



Physical layer security (PLS) solutions for passive eavesdropping in wireless communication

Christantus Obinna NNAMANI

A thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy (PhD)

Institute of Signals, Sensors and Systems,

School of Engineering and Physical Sciences

September 2022

The copyright in this thesis is owned by the author. Any quotation from the thesis or use of any of the information contained in it must acknowledge this thesis as the source of the quotation or information.

Abstract

An absolute secured wireless communication is unattainable. Nevertheless, communication models must be secure and unique across each layer of the model. The physical layer is the easiest layer through which information leaks, due to its broadcast nature. The security in the physical layer, measured as secrecy capacity, is subdivided into keyed and keyless security models. In practice, the eavesdropper's evasive and obscure random wireless channel model makes it difficult to optimise keyless security measure at the physical layer. Considering this practical challenge, the objective of this work is to use novel keyless approaches to reduce the ability of an illegitimate user to access the transmitted message via the physical layer. Physical layer security (PLS) was achieved through the deployment of unmanned aerial vehicles (UAV), intelligent reflecting surfaces (IRS), and communication sensing as security enablers in this thesis. The UAV operates with interfering signals while the IRS and sensing techniques optimise respective inherent properties leading to higher PLS performance. The thesis presents solutions to the parametric design of UAV, IRS, and wireless sensing technologies for PLS functionality. Designs and analysis herein follow from analytical derivations and numerical simulations. Specifically, the thesis presents a novel average secrecy rate formulation for passive eavesdropping with a reception rate upper bound by that of the legitimate receiver. The keyless PLS assessed from the formulations guaranteed positive rates with the design of a broadcast interfering signal delivered from a UAV. Based on the verification of the positive secrecy rate with passive eavesdropping, a swarm of UAVs improved the PLS of the communication system delivering more interfering signals. Furthermore, the functionalities of the interference driven UAV swarm were miniaturised with a system of aerial IRS. By harnessing inherent channel dynamics, a novel non-iterative design of the aerial IRS system was presented as a panacea to PLS requirements. Finally, the thesis presents the analysis of a legitimate receiver with a novel noise and interference filter as a sensing mitigation technique. The filter enhanced PLS by enabling the legitimate receiver to effectively extract desired information.

To
Mary, Mother of God and
my family (Chioma, Chimeremeze and Chidiuto) for their
undying love and support.

Acknowledgements

I express my sincere gratitude to my supervisors Prof. Mathini SELLATHURAI and Dr. Muhammad KHANDAKER for their enormous role and contributions to this work. Succinctly, this work reflects their dedication and availability at all the stages of the programme.

Furthermore, I am grateful to the Petroleum Technology Development Fund (PTDF), Nigeria for financially sponsoring me through this programme. Noteworthy also is the Department of Electronic Engineering, University of Nigeria Nsukka for encouraging me to study without stress.

With joy, I thank my research colleagues at the EM3.31 office, Heriot-Watt University Edinburgh, especially Dr Papageorgiou George, Dr Christie Etukudor and Dr Shoukry Hebatallah for helping me adapt to University and its environs. In addition to working from Heriot-Watt University, I had spent some time working from the University of Edinburgh and the University of Strathclyde libraries. I am indebted to the UK SCONUL access scheme that granted me access to these libraries.

Finally, the gain of this work is a reflection of the undying love and support from my family. My impeccable wife, Dr Chioma and my little smiling children (Chimeremeze and Chidiuto) are the victories of this work. I appreciate God for my parents, HRH Igwe Christopher and Lolo Calister Nnamani, whose love for education kept me at the University. My siblings and in-laws were also supportive throughout this journey. I am nothing without you, my family and friends. The list can go on but I must stop. Thank you all.

Declaration statement

Research Thesis Submission

Please note this form should be bound into the submitted thesis.

Name:	Christantus Obinna NNAMANI		
School:	School of Engineering and Physical Sciences		
Version: (<i>i.e.</i> First, Resubmission, Final)	Final	Degree Sought:	PhD

Declaration

In accordance with the appropriate regulations, I hereby submit my thesis and I declare that:

1. The thesis embodies the results of my own work and has been composed by myself
2. Where appropriate, I have made acknowledgement of the work of others
3. The thesis is the correct version for submission and is the same version as any electronic versions submitted*.
4. My thesis for the award referred to, deposited in the Heriot-Watt University Library, should be made available for loan or photocopying and be available via the Institutional Repository, subject to such conditions as the Librarian may require
5. I understand that as a student of the University I am required to abide by the Regulations of the University and to conform to its discipline.
6. I confirm that the thesis has been verified against plagiarism via an approved plagiarism detection application e.g. Turnitin.

Declaration statement

ONLY for submissions including published works

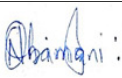
Please note you are only required to complete the Inclusion of Published Works Form (page 2) if your thesis contains published works)

7. Where the thesis contains published outputs under Regulation 6 (9.1.2) or Regulation 43 (9) these are accompanied by a critical review which accurately describes my contribution to the research and, for multi-author outputs, a signed declaration indicating the contribution of each author (complete)
8. Inclusion of published outputs under Regulation 6 (9.1.2) or Regulation 43 (9) shall not constitute plagiarism.

