right]^+, \ \forall n. \tag{4.28}$$

where λ_j is the dual Lagrangian variables. Both eqs. 4.27 - 4.28 are the optimal solution of eq. 4.26.

Moreover, $\flat$ and η are the non-negative parameters. $\flat$ and η parameters meet the following conditions, respectively.

$$p_b^a = \frac{1}{N-1} \sum_{n=1}^{N-1} p_b^*[n], \tag{4.29}$$

$$p_u^a = \frac{1}{N-1} \sum_{n=2}^{N} p_u^*[n]. \tag{4.30}$$

In order to get the Lagrange dual optimal solution, the dual Lagrange variable, λ must satisfy $\sum_{n=2}^{N} \lambda \leq 1$.

Proof. The proof is given in Appendix B. More detail information can be found in [41].

4.5 Sub-optimal Solution of the UAV-MR Trajectory Design

Now, the optimal UAV-MR trajectory location (x_u, y_u) is achieved for the optimal UAV-MR transmit power, p_b and the BS transmit power, p_u, which are achieved from Section 4.4. This scenario may also be correspondent to the practical situation; for example, the UAV-MR and the BS transmit the fixed power due to their hardware limitations. The sub-optimal problem can be expressed as follows.

$$\max_{x_u[n], y_u[n]} \sum_{n=2}^{N} [a_n - b_n], \tag{4.31a}$$

$$\text{s.t. } (4.13b) \ - \ (4.13c).$$

where

$$a_n = \log_2\left(1 + \frac{p_u[n]}{\sigma^2} \frac{\beta_0}{x_u[n]^2 + y_u[n]^2 + h_f^2}\right), \tag{4.32}$$

$$b_n = \log_2\left(1 + \frac{p_u[n]}{\sigma^2} \frac{\beta_0}{\min\limits_{(\triangle x_m, \triangle y_m) \in \varepsilon_m} (x_u[n] - x_m^a)^2 + (y_u[n] - y_m^a)^2 + h_f^2}\right). \tag{4.33}$$

Eq. 4.31 is still not a convex problem due to the objective function (i.e., eq. 4.31a) and the information causality constraint in eq. 4.13b. Moreover, this sub-optimal problem cannot be solved sub-optimally in the polynomial time due to the infinite number of possible multiple locations errors of the eavesdroppers, i.e., $(\triangle x_m, \triangle y_m)$. In order to tackle the non-convexity of eq. 4.31a and eq. 4.13b, slack variables z, t, u, and variable Γ are introduced to solve the problem sub-optimally.

Firstly, in order to tackle the non-convexity of eq. 4.13b, it can be reformulated as follows.

$$\sum_{j=2}^{n} \Gamma[j] \leq \sum_{j=1}^{n-1} \log_2 \left(1 + \frac{\beta_0 p_b[j]}{\sigma^2[(x_u[j]-x_b)^2 + (y_u[j]-y_b)^2 + h_f^2]}\right), \; n = 2, ..., N, \tag{4.34}$$

$$\Gamma[n] \leq \log_2 \left(1 + \frac{\beta_0 p_u[n]}{\sigma^2(x_u^2[n] + y_u^2[n] + h_f^2)}\right), \; n = 1, 2, ..., N-1, \tag{4.35}$$

where Γ is newly introduced variable. However, eqs. 4.34 - 4.35 are not convex. In order to tackle the non-convexity, slack variables, t and u are introduced in eqs. 4.34 - 4.35, respectively, as follows.

$$\sum_{j=2}^{n} \Gamma[j] \leq \sum_{j=1}^{n-1} \log_2 \left(1 + \frac{\beta_0 p_b[j]}{\sigma^2 t[j]}\right), \; n = 2, ..., N, \tag{4.36}$$

$$(x_u[j]-x_b)^2 + (y_u[j]-y_b)^2 + h_f^2 - t[j] \leq 0. \tag{4.37}$$

Eqs. 4.36 - 4.37 are reformulated by introducing the slack variable t from eq. 4.34.

$$\Gamma[n] \leq \log_2 \left(1 + \frac{\beta_0 p_u[n]}{\sigma^2 u[n]}\right), \; n = 1, 2, ..., N-1, \tag{4.38}$$

$$x_u[n]^2 + y_u[n]^2 + h_f^2 - u[n] \leq 0. \tag{4.39}$$

On the other hand, eqs. 4.38 - 4.39 are reformulated by introducing the slack variable u from eq. 4.35.

However, slack variables, t and u, can be expressed as follows

$$t \triangleq [t[1], t[2], t[3], ...t[N]]^\dagger, \tag{4.40}$$

$$u \triangleq [u[1], u[2], u[3], ...u[N]]^\dagger. \tag{4.41}$$

Moreover, first-order Taylor expansion can be applied to the logarithm functions of both eq. 4.36 and eq. 4.38. From eq. 4.36, it can be written using first-order Taylor expansion as follows.

$$\frac{\partial \log_2\left(1+\frac{\beta_0 p_b[j]}{\sigma^2 t[j]}\right)}{\partial t[j]} = -\frac{\frac{\beta_0 p_b[j]}{\sigma^2}}{(t^2[j]+\frac{\beta_0 p_b[j]}{\sigma^2}t[j])\ln 2}. \tag{4.42}$$

At feasible point $t^f[j]$, the following expression can be written, using $f(g^f)+f'(g)(g-g^f)\leq f(g)$, where $(.)^f$ and $(.)'$ are the feasible and partial derivative, respectively, as follows.

$$\frac{\frac{\beta_0 p_b[j]}{\sigma^2}(t^f[j]-t[j])}{t^f[j](t^f[j]+\frac{\beta_0 p_b[j]}{\sigma^2})\ln 2} + \left(1+\frac{\beta_0 p_b[j]}{\sigma^2 t^f[j]}\right) \leq \log_2\left(1+\frac{\beta_0 p_b[j]}{\sigma^2 t[j]}\right). \tag{4.43}$$

Using eqs. 4.42 - 4.43, eq. 4.34 can be reformulated as follows.

$$\sum_{j=2}^{n}\Gamma[j] \leq \sum_{j=1}^{n-1}\left[\frac{\frac{\beta_0 p_b[j]}{\sigma^2}(t^f[j]-t[j])}{t^f[j](t^f[j]+\frac{\beta_0 p_b[j]}{\sigma^2})\ln 2} + \log_2\left(1+\frac{\beta_0 p_b[j]}{\sigma^2 t^f[j]}\right)\right]. \tag{4.44}$$

Similarity, eq. 4.38 can be rewritten as

$$\frac{\partial \log_2\left(1+\frac{p_u^n}{u[n]}\right)}{\partial u[n]} = -\frac{p_u^n}{(u^2[n]+p_u^n u[n])\ln 2}, \tag{4.45}$$

where $p_u^n = \frac{\beta_0 p_u[n]}{\sigma^2}$. At feasible point $u^f[n]$, the following expression can be written, using $f(g^f)+f'(g)(g-g^f)\leq f(g)$, where $(.)^f$ and $(.)'$ are the feasible and partial derivative, respectively, as follows.

$$\frac{p_u^n(u^f[n]-u[n])}{u^f[n](u^f[n]+p_u^n)\ln 2} + \log_2\left(1+\frac{p_u^n}{u^f[n]}\right) \leq \log_2\left(1+\frac{p_u^n}{u[n]}\right), \tag{4.46}$$

Using eqs. 4.45 - 4.46, eq. 4.35 can be reformulated as follows

$$\Gamma[n] \leq \left[\frac{p_u^n(u^f[n]-u[n])}{u^f[n](u^f[n]+p_u^n)\ln 2} + \log_2\left(1+\frac{p_u^n}{u^f[n]}\right)\right]. \tag{4.47}$$

Due to introducing the slack variables, eq. 4.31 can be reformulated to eq. 4.48 as follows

$$\max_{x_u[n],y_u[n],z[n],t[n],u[n],\Gamma[n]} \sum_{n=2}^{N} \left[\Gamma[n] - \log_2\left(1 + \frac{p_u^n}{z[n]}\right)\right], \tag{4.48a}$$

$$\text{s.t.} \min_{(\triangle x_m,\triangle y_m)\in\varepsilon_m} (x_u[n] - x_m - \triangle x_m)^2 + (y_u[n] - y_m - \triangle y_m)^2 + h_f^2 \geq z[n], \tag{4.48b}$$

$$z[n] \geq h_f^2, \tag{4.48c}$$

$(4.13c)$, (4.37), (4.39), (4.44), (4.47),

where z is also a slack variable, followed by

$$z \triangleq [z[1], z[2], z[3], ..., z[N]^\dagger, \tag{4.49}$$

Eq. 4.31 and eq. 4.48 share the same sub-optimal solution of the UAV-MR trajectory location, i.e. sub-optimal solution of the UAV-MV trajectory location (x_u, y_u). This thesis focuses on solving eq. 4.48 in order to achieve sub-optimal solution of (x_u, y_u).

Proof. The proof is given in Appendix C.

However, eqs. 4.48 is still challenging to solve due to the infinite number of unknown possible errors from the actual location of eavesdropper m in eq. 4.48b.

To make eqs. 4.48b tractable, eq. 2.1 - 2.4 are substituted in eq. 4.48b as

$$-(x_u[n] - x_m^a - \triangle x_m)^2 - (y_u[n] - y_m^a - \triangle y_m)^2 + z[n] - h_f^2 \leq 0, \forall m, \tag{4.50}$$

$$\triangle\, x_m^2 + \triangle y_m^2 \leq l_m^2, \forall m. \tag{4.51}$$

$\mathcal{S}$*-Procedure* method is applied to tackle the infinite number of possible locations errors of the eavesdroppers. An overview of $\mathcal{S}$*-Procedure* is described in Appendix D.

Any feasible point $(\triangle x_m^f, \triangle y_m^f)$ exists, for example $(\triangle x_m^f, \triangle y_m^f) = (1, 1)$, such that

$$\triangle\, {x_m^f}^2 + \triangle {y_m^f}^2 \leq l_m^2. \tag{4.52}$$

Then the following implication holds

$$-(x_u[n]-x_m-\triangle x_m)^2-(y_u[n]-y_m-\triangle y_m)^2+z[n]-h_f^2 \leq 0 \Rightarrow \triangle x_m^2+\triangle y_m^2 \leq l_m^2 \quad (4.53)$$

if and only if $\varepsilon_m \geq 0$ exists such that

$$\begin{bmatrix} a_1[n] & a_2[n] & a_3[n] \\ b_1[n] & b_2[n] & b_3[n] \\ c_1[n] & c_2[n] & c_3[n] \end{bmatrix} \succeq 0, \quad (4.54)$$

where

$$a_1[n] = \varepsilon_m[n]+1, \quad (4.55)$$

$$a_2[n] = 0, \quad (4.56)$$

$$a_3[n] = x_m - x_u[n], \quad (4.57)$$

$$b_1[n] = 0, \quad (4.58)$$

$$b_2[n] = \varepsilon_m[n]+1, \quad (4.59)$$

$$b_3[n] = y_m - y_u[n], \quad (4.60)$$

$$c_1[n] = x_m - x_u[n], \quad (4.61)$$

$$c_2[n] = y_m - y_u[n], \quad (4.62)$$

$$c_3[n] = (x_u[n]-x_m)^2+(y_u[n]-y_m)^2+h_f^2-z[n]-l_m^2\varepsilon_m[n]. \quad (4.63)$$

Thus, eq. 4.54 is equivalent eq. 4.48b. Now, eq. 4.48 can be reformulated as follows

$$\max_{x_u[n],y_u[n],z[n],u[n],t[n],\Gamma[n]\varphi[n]} \sum_{n=2}^{N}\left[\Gamma[n]-\log_2\left(1+\frac{p_u^n}{z[n]}\right)\right], \tag{4.64a}$$

$$\text{s.t. } z[n] \geq h_f^2, \tag{4.64b}$$

$$\varepsilon_m[n] \geq 0, \tag{4.64c}$$

$$(4.13c),\ (4.37),\ (4.39),\ (4.44),\ (4.47),\ (4.54),$$

where φ is also a slack variables, which can be expressed as follows.

$$\varphi \triangleq [\varepsilon_1, \varepsilon_2, \varepsilon_3, ..., \varepsilon_m], \tag{4.65}$$

where $\varepsilon_m \triangleq [\varepsilon_m[1], \varepsilon_m[2], \varepsilon_m[3], ..., \varepsilon_m[N]]^{\dagger}$. Moreover, eq. 4.64 is not still a convex problem due to eq. 4.64a. Eq. 4.54 is a a function of $(x_u[n], y_u[n], z[n], \varepsilon_m[n])$, which is not linear in nature because of the presence of $[.]^2$. Thus, these make eq. 4.64 too challenging to solve it optimally.

In order to solve eq. 4.64, an efficient algorithm is proposed in this work, which can solve the non-convex problem iteratively. Moreover, this algorithm can achieve the approximate solution of eq. 4.64. The explanation of the algorithm is described as follows.

- Let the following the feasible points of the UAV-MR trajectory location, (x_u, y_u), and the slack variable, z,

$$\mathbf{x_u} \triangleq [x_u^f[1], x_u^f[2], x_u^f[3], ..., x_u^f[N]], \tag{4.66}$$

$$\mathbf{y_u} \triangleq [y_u^f[1], y_u^f[2], x_u^f[3], ..., y_u^f[N]], \tag{4.67}$$

$$\mathbf{z} \triangleq [z^f[1], z^f[2], z^f[3], ..., z^f[N]]. \tag{4.68}$$

- The first order Taylor expansion has been implemented in $\log_2\left(1+\frac{p_u^n}{z[n]}\right)$, where $p_u^n = \gamma p_u[n]$, can be expressed using the first order Taylor expansion at feasible point

$z^f[n]$ as follows.

$$\frac{\partial \log_2\left(1+\frac{p_u^n}{z[n]}\right)}{\partial z[n]} = -\frac{p_u^n}{(z^2[n]+p_u^n z[n])\ln 2}. \tag{4.69}$$

At feasible point $z^f[n]$, the following expression can be written, using $f(g^f)+f'(g)(g-g^f) \leq f(g)$, where $(.)^f$ and $(.)'$ are the feasible and partial derivative, respectively, as follows.

$$\frac{p_u^n(z^f[n]-z[n])}{z^f[n](z^f[n]+p_u^n)\ln 2} + \log_2\left(1+\frac{p_u^n}{z^f[n]}\right) \leq \log_2\left(1+\frac{p_u^n}{z[n]}\right). \tag{4.70}$$

- Moreover, the first order Taylor expansion of $x_u^2[n]$ and $y_u^2[n]$ is also implemented at feasible points $x_u^f[n]$ and $y_u^f[n]$, respectively, as follows.

$$\frac{\partial x_u^2[n]}{\partial x_u[n]} = 2x_u[n], \tag{4.71}$$

$$\frac{\partial y_u^2[n]}{\partial y_u[n]} = 2y_u[n]. \tag{4.72}$$

Using $f(g^f)+f'(g)(g-g^f) \leq f(g)$, it can be written as follows.

$$-{x_u^f}^2[n] + 2x_u^f[n]x_u[n] \leq x_u^2[n], \tag{4.73}$$

$$-{y_u^f}^2[n] + 2y_u^f[n]y_u[n] \leq y_u^2[n]. \tag{4.74}$$

- Moreover, $c_3[n]$ needs to be expressed at some feasible points due to the non-linear parameter, i.e., $[.]^2$. Using eq. 4.73 -4.74, the following can be found.