* Please note that it is the responsibility of the candidate to ensure that the correct version of the thesis is submitted.

Signature of Candidate:		Date:	27 - 9 - 2022
-------------------------	---	-------	---------------

Submission

Submitted By (<i>name in capitals</i>):	CHRISTANTUS OBINNA NNAMANI
Signature of Individual Submitting:	
Date Submitted:	27 - 9 - 2022

For Completion in the Student Service Centre (SSC)

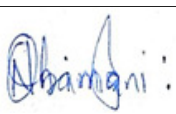
Limited Access	Requested	Yes		No		Approved	Yes		No	
<i>E-thesis Submitted (mandatory for final theses)</i>										
Received in the SSC by (<i>name in capitals</i>):						Date:				

Inclusion of Published Works


Please note you are only required to complete the Inclusion of Published Works Form if your thesis contains published works under Regulation 6 (9.1.2)


Declaration

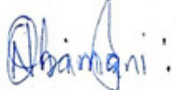
This thesis contains one or more multi-author published works. In accordance with Regulation 6 (9.1.2) I hereby declare that the contributions of each author to these publications is as follows:

Citation details	Christantus O. Nnamani , M. R. A. Khandaker, and M. Sellathurai, "UAV-aided jamming for secure ground communication with unknown eavesdropper location," <i>IEEE Access</i> , vol. 8, pp. 72 881–72 892, Apr. 2020
Christantus O. Nnamani	Generated the main idea of the work, solved the equations, carried out the simulations and wrote the published work.
M. R. A. Khandaker	Reviewed the published work.
M. Sellathurai	Reviewed the published work.
Signature:	
Date:	27 - 9 - 2022

Declaration statement

Citation details	Nnamani, Christantus O. , M. R. Khandaker, and M. Sellathurai, "Secrecy rate maximization with grid-ded UAV swarm jamming for passive eavesdropping," in <i>2021 IEEE Global Commun. Conf. (GLOBECOM)</i> , 2021, pp. 01–06
Christantus O. Nnamani	Generated the main idea of the work, solved the equations, carried out the simulations and wrote the published work.
M. R. A. Khandaker	Reviewed the published work.
M. Sellathurai	Reviewed the published work.
Signature:	
Date:	27 - 9 - 2022

Citation details	Christantus O. Nnamani , M. R. A. Khandaker, and M. Sellathurai, "Secure data collection via UAV-carried IRS," <i>ICT Express, Elsevier</i> , 2022, Accepted
Christantus O. Nnamani	Generated the main idea of the work, solved the equations, carried out the simulations and wrote the published work.
M. R. A. Khandaker	Reviewed the published work.
M. Sellathurai	Reviewed the published work.
Signature:	
Date:	27 - 9 - 2022

Citation details	Christantus O. Nnamani and M. Sellathurai, “Interference and noise cancellation for joint communication radar (JCR) system based on contextual information,” <i>IEEE</i> , 2022, Submitted
Christantus O. Nnamani	Generated the main idea of the work, solved the equations, carried out the simulations and wrote the published work.
M. Sellathurai	Reviewed the published work.
Signature:	
Date:	27 - 9 - 2022

Please included additional citations as required.

Contents

Abstract	i
Dedication	ii
Acknowledgements	iii
Declaration statement	iv
Contents	ix
List of Tables	xii
List of Figures	xiii
Abbreviations	xv
Symbols	xviii
Publications	xx
1 Introduction	1
1.1 Background	1
1.2 Principles of Physical Layer Security (PLS)	3
1.3 Evolution of PLS in Wireless Communication	4
1.4 Technologies Deployed for Improved PLS	9
1.4.1 Unmanned Aerial Vehicle (UAV)	9
1.4.1.1 UAV Classification	10
1.4.1.2 UAV Swarm	11
1.4.2 Intelligent Reflecting Surfaces (IRS)	12
1.4.3 Wireless Communication Sensing	12
1.5 Scenario Description	13
1.6 Thesis Outline	14
1.7 Notations	17

2	Physical Layer Security Optimisation for Passive Eavesdropping	18
2.1	Related Works	18
2.2	System Model	23
2.2.1	Problem Formulation	28
2.3	Proposed Solution	31
2.3.1	Optimising the Source Power (P_A)	31
2.3.2	Optimising the UAV Jamming Power (P_u)	32
2.3.3	Optimising the UAV Trajectory (\mathbf{Q})	34
2.3.4	Overall Procedure	35
2.4	Simulation Results and Analysis	37
2.5	Chapter Summary	47
3	Physical Layer Security Improvement with UAV Swarm	49
3.1	Existing Techniques and Discussions	49
3.2	System Model and Problem Formulation	51
3.3	Proposed Solution	56
3.3.1	Solving for Beamforming Vectors	57
3.3.2	Solving for Trajectory of the UAV Swarm	58
3.3.3	Overall Solution	61
3.4	Results and Analysis	63
3.5	Chapter Summary	70
4	Physical Layer Security with UAV-Carried IRS	71
4.1	Overview of IRS on PLS	72
4.2	System Model and Problem Formulation	75
4.3	Proposed Solution	81
4.3.1	Solving for Θ	82
4.3.1.1	Generic Model	82
4.3.1.2	Modified Approach	84
4.3.2	Solving for \mathbf{w}	87
4.3.2.1	Generic Approach	87
4.3.2.2	Modified Approach	88
4.3.3	Solving for \mathbf{Q}	88
4.3.3.1	Generic Approach	88
4.3.3.2	Modified Approach	90
4.3.4	Overall Iterative and Non-iterative Algorithm	91
4.4	Results and Discussions	93
4.5	Chapter Summary	101
5	Physical Layer Security for Joint Wireless Communications and Sensing	102
5.1	Prospects of Communication Sensing	103
5.2	Cohabiting Collaboration: A Case Study of Joint Communication and RADAR (JCR)	106