$$\begin{aligned} c_3^f[n] = h_f^2 - z[n] - {x_u^f}^2[n] - {y_u^f}^2[n] + 2x_u^f[n]x_u[n] + x_m^2 \\ + y_m^2 + 2y_u^f[n]y_u[n] - 2x_m x_u[n] - 2y_m y_u[n] - l_m^2 \varepsilon_m[n]. \end{aligned} \tag{4.75}$$

Thus, using the approximation in eqs. 4.66 - 4.75, eq. 4.64 is approximated to eq. 4.76 as follows

$$\max_{x_u[n],y_u[n],z[n],t[n],u[n],\Gamma[n],\varphi[n]} \sum_{n=2}^{N} \Big[\Gamma[n] - q[n]\Big], \tag{4.76a}$$

$$\text{s.t.} \begin{bmatrix} a_1[n] & a_2[n] & a_3[n] \\ b_1[n] & b_2[n] & b_3[n] \\ c_1[n] & c_2[n] & c_3^f[n] \end{bmatrix} \succeq 0, \tag{4.76b}$$

$$z[n] \geq h_f^2, \tag{4.76c}$$

$$\varepsilon_m[n] \geq 0, \tag{4.76d}$$

$$(4.13c),\ (4.37),\ (4.39),\ (4.44),\ (4.47),$$

where

$$q[n] = \frac{p_u^n(z^f[n] - z[n])}{z^f[n](z^f[n] + p_u^n)\ln 2} - \log_2\left(1 + \frac{p_u^n}{z^f[n]}\right). \tag{4.77}$$

$q[n]$ is derived from eq. 4.70. Eq. 4.76 is a semidefinite programming problem. The solution of the newly formulated problem eq. 4.76 has a feasible solution to eq. 4.64. This can be shown as follows.

- Using the eqs. 4.73 - 4.74, which are lower bounds for $x_u^2[n]$ and $y_u^2[n]$, respectively, the following condition is true.

$$\begin{bmatrix} a_1[n] & a_2[n] & a_3[n] \\ b_1[n] & b_2[n] & b_3[n] \\ c_1[n] & c_2[n] & c_3[n] \end{bmatrix} \succeq \begin{bmatrix} a_1[n] & a_2[n] & a_3[n] \\ b_1[n] & b_2[n] & b_3[n] \\ c_1[n] & c_2[n] & c_3^f[n] \end{bmatrix}. \tag{4.78}$$

  Thus, eq. 4.76b implies to eq, 4.54. Thus, the solution of eq. 4.76 is a feasible solution to eq. 4.64.

- From eq. 4.70, it is clear that eq. 4.70 is a lower bound of $\log_2\left(1+\frac{p_u^n}{z[n]}\right)$. Thus, lower bound of eq. 4.64a is maximized using eq. 4.76a, which is equal to the lower bound at $(\mathbf{x_u^f}, \mathbf{y_u^f}, \mathbf{z^f})$ feasible point. Thus, eq. 4.76a shares the same or smaller solution $(\mathbf{x_u^f}, \mathbf{y_u^f}, \mathbf{z^f})$ than eq. 4.64a.

Now, eq. 4.76 can be solved using IPM. An overview of the IPM is described in Appendix E.

4.6 Proposed Efficient Algorithm

Now, an efficient algorithm is proposed to solve the original problem in eq. 4.13 optimally. The detail of the overall achievable secrecy rate problem is summarized in the algorithm 1. The algorithm 1 solves eq. 4.13 sub-optimally, using eq. 4.26 and eq. 4.76. Eventually, the algorithm can achieve the optimal solution until it converges. However, the solution of the UAV-MR trajectory location and the UAV-MR and the BS transmit power is given as follows.

- The UAV-MR and the BS transmit power is optimized under given UAV-MR trajectory location, using eq. 4.26.
- The UAV-MR trajectory is optimized under the optimal the UAV-MR, and the BS transmit power, using eq. 4.76.
- The overall algorithm is solved iteratively until it converges.

The overall algorithm solves the original problem both alternatively and iteratively. It continues until algorithm 1 converges. The algorithm 1 is summarized as follows.

4.7 Summary of the Chapter

This chapter solves the achievable secrecy rate maximization problem in several steps as the conventional optimization techniques cannot solve the problem. Firstly, the discrete time is applied to the optimization problem so that the UAV-MR trajectory location, and the transmit power of the UAV-MR and the BS constraints can be analyzed in each static and the equal time slot. After that, the non-smoothness of the objective function is tackled. Then, two sub-problems of the original optimization problem are formulated. They are

Algorithm 1 Proposed algorithm for optimal solution in eq. 4.13

```
1:  **Initialize** : $x_u^f[n] = x_{u(j-1)}^f[n]$, $y_u^f[n] = y_{u(j-1)}^f[n]$, $p_u[n] = p_{u(j-1)}[n]$, $p_b[n] = p_{b(j-1)[n]}$,
    and $j = 0$.
2:  Set $j \longleftarrow j + 1$
3:  **Optimization**:
4:  **repeat**
5:      Solve sub-optimal UAV-MR and BS transmit power design (i.e., eq. 4.26) under
    given UAV-MR trajectory location $x_u$ and $y_u$.
6:      Obtain optimal solution $p_u$ and $p_b$.
7:      Solve sub-optimal UAV-MR trajectory design (i.e., eq. 4.76) under the optimal UAV-
    MR transmit power, $p_u$ and BS transmit power, $p_b$.
8:      Obtain optimal solution $x_u$ and $y_u$.
9:      Then go to Step: 5.
10: **until** convergence
```

named as the UAV-MR, and the BS transmit power optimization location under the given UAV-MR trajectory. After that, the UAV-MR trajectory location is optimized under given the UAV-MR, and the BS transmit power. Finally, an efficient algorithm is proposed based on DC, $\mathcal{S}$-*Procedure*, and IPM methods.

CHAPTER 5
SIMULATION RESULTS

This chapter presents the simulation results, which validate the improved achievable secrecy rate performance based on the proposed robust joint UAV-MR trajectory, and transmit power of the UAV-MR and the BS, i.e., the algorithm 1. The proposed robust model in the algorithm 1 is compared with the backbench method, named as the non-robust UAV-MR trajectory, and transmit power of the UAV-MR, and the BS optimization. The non-robust approach is defined as follows. Like the known locations of the BS and the ground user to the UAV-MR, the UAV-MR also considers the approximate location as the exact locations of the eavesdroppers on the ground. The non-robust scheme in terms of the locations of the eavesdroppers is defined as follows.

$$x_m^a = x_m + \triangle x_m, \tag{5.1}$$

$$y_m^a = y_m + \triangle y_m, \tag{5.2}$$

where $(\triangle x_m, \triangle y_m) = (0, 0)$. Thus, $x_m^a = x_m$ and $y_m^a = y_m$. However, the UAV-MR flies, following the unidirectional trajectory path from the BS to the ground user, at a fixed velocity during the UAV-MR flight time. The acceleration process and the deceleration process of the UAV-MR are considered insignificant in the proposed system. The list of parameters used in the simulation is illustrated in Table 5.1.

5.1 The UAV-MR Trajectory Design

Fig. 5.1 shows the UAV-MR trajectory locations for the proposed algorithm 1. It can be seen from Fig. 5.1, the UAV-MR starts hovering between the BS and the ground user. Moreover, the UAV-MR starts hovering from the BS to the ground user, followed by a trajectory path. For the UAV-MR trajectory path, it can be seen that the UAV-MR keeps

Table 5.1: List of parameters used in the simulation

Symbol	Description
The radius of circular region of the eavesdropper	8 m
Approximate location of the eavesdropper	$(-400, 0)$ m
The BS location	$(100, 500)$ m
The UAV-MR fixed altitude	80 m
Dicretized equal time slot	1
The UAV-MR flying speed	50 m/s
At $d_0 = 1$ m distance, $\gamma (= \frac{\beta_0}{\sigma^2})$	80 dB

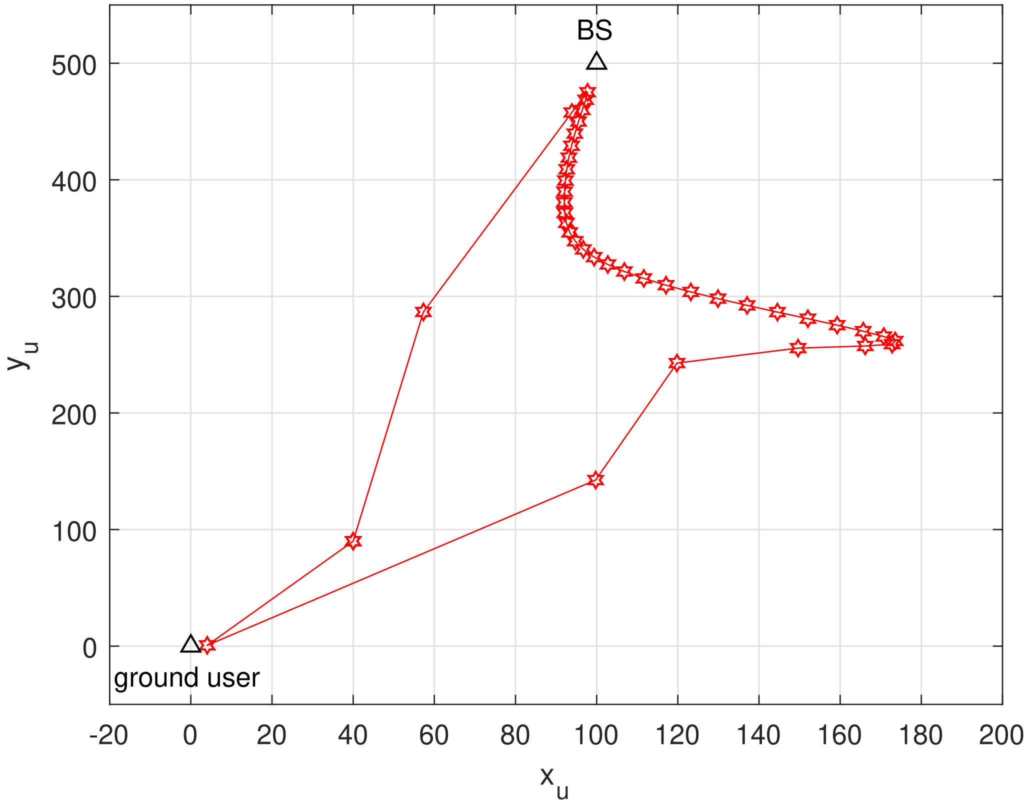

Fig. 5.1: The UAV-MR robust trajectory design.

a safe distance from the location of the eavesdropper. The location of the eavesdropper is considered $(-400, 0)$ to design the trajectory path. Eventually, when the UAV-MR flight time increases, the proposed algorithm 1 is proved efficient. For the proposed algorithm, the UAV-MR flies towards the ground user while keeping a safe distance from the eavesdropper. Eventually, the UAV-MR reaches the peak point near to the ground user. Thus, the proposed algorithm 1 efficiently adjusts the UAV-MR hovering from the eavesdropper.

5.2 The Achievable Secrecy Rate vs the UAV-MR Flight Time

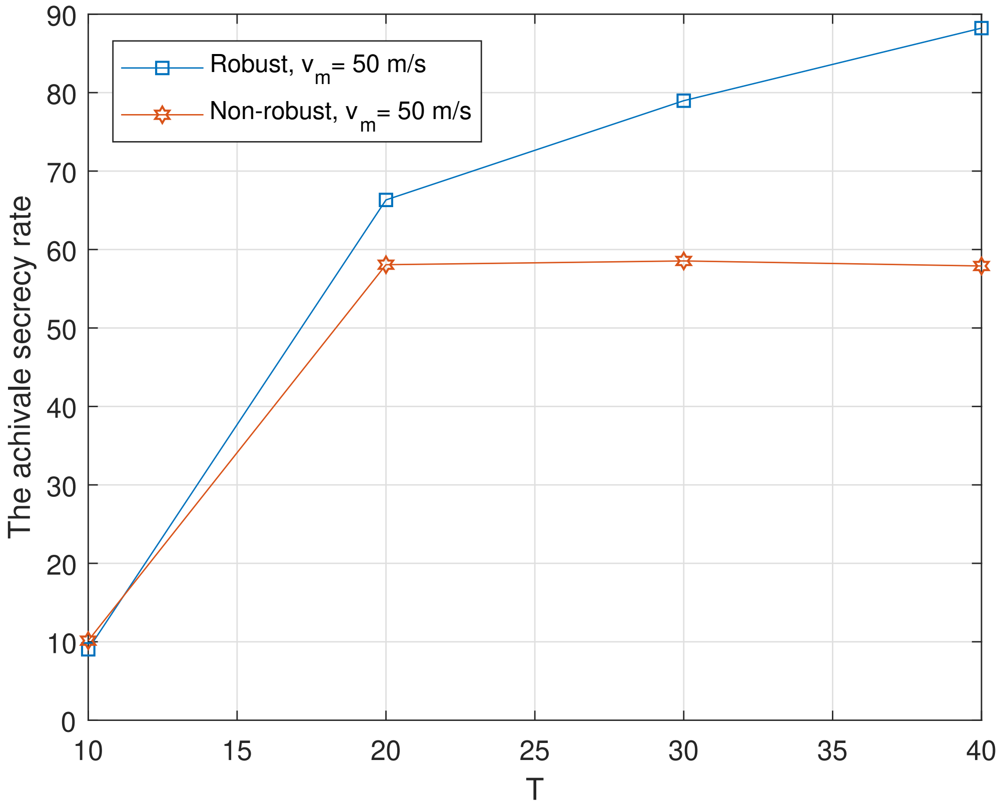

Fig. 5.2: The achievable secrecy rate at UAV-MR velocity.

The achievable secrecy rate is achieved for the UAV-MR velocity versus the UAV-MR flight time in Fig. 5.2 for both robust and non-robust scheme. For robust scheme, it is observed that the UAV-MR achieves the improved secrecy rate when the UAV-MR velocity is $v_m = 50$ m/s. On the other hand, the non-robust scheme does not guarantee improved performance compared to the robust scheme, when the UAV-MR speed is the same. Finally, the achievable secrecy rate is improved for the higher UAV-MR flight time,

T, for the proposed algorithm 1. On the other hand, the non-robust achievable secrecy rate becomes stable after a specific UAV-MR flight time. Thus, the achievable secrecy rate is significantly improved for the proposed algorithm 1, compared to the non-robust approach.