5.3	System Model of a Communication/RADAR Cohabiting Scenario . .	108
5.3.1	Case 1: No RADAR Target	110
5.3.2	Case 2: RADAR Target Present	111
5.4	Interference Mitigation	112
5.4.1	Cooperative Systems: RADAR receiver is the eavesdropper . .	112
5.4.2	Cooperative Systems: Eavesdropper is an External Node . . .	114
5.4.3	Uncooperative Systems	122
5.4.3.1	Autoencoder Formulation and Design	123
5.4.3.2	Autoencoder Input Preparation	125
5.4.3.3	Autoencoder Training and Validation Phase	126
5.4.3.4	Autoencoder Testing Phase	126
5.5	Results and Discussions	127
5.6	Chapter Summary	135
6	Conclusion and Recommendation	137
6.1	Summary	137
6.2	Recommendation	139
A	Proof of the Sum Composition from Section 2.3.1	141
B	UAV-IRS Signal to Interference Noise (SINR) Distribution	143
C	KKT Solution to P4.5 in Section 4.3.3.1	149
	References	151

List of Tables

1.1	Overview of PLS algorithms	9
1.2	Features of UAV classification	11
2.1	Simulation parameters for jamming of obscured eavesdropper	38
3.1	Parameters for simulating the UAV swarm problem	64
4.1	Parameters for UAV-carried IRS simulation	93
5.1	Parameter description of the JCR model	127

List of Figures

1.1	Shannon communication model.	5
1.2	Wyner wiretapper.	5
1.3	Gaussian version of Wyner wiretapper.	6
1.4	Wireless communication model.	8
1.5	UAV classification.	10
1.6	General thesis system model discussed.	13
2.1	UAV-aided jamming for secure communication.	23
2.2	Convergence analysis of algorithm 1.	36
2.3	Comparing transmitted power from Alice and UAV for $T = 20s$	39
2.4	Average secrecy rate with ‘unknown’ as well as ‘known’ eavesdropper locations, and direct UAV flight path.	40
2.5	UAV flight trajectory in 2D and 3D view while Eve location is unknown (For clarity, we use $\delta = 10$).	42
2.6	UAV flight trajectory as a function of time (For clarity, we use $\delta = 10$). . . .	43
2.7	Effect of average received envelop power of Eve on average secrecy rate. . . .	44
2.8	Influence of UAV altitude (height) on average secrecy rate under the proposed scheme.	45
2.9	Influence of UAV flying speed on average secrecy rate with obscure Eve.	46
2.10	Average secrecy rate versus signal-noise-ratio (SNR) with obscure Eve. . . .	47
3.1	UAV Swarm interaction with ground stations	52
3.2	Convergence analysis of algorithm 2 with $K = 9$	63
3.3	Comparative performance of the UAV Swarm on average secrecy rate when the eavesdropper location is known and unknown.	65
3.4	Effect of radius of Eve region on average secrecy.	66
3.5	Comparative performance of the average secrecy rate of the UAV Swarm and single UAV jammer for $K = 9$, $\mathbf{\Omega}_b = [200, 0, 0]^T$, $\hat{\mathbf{\Omega}}_e = [200, 150, 0]^T$, $\mathbf{q}_f = [150, 100, 100]^T$	67
3.6	Beam Pattern at $T = 600$ and $\varepsilon = 300m$	68
3.7	The UAV swarm trajectory for $T = 600s$	69
4.1	Schematic of the UAV-IRS interaction with ground nodes	75
4.2	Convergence on iterative algorithm 3	92
4.3	UAV trajectory for different locations of Eve.	94

4.4	Average secrecy versus time of flight (T) for different transmit power (dBm) for $K = 16$, $r = 1\text{m}$, $\rho_0 = 120\text{dBm}$, and $P = 1\text{dBm}$	95
4.5	Average secrecy rate versus Radius of sensor location for $K = 16$ and $T = 300\text{s}$	96
4.6	Average secrecy rate versus distance between Bob and Eve for $K = 16$, $r = 1\text{m}$, $P = 10\text{dBm}$ and $T = 300\text{s}$	97
4.7	Average secrecy rate versus transmit power for $K = 16$, $r = 1\text{m}$ and $T = 300\text{s}$	98
4.8	Influence of the number of IRS on Average secrecy rate at uncorrelated formation of Eve and Bob channel ($r = 1\text{m}$ and $P = 10\text{dBm}$, $T = 300\text{s}$).	99
5.1	MIMO Communication and RADAR cohabitation system	110
5.2	Signal architecture of the wireless communication and RADAR cohabitation systems with interaction from a passive eavesdropper . . .	115
5.3	Convergence of the sensing algorithm 5.	122
5.4	Layer interaction of the autoencoder	124
5.5	Data flow to the autoencoder	125
5.6	Average secrecy rate analysis where the only the communication and RADAR cohabiting parameters influence the beamformer.	128
5.7	Average secrecy rate analysis where an external eavesdropper and the communication and RADAR cohabiting parameters influence the beamformer.	130
5.8	Impact of the beamforming design on the RADAR receiver for $N_C = 30$	131
5.9	Impact of the beamforming design on the RADAR transmitter for $N_D = 4$	132
5.10	RMSE performance graph of test Communication signals.	133
5.11	RMSE performance graph of test RADAR reflected signals.	135