5.3 The Achievable Secrecy Rate for Different Eavesdropper Circular Regions

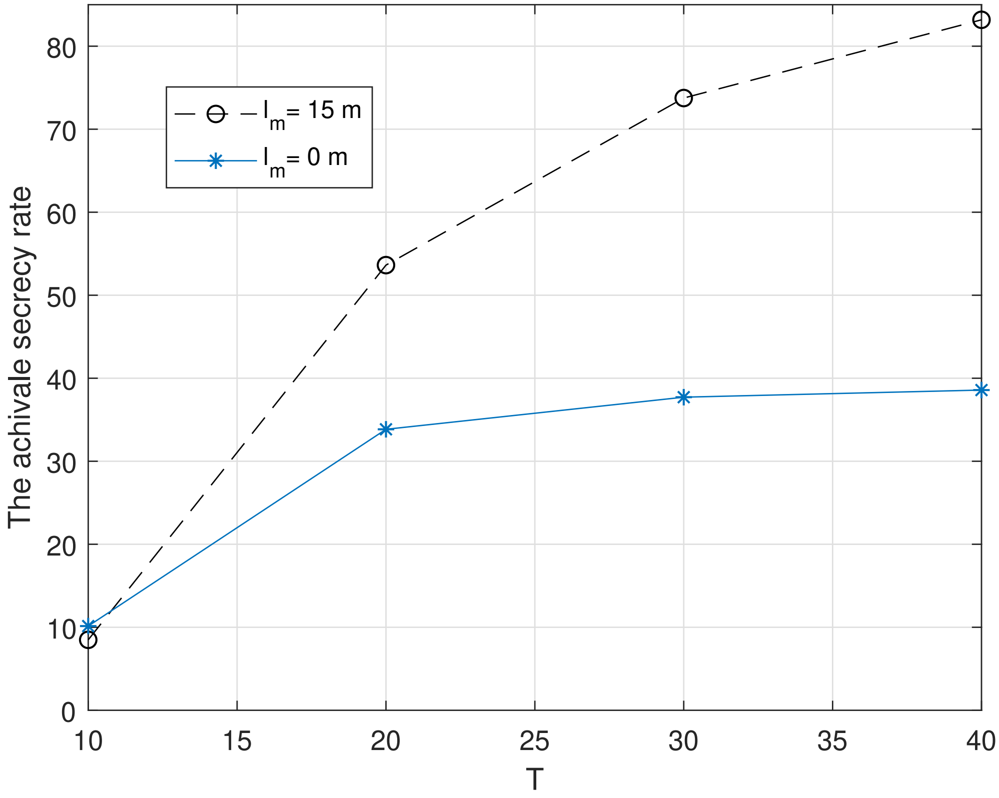

Fig. 5.3: The achievable secrecy rate for the circular regions of the eavesdroppers.

Fig. 5.3 shows the achievable secrecy rate for the proposed algorithm 1, when the circular region of the eavesdropper's location is 15 m. Then, this is compared with the non-robust scheme, meaning the UAV-MR considers the approximated location of the eavesdropper as the exact location, $i.e., l_m = 0$ As shown in Fig. 5.3, the higher secrecy rate for the proposed algorithm 1 is achieved for the circular region of the eavesdropper, which makes the proposed algorithm 1 efficient. On the other hand, the achievable secrecy rate significantly decreases when there is no circular region for the eavesdroppers to tract its location.

5.4 The Achievable Secrecy Rate vs the UAV-MR Average Power

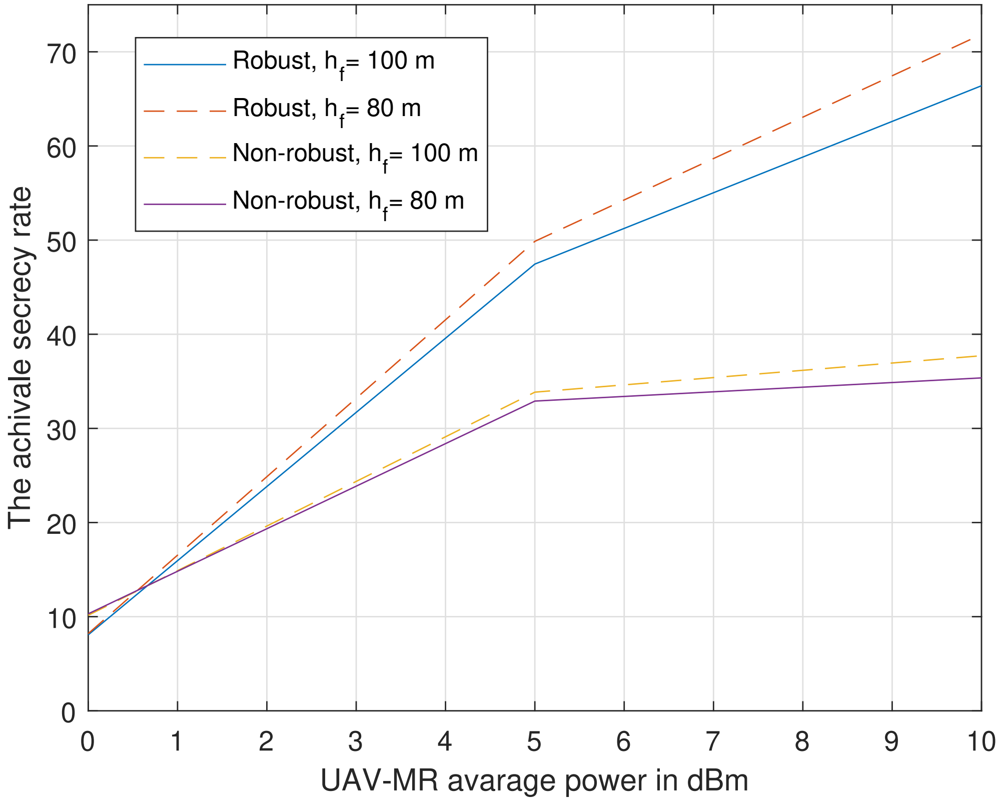

Fig. 5.4: The achievable secrecy rate at various UAV-MR altitude vs the UAV-MR average power.

Fig. 5.4 describes the achievable secrecy rate both for the proposed algorithm 1 and the non-robust scheme versus the UAV-MR average power. The achievable secrecy rate increases with the increase of the UAV-MR average power, as shown in Fig. 5.4. However, comparing with the non-robust algorithm, the proposed algorithm 1 proves the improved achievable secrecy rate performance. However, both robust and non-robust algorithm, the achievable secrecy rate increases with the increment of the UAV-MR average power. The achievable secrecy rate varies because the achievable secrecy rate maximization problem (eq. 4.13) is dependent on the UAV-MR trajectory location in the high transmit power zone. From Fig. 5.4, it is also seen that the UAV-MR has the better achievable secrecy rate for the UAV-MR altitude, 80 m, for the proposed algorithm 1. Thus, when the UAV-MR altitude is 80 m, the proposed algorithm 1 has the best performance.

CHAPTER 6
CONCLUSIONS AND DISCUSSIONS

This chapter summarizes the contribution of this investigation so that the readers can get the idea of the contribution and challenges of the proposed UAV-MR physical layer security via joint robust resource allocation. The main idea of the proposed system model is described as follows:

The UAV-MR based next-generation wireless networks is considered via robust joint UAV-MR trajectory location, and transmit power of the UAV-MR and the BS optimization. Moreover, the system considers the active presence of multiple eavesdroppers in the network. Though the UAV-MR knows the actual location of the BS and the ground user, the actual locations of eavesdroppers are unknown to the UAV-MR. The UAV-MR only knows the circular region, where the eavesdroppers are located. The information causality constraint is also considered in the system, which allows the UAV-MR to forward only received secure information from the BS to the ground user. Finally, the proposed model aims to maximize the achievable secrecy rate.

The thesis discusses the prospect and challenges of the UAV-MR based next-generation wireless networks as follows. The literature review, along with the UAV-MR description, has been studied in the Chapter 1. Chapter 1 covers the related, and recent research conducted in the field of physical layer security.

Chapter 2 focuses on the overview of the proposed UAV-MR robust resource allocation to secure the physical layer of next-generation wireless networks. Chapter 2 has a detailed explanation of the various parameters, such as LOS communication links, etc. Moreover, the advantages of UAV-MR over the UAV-SR is discussed. Moreover, how the unknown presence of multiple eavesdroppers affects the overall system performance, is discussed. The 3D location of the UAV-MR, the BS, and the ground user are also illustrated in the chapter.

The summary of Chapter 3 is described as follows. The problem formulation is discussed in detail. This chapter formulates the BS to UAV-MR achievable data rate, considering the channel power gain based on reference distance $d_o = 1$ m. Though the UAV-MR is changing its location with time, the BS has a fixed location on the ground. However, the channel gain between the UAV-MR and the BS is calculated prior data rate formulation. Moreover, the average and maximum BS transmit power constraints are considered while formulating the BS to UAV-MR data rate. After that, the UAV-MR to ground user achievable channel gain is calculated before the UAV-MR to ground user data rate calculation. The data rate is calculated based on LOS communication link. Moreover, the average and maximum UAV-MR transmit power constraint to also considered, which is also essential to tackle the achievable secrecy rate optimization problem.