Abbreviations

1D	one dimension
2D	two dimension
3D	three dimension
5G	fifth generation
ADC	analog to digital converter
AI	artificial intelligence
AN	artificial noise
ANN	artificial neural network
AP	access point
AWGN	additive white gaussian noise
BS	base station
CDF	cummulative density function
CLT	central limit theory
CRB	cramer rao bound
CSI	channel state information
DFRC	dual-function radar communication
DoD	department of defence
DSA	dynamic spectrum allocation
FSA	fixed spectrum allocation
FW	fixed wing
G2U	ground to unmanned aerial vehicle
HAD	hybrid-analog-digital
HAP	high altitude platform

i.i.d	independent and identically distributed
IoT	internet of things
IRS	intelligent reflecting surfaces
ISM	industrial, scientific and medical
ISO	international organization for standardization
JCR	joint communication radar
KKT	karush-kuhn-tucker
KPM	key performance metric
LAP	low altitude platform
LoS	line of sight
LSE	logarithm-summation-exponential
MISO	multiple-input-single-output
MIMO	multiple-input-multiple-output
M-MIMO	massive multiple-input-multiple-output
NUCA	non-uniform circular array
NULA	non-uniform linear array
OSI	open system interconnection
P2P	peer-to-peer
PDF	probability density function
PLS	physical layer security
RADAR	radio detection and ranging
ReLU	rectified linear unit
RF	radio frequency
RMSE	root mean square error
RW	rotary wing
SCA	successive convex approximation
SDP	semi-definite programming
SIMO	single-input-multiple-output
SINR	signal to interference noise ratio
SNR	signal to noise ratio
TCP/IP	transmission control protocol/Internet protocol

U2G	unmanned aerial vehicle to ground
UAS	unmanned aircraft system
UAV	unmanned aerial vehicle
UCA	uniform circular array
ULA	uniform linear array
VANET	vehicular ad hoc networks

Symbols

P	power	W (Js^{-1})
A	legitimate transmitter (Alice)	
B	legitimate receiver (Bob)	
E	eavesdropper (Eve)	
\mathbb{E}	expected value	
C_s	secrecy capacity	bits/s
R_s	average secrecy rate	bits/s
f	transmission frequency	Hz
H	UAV altitude	m
T	UAV flight time	s
N	number of samples	
Z	UAV maximum speed	m/s
\mathbf{Q}	UAV trajectory	
\mathbf{W} and \mathbf{w}	beamforming weight matrix and vector	
ω_c	angular carrier frequency	rads^{-1}
γ	signal to noise ratio	
λ	wavelength	m
$\boldsymbol{\Omega}$	Location in the $\{x, y, z\}$ directions	m
ρ_0	power at reference distance of 1m	W (Js^{-1})
$\boldsymbol{\Theta}$	matrix of reflection coefficients	
θ	signal arrival/departure angle	rad
ϵ	acceptable convergence error	

Symbols

ψ	ground pathloss
ζ	exponential random variable with unit mean

Publications

- (a) **Christantus O. Nnamani**, M. R. A. Khandaker, and M. Sellathurai, “UAV-aided jamming for secure ground communication with unknown eavesdropper location,” *IEEE Access*, vol. 8, pp. 72 881–72 892, Apr. 2020
- (b) **Nnamani, Christantus O.**, M. R. Khandaker, and M. Sellathurai, “Secrecy rate maximization with gridded UAV swarm jamming for passive eavesdropping,” in *2021 IEEE Global Commun. Conf. (GLOBECOM)*, 2021, pp. 01–06
- (c) **Christantus O. Nnamani**, M. R. A. Khandaker, and M. Sellathurai, “Secure data collection via UAV-carried IRS,” *ICT Express, Elsevier*, 2022, Accepted
- (d) **Christantus O. Nnamani** and M. Sellathurai, “Inter-ference and noise cancellation for joint communication radar (JCR) system based on contextual information,” *IEEE*, 2022, Submitted

Chapter 1

Introduction

Remote monitoring of infrastructure and machineries are necessary for technological adaption to global connective singularity. It was promoted by advances in the Internet of Things (IoT), fifth generation (5G), and beyond. But these advances increase the requirement for secured and guaranteed communication. Therefore, this thesis aims to explore means of ensuring secured data communication between a remote transmitter and desired receivers using the unmanned aerial vehicles (UAV), intelligent reflecting surfaces (IRS), and wireless communication sensing as regulatory agents. In this chapter, a background to the challenge of seamless secured remote connectivity, and the regulatory agents were presented. The discourse of this chapter conclude with an overview of the thesis contribution.

1.1 Background

The maintenance of diverse industrial infrastructure is key to sustaining robust global supply chain. An example of such diverse infrastructure is the interconnection of pipeline systems for the oil and gas industry.

These infrastructures need monitoring to ascertain their reliability and possible activation of redundant control mechanism when failure occur. The monitoring requirement allow for the installation of sensory devices to collect various data transmissible to a central station for processing and decision making. The central station is required because the sensory devices are deficient with computational and power capabilities. The data is transmitted to the central station by collective inter-working (e.g. beamforming) of the sensors or using hop-to-hop (which can be automated or manual) transmission method [1]. But the distributed location of the infrastructures and distances to the central station in both the inter-working and hop-to-hop methods, makes it easier for eavesdroppers to purloin the transmitted data.

These eavesdroppers can be classified as active or passive depending on their status and activity within network. The active eavesdroppers continue to transmit data while listening to the leaked data. They are easily detectable based on their activities using well defined user geometric identification techniques [2]. Whereas the passive eavesdroppers are termed “quiet” as they only receive the leaked data while trying to mask their presence [3]. In this thesis, emphasis is laid on passive eavesdropping since they are more difficult to manage and pose greater challenge in securing information leakage.

Furthermore, the data collected by the passive eavesdroppers can be used in several legal and/or illegal ways. For example, in terms of pipeline monitoring, legal use may entail security re-evaluation, while illegal use may enable vandals to determine the activity of the pipeline and possible points of attack. Therefore, research into improving wireless communication-oriented security of infrastructure monitoring systems against eavesdropping is necessary against illegal use. We note that securing pipeline monitoring communication infrastructure is the primary application of thesis. However, since the scope of the communication-oriented security models are applicable to other sensor networks and peer-to-peer (P2P) communication, the thesis subsequently de-emphasis pipeline application.

1.2 Principles of Physical Layer Security (PLS)

A paramount interest of private businesses, public or government institutions, military and intelligence services is the protection of confidential and sensitive information. In the event that such data/information is made public, the affected organisation may face legal or financial ramifications. At the very least, they will suffer loss of customer trust (e.g. with respect to production companies, etc.); but in the worst case, it could lead to the complete annihilation of the organisation (e.g. with respect to the military, etc.). Therefore, secure communications are obligatory to most businesses/organisations; and in this sense seen as a primordial requirement of technological and industrial advances.

As technology continue to explode, especially with the gains of the IoT, 5G and future generation networks, adverse robust ways of information theft continue to grow [4]. In practice, an absolute secured communication is unattainable, nevertheless, theories seem to support some acceptable measure of security parameters [5, 6]. It is important that we continue to improve on the security parameters in line with the growth in technology.

Furthermore, due to technological growth and the need for standardisation, it became apparent that the structure of communication should be split into layers. This layered structure birthed the open system interconnection (OSI) [7, 8] published by the international organisation for standardisation (ISO) and the Internet model (transmission control protocol/Internet Protocol (TCP/IP) suite) [9] published by the USA department of defence (DoD). Generally, each layer of the OSI or the TCP/IP model communicate uniquely. Such unique communication aims to guarantee effective and secured communication. Nevertheless, information leakage still occur due to the resilience and adaptation of illegitimate listeners. However, researchers continue to develop several algorithms and techniques to secure the communication in each layer of the models, especially in the physical layer [6].

The physical layer is the easiest layer to purloin information in wireless communication, and it is similar to both the OSI and TCP/IP models [6]. In the higher layers of

the OSI and TCP/IP models, virtual P2P communications were established between the transmitter and receiver sections using packet headers and trailers. However, the headers and trailers cannot apply to the physical layer because it has a broadcast nature. It also deals with the processing of the encapsulated message for transmission via the channel in form of a broadcast [10]. In wireless communications, it means that it converts the message to electromagnetic waves referred to as radio signals. These signals are susceptible to eavesdropping since they are broadcast to defined directions [6]. Securing these signals lead to the concept of physical layer security (PLS).

The PLS is divided into keyed and keyless security models [11, 12]. The primary objective of both models is to reduce the ability of an illegitimate receiver, or eavesdropper, to gain access or properly decode the transmitted message. While the keyed model use information obscurity as its main tool, the keyless model detects possible information leak in the presence of eavesdropper(s) and attempts to decrease the quality of information it receives [13]. Several algorithms such as [14, 15], examine the generation of keys for keyed PLS. However, the main limitation of the keyed PLS is the complexity of exchanging the security keys between the transmitter and the legitimate receiver [16]. This has encouraged the acceptability and attraction of keyless PLS. In this thesis, keyless PLS is therefore discussed as a panacea to PLS.

1.3 Evolution of PLS in Wireless Communication

With the advent of mobile communication in the early 1990s, they have been rapid spread of wireless communications services spanning into the 5G applications [13, 17]. But securing these wireless communication and services are paramount issues. In this section, an evolutionary description of securing the wireless communication using PLS was presented.

The discussions on PLS dated to Shannon's theorem popularly referred to as noisy channel coding theorem or Shannon limit on communication channel of 1945 [18].