However, the active presence of eavesdroppers may degrade overall system performance. Thus, this chapter also considers the UAV-MR-eavesdroppers achievable data rate. While calculating the UAV-MR-eavesdroppers achievable data rate, the data rate is maximized based on the unknown locations of eavesdroppers.

The main idea of Chapter 4 is described as follows. This chapter mainly focuses on the formulating the achievable secrecy rate maximization problem. However, the optimization problem is not tractable due to its non-convexity, and the infinite number of possible errors of finding the actual locations of eavesdroppers. This chapter also proposes a step by step process to solve the complex achievable secrecy rate maximization problem. Firstly, the discrete linear state space is applied to the optimization problem. However, it is still challenging to tackle the optimization problem due to the non-smoothness of the objective function. Thus, the non-smoothness of the objective function is tackled. Moreover, Chapter 4 solves the optimization problem sub-optimally, such as the sub-optimal solution of the UAV-MR and the BS transmit power under the given UAV-MR trajectory location, and the sub-optimal solution of the UAV-MR trajectory location under the optimal UAV-MR and the BS transmit power.

Firstly, the sub-optimal UAV-MR and the BS transmit power is achieved under given the optimal UAV-MR trajectory location, using the dual Lagrangian variables and standard Karush-Kuhn-Tucker conditions (KKT) conditions.

Secondly, the sub-optimal UAV-MR trajectory location is solved as follows. Slack variables are introduced to tackle non-convexity of the objective function and the infinite number of possible error in eavesdroppers actual locations. Moreover, this infinite number of possible error in eavesdroppers actual locations are transformed into a new formulation based on $\mathcal{S}$-*Procedure*. Finally, based on Taylor expression, the optimization problem is solved, and the sub-optimal solution of the UAV-MR trajectory location is achieved.

At the end of Chapter 4, an efficient algorithm is proposed, which solves the achievable secrecy rate maximization problem iteratively and alternatively.

Chapter 5 provides the simulation results, and compares the proposed achievable secrecy rate maximization problem, with some backbench methods, such as joint robust resource allocation.

REFERENCES

[1] Eyes of the army US: Army roadmap for unmanned aircraft system 2010-2035, *US. Army UAS Center of Excellence (ATZQ-CDI-C)*, Alabama.

[2] A. Watts 1, V. Ambrosia, and E. Hinkley, "Unmanned aircraft systems in remote sensing and scientific research: Classification and considerations of use," *Remote Sensing*, vol. 4, no. 6, pp. 1671-1692, June 2012.

[3] https://en.wikipedia.org/wiki/High-altitude_platform_station

[4] Y. Zeng. 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.

[5] M. Mozaffari1, W. Saad, M. Bennis, Y. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Communications Surveys & Tutorials*, March 2019.

[6] *Paving the Path to 5G: Optimizing Commercial LTE networks for drone communication.* Accessed: January 2018. [Online]. Available: https://www.qualcomm.com/news/onq/2016/09/06/paving-path-5goptimizing-commercial-lte-networks-drone-communication

[7] *Ericsson and china mobile conduct world's first 5G drone prototype field trial.* Accessed: January 2018. [Online]. Available: https://www.ericsson.com/en/news/2016/8/ericsson-and-china-mobileconduct-worlds-first-5g-drone-prototype-field-trial

[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, June 2015.

[9] J. Lyu, Y. Zeng, R. Zhang, and T. J. Lim, "Placement optimization of UAV-mounted mobile base stations," *IEEE Communication Letters*, vol. 21, no. 3, pp. 604-607, March 2017.

[10] V. Sharma, M. Bennis, and R. Kumar, "UAV-assisted heterogeneous networks for capacity enhancement," *IEEE Communication Letters*, vol. 20, no. 6, pp. 1207-1210, June 2016

[11] Q. Wu, J. Xu, and R. Zhang, "Capacity characterization of UAV-enabled two-user broadcast channel," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 9, pp. 1955-1971, September 2018.

[12] T. A. Johansen, A. Zolich, T. Hansen, and A. J. Sorensen, "Unmanned aerial vehicle as communication relay for autonomous underwater vehicle-field tests," *in Proc. IEEE Globecom Workshops (GC Wkshps)*, pp. 1469-1474, December 2014.

[13] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470-2492, June 2008.

[14] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Mobile unmanned aerial vehicles (UAVs) for energy-efficient internet of things communications," *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7574-7589, November 2017.

[15] J. How, Y. Kuwata, and E. King, "Flight demonstrations of cooperative control for UAV teams," *in AIAA 3rd Unmanned Unlimited Technical Conference, Workshop and Exhibit*, 2004, pp. 6490.

[16] J. Tisdale, Z. Kim, and J. K. Hedrick, "Autonomous UAV path planning and estimation," *IEEE Robotics Automation Magazine*, vol. 16, no. 2, pp. 35-42, June 2009.

[17] P. Chandler, S. Rasmussen, and M. Pachter, "UAV cooperative path planning," *in AIAA Guidance, Navigation, and Control Conference and Exhibit*, 2000, pp. 4370.

[18] C. D. Franco and G. Buttazzo, "Energy-aware coverage path planning of UAVs," *in Proc. of IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC)*, pp. 111-117, April 2015.

[19] E. I. Grøtli and T. A. Johansen, "Path planning for UAVs under communication constraints using splat and milp," *Journal of Intelligent & Robotic Systems*, vol. 65, no. 1-4, pp. 265- 282, 2012.

[20] Q. Wu, Y. Zeng, and R. Zhang, "Joint trajectory and communication design for UAV enabled multiple access," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 2109-2121, March 2018.

[21] G. Zhang, X. Li, M. Cui, G. Li, and L. Yang, "Signal and artificial noise beamforming for secure simultaneous wireless information and power transfer multiple-input multiple-output relaying systems," *IET Communications*, vol. 10, no. 7, pp. 796-804, May 2016.

[22] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, "Wireless powered cooperative jamming for secure OFDM system," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1331-1346, February 2018.

[23] F. Jiang and A. L. Swindlehurst, "Optimization of UAV heading for the ground-to-air uplink," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 5, pp. 993-1005, June 2012.

[24] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687-4698, October 2008.

[25] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 693-702, September 2011.

[26] J. Tang, H. Wen, L. Hu, H. Song, G. Zhang, F. Pan, and H. Liang, "Associating MIMO beamforming with security codes to achieve unconditional communication security," *IET Communications*, vol. 10, no. 12, pp. 1522-1531, August 2016.

[27] J. Tang, M. Dabaghchian, K. Zeng, and H. Wen, "Impact of mobility on physical layer security over wireless fading channels," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 7849-7864, December 2018.

[28] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 180-190, January 2016.

[29] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - Part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515-5532, November 2010.

[30] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5103-5113, December 2013.

[31] G. Zheng, L. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317-1322, March 2011.

[32] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, October 1975

[33] M. Cui, G. Zhang, Q. Wu, and D. Ng, "Robust trajectory and transmit power design for secure UAV communications," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 9042-9046, May 2018.

[34] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled moving relaying," *IEEE Communication Letter*, vol. 6, no. 3, pp. 310-313, June 2017.

[35] G. Zhang, H. Yan, Y. Zeng, M. Cui, and Y. Liu, "Trajectory optimization and power allocation for multi-hop UAV relaying communications," *IEEE Access*, vol. 6, pp. 48566-48576, August 2018.

[36] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1123-1152, November 2015.

[37] J. Laneman, D. Tse, and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062-3080, December 2004.

[38] Y. Zhao, R. Adve, and T. J. Lim, "Improving amplify-and-forward relay networks: Optimal power allocation versus selection," *IEEE Transactions on Wireless Communications*, vol. 6, no. 8, pp. 3114-3123, August 2007.

[39] Y. Hong, W. Huang, F. Chiu, and C. Luo, "Cooperative communications in resource-constrained wireless networks," *IEEE Signal Processing Magazine*, vol. 24, no. 3, pp. 47-57, May 2007.