The theorem states that the maximum error free information rate is upper bound by its maximum rate through the channel. It implies that the channel is ideal, free from noise and interference. It also means that perfect secrecy is possible if the signal received by the eavesdropper does not contain any information of the transmitted message since the channels are unique to each user. A typical Shannon model is illustrated in fig. 1.1. However, this assertion is plausible only when we neglect the processing and listening capability of the eavesdropper or the possibility of its knowledge of the transmit codebook [19]. These inherent assumptions of Shannon theory limits its application to practical wireless communication models.

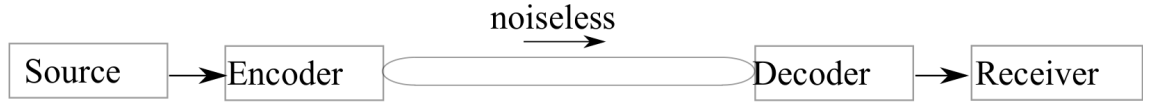


FIGURE 1.1: Shannon communication model.

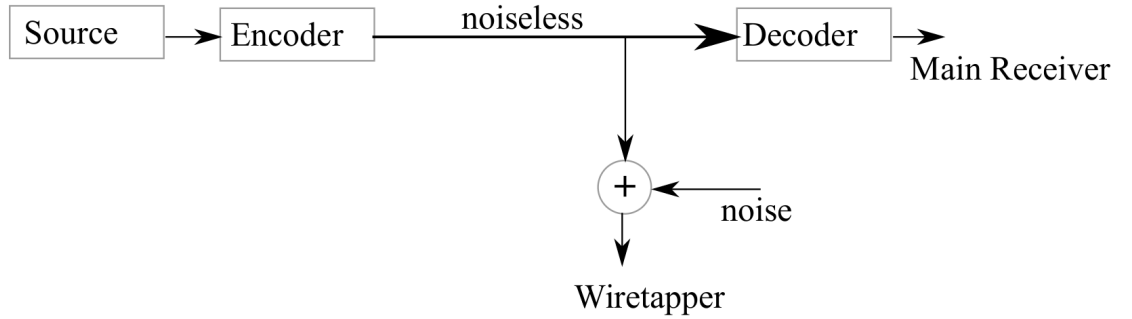


FIGURE 1.2: Wyner wiretapper.

Subsequently, A.D. Wyner in 1975 defined a wiretapper channel without the computational limitation of Shannon. The wiretapper refers to a passive eavesdropper that does not attempt to alter the transmitted message. Wyner assumed a noisy channel for the wiretapper and a noiseless channel for the legitimate receiver as shown in fig. 1.2 [20, 21]. Wyner further defined the equivocation “as a measure of the degree to which the wiretapper is confused” [21] by using a randomised invertible encoder. Furthermore [21] records that it is possible to transmit under the Wyner conditions

and still obtain a near perfect secrecy because of the ideal status given to the legitimate channel. It is noteworthy that the attempts to pursue perfect secrecy with the Wyner wiretapper led to discourse into keyed and keyless PLS.

The keyed PLS emphasise on confusing the eavesdropper by using variable key lengths and configurations for message encryption. This makes it difficult for the illegitimate receiver to decipher the message without knowledge of the encryption key. In contrast, keyless PLS uses the dynamic intrinsic properties of communication channels to support the legitimate receiver's signal, while reducing the information content of the signal received by the eavesdropper. Such intrinsic channel properties include fading, interference, multipath, shadowing and noise [22]. Without undermining the security benefits of keyed PLS and higher level security, the keyless PLS tends to enjoy the following advantages:

- (a) The complexity of key management and distribution is subdued with the keyless PLS.
- (b) Keyless PLS enjoys less overhead with no alterations to the legitimate message.
- (c) The security system is robust due to inherent stochastic channel distribution.

It is based on these benefits that we have focused on developing algorithms to improve the keyless PLS in this thesis.

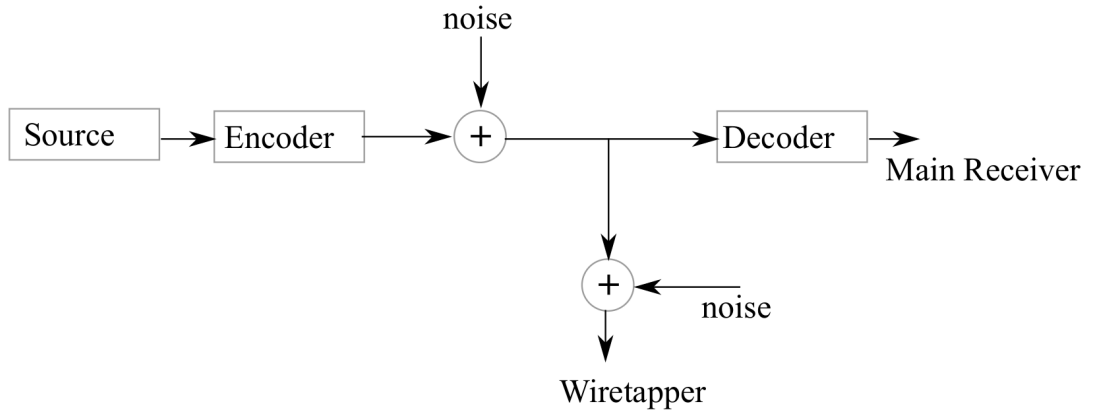


FIGURE 1.3: Gaussian version of Wyner wiretapper.