[40] M. Thakur, N. Fawaz, and M. Mdard, "Optimal relay location and power allocation for low SNR broadcast relay channels," *International Conference on Computer Communications and Networks (INFOCOM)*, Shanghai, China, pp. 2822-2830, April 2011.

[41] Y. Zeng, R. Zhang, and T. Lim, "Throughput maximization for UAV enabled mobile relaying systems," *IEEE Transactions on Wireless Communications*, vol. 64, no. 12, pp. 4983-4996, December 2016.

[42] A. Gawanmeh and A. Alomari. "Taxonomy analysis of security aspects in cyber-physical systems applications," *IEEE Proceedings of International Conference on Communications (ICC) Workshop*, May 2018.

[43] X. Lin, V. Yajnanarayana, S. Muruganathan, S. Gao, H. Asplund, H. Maattanen, M. Bergstrm, S. Euler, and Y. Wang, "The sky is not the limit: LTE for unmanned aerial vehicles," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 204-210, April 2018.

[44] A. Merwaday and I. Guvenc, "UAV assisted heterogeneous networks for public safety communications," *in Proc. IEEE Wireless Communications & Networking Conference (WCNC)*, March 2015, pp. 329-334

[45] E. Frew and T. Brown, "Airborne communication networks for small unmanned aircraft systems," *Proceedings of the IEEE*, vol. 96, no. 12, pp. 2008-2027, December 2008.

[46] W. Guo, S. Zhou, Y. Chen, S. Wang, X. Chu, and Z. Niu, "Simultaneous information and energy flow for IoT relay systems with crowd harvesting," *IEEE Communications Magazine*, vol. 54, no. 11, pp. 143-149, September 2016.

[47] U. Mengali and A. N. D'Andrea, "Synchronization techniques for digital receivers," New York, NY, USA: Springer, 1997.

[48] I. Yaliniz, A. El-Keyi, and H. Yanikomeroglu, "Efficient 3-D placement of an aerial base station in next generation cellular networks," *IEEE Proceedings of International Conference on Communications (ICC)*, pp. 1-5, July 2016.

[49] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski, "Information causality as a physical principle," *Nature*, vol. 461, no. 7267, pp. 1101-1104, October 2009.

[50] G. Zhang, Q. Wu, M. Cui, and Rui Zhang, "Securing UAV communications via joint trajectory and power control," *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, pp. 1376-1389, January 2019.

[51] A. Li, Q. Wu, and R. Zhang, "UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 181-184, February 2019.

[52] D. Goeckel, A. Sheikholeslami, T. Sobers, B. Bash, D. Towsley, and S. Guha, "Covert communications in a dynamic interference environment," *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Kalamata, Greece, June 2018.

[53] S. Boyd and L. Vandenberghe, *Convex optimization*, Cambridge, U.K.: Cambridge University Press, 2004.

[54] F. Uhlig, "A recurring theorem about pairs of quadratic forms and extensions: A survey, linear algebra, and its applications," *Linear Algebra and its Applications*, vol. 25, pp. 219-237, 1979.

[55] I. Polik and T. Terlaky, "A Survey of the S-Lemma," *SIAM Review*, vol. 49, pp. 371-418, 2007.

[56] A. Forsgren, P. Gill, and H. Wright, "Interior methods for nonlinear optimization," *SIAM Review*, vol. 44, pp. 525-597, 2002.

[57] N. Karmarkar, "A new polynomial-time algorithm for linear programming," *Combinatorica*, pp. 373-395, 1984.

[58] J. Lustig, E. Marsten, and F. Shanno, "Computational experience with a primal-dual interior point method for linear programming," *Linear Algebra and Its Applications* vol. 152, pp. 191-222, 1991.

[59] S. Mehrotra, "On the implementation of a primal-dual interior point method," *SIAM Journal on Applied Mathematics*, pp. 575-601, July 2006.

[60] A. Gil, J. Segura, M. Temme, "Numerical methods for special functions," *Society for Industrial and Applied Mathematics*, vol. 99, 2007.

[61] K. Anstreicher, "Ellipsoidal approximations of convex sets based on the volumetric barrier," *Mathematics of Operations Research*, vol. 24, no. 1, pp. 1-272, 1999.

APPENDICES

APPENDIX A

Non-smoothness of Objective Function

The optimal solution of both eq. 4.13a and eq. 4.14a is proved to be equal, meaning eq. 4.13a and eq. 4.14a share the same optimal solution.

The $\mathcal{X}_a^*$ is defined as the optimal value of eq. 4.13a, and the $\mathcal{X}_b^*$ is the optimal value of eq. 4.14a.

As $[.] \leq [.]^+$, $\forall .$, then it can be written as

$$\mathcal{X}_b^* \leq \mathcal{X}_a^*. \tag{A.1}$$

However, $(x_u^*, y_u^*, p_b^*, p_u^*)$ define the optimal solutions to eq. 4.13a. The expression of p_b^*, p_u^* can be written as follows

$$p_b^* = \{p^*[1], p^*[2], ..., p^*[N{-}1]\}, \tag{A.2}$$

$$p_u^* = \{p^*[2], p^*[3], ..., p^*[N]\}. \tag{A.3}$$

Now let $f(p_u[n]) = r_s$. The feasible solution of eq. 4.14a can be expressed as follows

$$p_b^* = \{p^*[1], p^*[2], ..., p^*[N{-}1]\}, \tag{A.4}$$

$$p_u^* = \{p^*[2], p^*[3], ..., p^*[N]\}. \tag{A.5}$$

Let the objective values of eq. 4.14a attain at $(x_{u*}, y_{u*}, p_{b*}, p_{u*})$ as $\mathcal{X}_*$. The newly constructed solution $(x_{u*}, y_{u*}, p_{b*}, p_{u*})$ ensures that $\mathcal{X}_*{=}\mathcal{X}_a^*$.

Since $(x_{u*}, y_{u*}, p_{b*}, p_{u*})$ is feasible to eq. 4.14a, it follows that $\mathcal{X}_* \leq \mathcal{X}_b^*$ and $\mathcal{X}_b^* \geq \mathcal{X}_a^*$. Finally, $\mathcal{X}_a^* = \mathcal{X}_b^*$.

Thus, the proof is complete.

APPENDIX B

Sub-optimal Solution of the UAV-MR and the BS Transmit Power

It is clear that $p_b[n]$ and $p_b[n]$ have the optimal solution, which can be illustrated as the form of liquid filling. However, $p_b[n]$ and $p_b[n]$ have different characteristics, which are equivalent to different liquid levels. Technically, the power allocation of the base station, p_b and UAV-MR, p_u can be considered as staircase liquid filling over the slots. The power allocation of the BS and the UAV-MR is possible due to the non-negative and non-increasing parameter, $\flat$.

However, due to the presence of eavesdroppers, the UAV-MR liquid level does not always monotone over the UAV-MR flight period. Now, the dual optimal variable λ_n that minimizes the Lagrange dual function needs to be found. The ellipsoid method [61] can be applied to tackle the Lagrange duality. The following constraints can minimize the function.

$$\sum_{n=2}^{N} \lambda_n \leq 1, n = 2, 3, 4, ..., N, \tag{B.1}$$

$$\lambda_n \geq 0, n = 2, 3, 4, ..., N, \tag{B.2}$$

where λ_n is the Lagrange dual variable. Using the above process and methods, the achievable secrecy maximization problem can be tackled. However, $p_u[n]$ needs to be updated iteratively while solving the achievable secrecy rate maximization problem. This is summarized in algorithm 1.

The optimal solution of the UAV-MR transmit power, and the BS transmit power can be proved in the following way as well.

In the optimization problem 4.24, the information-causality constraint in eq. 4.23 is coupled with the UAV-MR, and the BS transmit power. Thus, it is essential to decouple them, which can be done by using the partial Lagrangian method. The partial Lagrangian is the function of $L(p_u, p_b, \Gamma, \lambda_n)$. $L(p_u, p_b, \Gamma, \lambda_n)$ can be expressed as follows

$$\begin{aligned}
L(p_u, p_b, \Gamma, \lambda_n) &= \sum_{n=2}^{N} \left[\Gamma[n] - \log_2 \left(1 + \frac{p_u^f[n] c_{ue}^{new}[n]}{\sigma^2} \right) - \frac{c_{ue}^{new}[n](p_u^f[n] - p_u[n])}{(\sigma^2 + p_u^f[n] c_{ue}^{new}[n])} \right] \\
&+ \sum_{n=2}^{N} \left[\lambda_n \Bigg(\sum_{j=1}^{n-1} \log_2 \left(1 + \frac{p_b[n] c_{bu}[n]}{\sigma^2} \right) - \sum_{j=2}^{n} \Gamma[j] \Bigg) \right] \\
&= \sum_{n=2}^{N} \left[\Bigg(1 - \sum_{j=n}^{N} \lambda_j \Bigg) \Gamma[n] - \sum_{n=2}^{N} \left(\log_2 \left(1 + \frac{p_u^f[n] c_{ue}^{new}[n]}{\sigma^2} \right) + \frac{c_{ue}^{new}[n](p_u^f[n] - p_u[n])}{(\sigma^2 + p_u^f[n] c_{ue}^{new}[n])} \right) \right] \\
&+ \sum_{n=1}^{N-1} \left[\Bigg(\sum_{n=1}^{N} \lambda_j \Bigg) \log_2 \left(1 + \frac{p_b[n] c_{bu}[n]}{\sigma^2} \right) \right].
\end{aligned} \tag{B.3}$$

Thus, the Lagrange dual function of eq. 4.24 can be expressed as follows

$$\max_{p_u[n], p_b[n], \Gamma[n], \lambda_n[n]} \quad L(p_u, p_b, \Gamma, \lambda_n), \tag{B.4a}$$

$$\text{s.t. } (4.23), \ (4.13d) \ - \ (4.13g),$$

where $\lambda_n \leq 0, \forall n$. In order to achieve the optimal value, this project focuses only on eq. B.4 can be maximized using eq. B.3 to achieve the dual function with fixed λ_n. Then the dual solution of λ_n^* can be found by minimizing the dual function. Finally, the optimal value of the UAV-MR transmit power, and the BS transmit power can be achieved based on λ_n^*. Thus, the minimization of Lagrange dual function over UAV-MR transmit power and BS transmit power, where λ_n is fixed, can be derived from eq. B.3.

If the function over p_b is $f_{p_b}(\lambda_n)$ and the function over p_u is $f_{p_u}(\lambda_n)$, then the following expression can be written

$$f(\lambda_n) = f_{p_u}(\lambda_n) + f_{p_b}(\lambda_n), \tag{B.5}$$

where

$$f_{p_u}(\lambda_n) = \max_{p_u[n],\Gamma[n]} \sum_{n=2}^{N} \left[\Gamma[n] - \log_2 \left(1 + \frac{p_u^f[n] c_{ue}^{new}[n]}{\sigma^2} \right) - \frac{c_{ue}^{new}[n](p_u^f[n] - p_u[n])}{(\sigma^2 + p_u^f[n] c_{ue}^{new}[n])} \right], \tag{B.6a}$$

s.t. $(4.13f) \ - \ (4.13g)$.

and

$$f_{p_b}(\lambda_n) = \max_{p_b[n]} \sum_{n=1}^{N-1} \left[\left(\sum_{n=1}^{N} \lambda_j \right) \log_2 \left(1 + \frac{p_b[n] c_{bu}[n]}{\sigma^2} \right) \right], \tag{B.7a}$$

s.t. $(4.13d) \ - \ (4.13e)$.

Thus, in order to obtain the sub-optimal solution of the UAV-MR transmit power, p_u and the BS transmit power, p_b, eq. B.6 and eq. B.7, respectively, need to be solved. However, it is assumed that Lagrange dual variable, λ_n is given while solving those eq. B.6 and eq. B.7. Thus, by applying the standard KKT conditions, the optimal solution of the UAV-MR transmit power, p_u, and the BS transmit power p_b can be achieved.

Thus, the proof is complete.

APPENDIX C

Sub-optimal Solution of the Shared UAV-MR Trajectory Design

In both problems, followings are active.

$$x_u^2[n] + y_u^2[n] + h_f^2 - u[n] \leq 0, \tag{C.1}$$

$$\min_{(\triangle x_m, \triangle y_m) \in \varepsilon_m} (x_u[n] - x_m^a)^2 + (y_u[n] - y_m^a)^2 + h_f^2 \geq z[n]. \tag{C.2}$$

The contradiction theory can prove the sub-optimal solution of eq. 4.14 and eq. 4.31 is equivalent, meaning they share the same sub-optimal solution.

Let both eq. C.1 and eq. C.2 are not active. Due to their inactivity, the objective function of eq. 4.31, which is $\sum_{n=2}^{N} \left[\Gamma[n] - \log_2\left(1 + \frac{p_u^n}{z[n]}\right)\right]$, can be improved with the increment of $z[n]$.

Thus, the proof is complete.

APPENDIX D

$\mathcal{S}$-*Procedure*

$\mathcal{S}$-*Procedure* defines a mathematical result, which tackles the non-negative quadratic form under quadratic inequalities [53] - [55]. Let A and B; a and b; w_1 and w_2; and δ are the symmetric matrices, vectors, and real numbers, non-negative number, respectively. The inequality holds if and only if there exists n_0 such that the following inequality holds

$$n_0^T A n_0 + 2a^T n_0 + w_1 \leq 0, \tag{D.1}$$

Fianlly, the implication can be expressed as

$$n_1^T A n_1 + 2a^T n_0 + w_1 \leq 0, \tag{D.2}$$

$$n_2^T A n_2 + 2a^T n_0 + w_2 \leq 0, \tag{D.3}$$

Eqs. D.2 - D.3 holds the following such that it is positive semidefinite

$$\varepsilon \begin{bmatrix} A & a \\ a^T & w_1 \end{bmatrix} - \begin{bmatrix} B & b \\ b^T & w_2 \end{bmatrix}.$$

where ε is a non-negative number.

APPENDIX E

Interior Point Method (IPM)

An interior point method (IPM) is a non-linear programming [56–59], which can solve the non-linear optimization problem. Mathematically, it can be expressed as follows.

$$\min g(x), \tag{E.1a}$$

$$\text{s.t. } d^j \geq 0. \tag{E.1b}$$

where eq. E.1a is a non-linear objective function, having the constraint in eq. E.1b. Moreover, j is defined as $j = 1, 2, 3, ..., n$. A barrier function can be introduced as

$$g(x) = b^f(x, y) + y \sum_{j=1}^{n} \log(d^j(x)). \tag{E.2}$$

Eq. E.2 converges to the solution of eq. E.1a. y is defined as barrier parameter, which also converges to 0. The barrier function gradient can be expressed as

$$f - f^* = y \sum_{j=1}^{n} \frac{\triangle d^j(x)}{d^j(x)}. \tag{E.3}$$

Using the eq, E.3, it can proved that f is the gradient of $g(x)$. Now, a dual variable is introduced as follows.

$$\lambda \in \mathbb{R}^m, \tag{E.4}$$

$$\lambda_j = \frac{y}{d^j}. \tag{E.5}$$

Eq. E.4 can be refereed as complementary slackness in KKT conditions. Using the eq. E.3 - E.5, the follwing matrix can be achieved

$$W^T = \frac{f}{\lambda}. \tag{E.6}$$

where W is a matrix. The following expression can be achieved using the Newton method [60], which can update (u, v) for (x, λ) as follows

$$\begin{bmatrix} Au & -W^T u \\ BWu & Dv \end{bmatrix} = \begin{bmatrix} -f & -W^T \lambda \\ y & -Dy \end{bmatrix}. \tag{E.7}$$

D and B are the diagonal matrices of λ and d^j, respectively. Moreover, in eq. E.7, λ must be greater or equal than zero, which can be proved using the eq. E.5.