Considering keyless PLS, the Wyner model was adapted to a realistic model by Leung and Hellman in 1978 [23]. They showed that by applying a noisy Gaussian channel to the legitimate user, some degree of equivocation was maintained. Secrecy capacity given in (1.1) was then defined as a measure of the equivocation. A pictorial representation of the model developed by [23] is shown in fig. 1.3.

$$C_s = [\log(1 + \gamma_B) - \log(1 + \gamma_E)]^+, \quad (1.1)$$

where $[x]^+ = \max(x, 0)$ and $\gamma_i \forall i \in \{B, E\}$ represents the signal to noise ratio (SNR) at the legitimate receiver (B) and the eavesdropper (E).

Equation (1.1) gives the secrecy capacity as the difference of Shannon's information rate at the legitimate receiver and the eavesdropper. The higher the secrecy capacity, the greater guarantee that the communication is secured from a physical layer perspective. However, positive secrecy capacity is possible with respect to (1.1), if and only if the channel quality of the legitimate receiver is better than that of the eavesdropper.

Following the description of the secrecy capacity, two main key performance metric (KPM) were developed to enable the quantification of PLS of wireless communication. The KPM are the secrecy rate and the secrecy outage probability defined mathematically as (1.2) and (1.3) respectively [24].

$$R_s = \max_{P(t)} C_s, \quad (1.2)$$

$$P_{outage} = \Pr[C_s < R_t], \quad (1.3)$$

where $P(t)$ is the instantaneous transmit power. While the secrecy rate presents a direct measure between the capacities of the legitimate receiver and the eavesdropper, the outage probability compares the deviation of the secrecy capacity from a set or desired threshold [24, 25]. In other words, secrecy rate defines PLS of a communication system over time while secrecy outage probability is not time bound. Since the average secrecy rate is defined by time, it allows for investigation of the

the distribution of the secrecy capacity rather than direct probabilities of secrecy outage probability. Therefore, although both KPMs are frequently used in literature to define PLS, in this thesis, we have used secrecy rates (defined as average secrecy rate) as the primary KPM, due it's robustness to define PLS over the communication time frame.

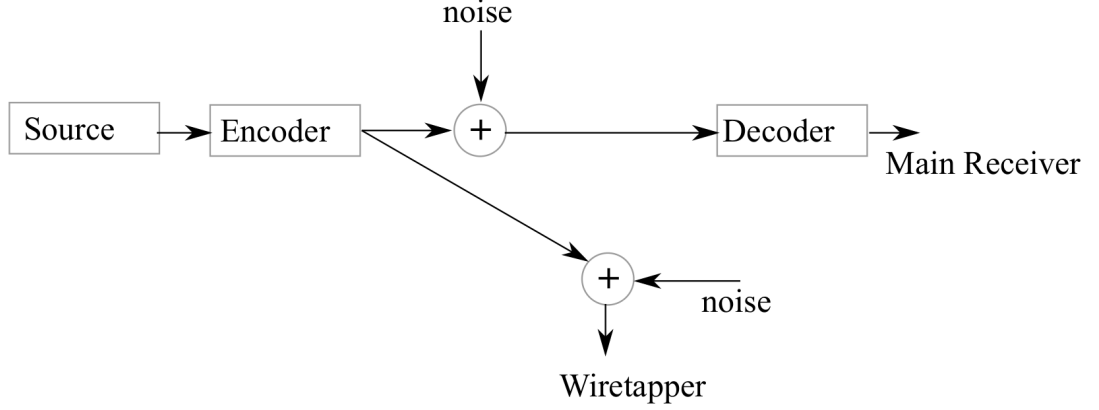


FIGURE 1.4: Wireless communication model.

The condition for positive secrecy capacity is strict in the wireless communication model, shown in fig. 1.4. The strictness is due to the independent noise level between the legitimate receiver and eavesdropper in the wireless domain. Hence, the constraint on better channel quality of the desired receiver cannot be guaranteed [26,27]. However, to ensure secured physical layer communication, techniques of improving the channel quality of the legitimate receiver or worsening that of the eavesdropper continue to evolve. The variable rate scheme is an example that cause the transmission be stopped when the channel conditions at the eavesdropper is better than the legitimate receiver [5]. Another example is the deployment of jamming [28,29] and artificial noise signals [30] to worsen the channel quality of the eavesdropper. Studies in literature continue to merge advances in technology with designs of key-less PLS systems. Table 1.1 presents a general overview of the contributions from the literature in comparison to the works presented in this thesis.

TABLE 1.1: Overview of PLS algorithms

Reference	Eavesdropper		Jamming	Key technology
	Active	Passive		
[5]	✓	✓	✗	Variable rate
[29, 31–33]	✓	✗	✓	UAV, M-MIMO
[Thesis]	✗	✓	✓	UAV, IRS, Sensing

1.4 Technologies Deployed for Improved PLS

Studies into PLS adapts to the growth of technologies that support wireless communication. This is because these advances increase the processing and computational ability of the eavesdropper too. In this section, we introduce on key technologies that have been implemented within this thesis as solutions to current PLS demands.

1.4.1 Unmanned Aerial Vehicle (UAV)

Unmanned aerial vehicle (UAV) is fundamentally an automated aircraft without direct on-board human supervision [34, 35], [36]. It is a component of the unmanned aircraft system (UAS) which comprise of the UAV, ground station and a communication link. The UAV flight maybe remotely controlled or programmed [37, 38]. In recent times, UAVs have been the subject of concerted research, primarily due to their vast applications and unique properties of autonomy, and flexibility [17]. Although it was initially designed for military use, its application currently spans various application domains such as agricultural, scientific, product delivery and recently, in wireless communications.

1.4.1.1 UAV Classification

UAVs are classified based on their peak flight heights (altitude) and the type of wing build up [39]. These classification also guarantees their unique properties and subsequently their suitability for specific applications. For example, for long term wireless communication coverage over a large area, it is typical to deploy high altitude platform (HAP). Figure 1.5 and table 1.2 presents the classifications and features respectively. It is important to note that typically HAP is usually fixed wing while low altitude platform (LAP) can be fixed wing (FW) and/or rotary wing (RW). The flight duration in table 1.2 is also a function of several factors like energy source, type of UAV, specific deployment function, UAV weight, and speed of the UAV.

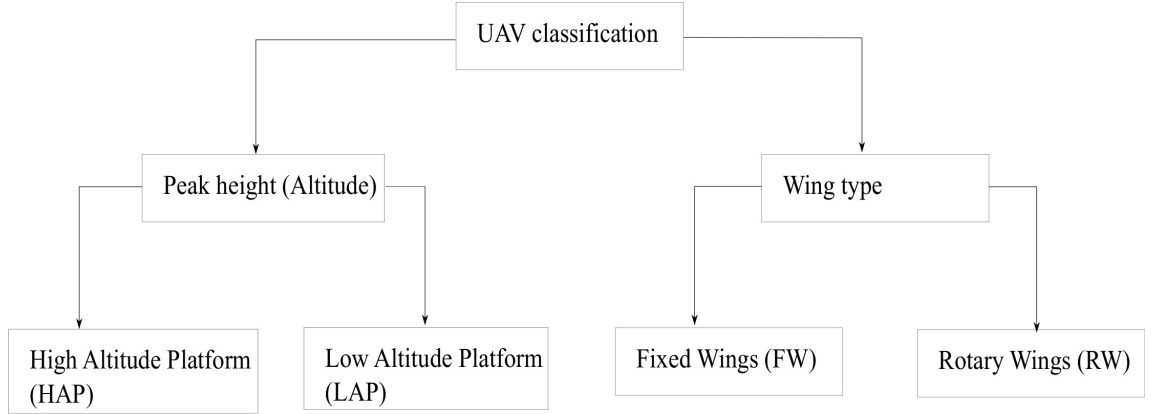


FIGURE 1.5: UAV classification.

Although the application of UAV is vast, its deployment is still subjected to various regulatory issues due to concerns on privacy, accident, and data security/protection [35]. UAV regulations are usually country or geographical specific but generally includes ethical and technical constraints, administration, application and operational boundaries. Therefore, operating UAVs for wireless communication applications ensures that the wireless domain supports for other wireless communication applications is maintained with no additional risk to the environment or the populace.

TABLE 1.2: Features of UAV classification

HAP	LAP	FW	RW
Wide coverage	Limited coverage	Cannot hover	Can hover
Quasi-stationary	Non-stationary	Travel with high speed	Lower speed
Cost intensive	Cost effective compared to HAP	Expensive compared to RW	Cheap
Longer flight duration (Days or Months)	Less flight duration (several hours)	Several hours	Very few hours (<2hours)
Limited deployment flexibility	Fast and flexible deployment	Large payload	Small payload

1.4.1.2 UAV Swarm

A collection of independent mobile individual entities that are autonomous but interact reactively to produce an aggregated behaviour, called a global behaviour, is referred to as a swarm [40, 41]. The global behaviour can be referred to as the behaviour from a single but larger entity. Some practical examples of swarming in nature include, the movement of flocking birds or a school of fish and the swarming bees. With advances in technology, these natural occurrences were adopted into the use of collaborative UAVs applications (including wireless communication applications). The group of collaborative UAVs are referred to as UAV swarm or the internet of drones. The entities of the UAV swarm are individual autonomous UAVs. Although for wireless communication purpose, the UAV swarm was primarily designed to provide ubiquitous communication in 5G, its application in keyless PLS is gaining greater popularity in recent times [34]. However, control of the individual UAVs in the swarm to act as a single entity is an open research aspect based on its application.

In general, UAV swarm control is broadly classified, based on its decision making process, into centralised and decentralised control [41]. The centralised control defines explicitly the unique behaviour of elements of the swarm via a central control system while the decentralised control allows each swarm element to independently access its local (immediate environment) or global (entire environment) information and makes decisions based on the information that controls its behaviour.

1.4.2 Intelligent Reflecting Surfaces (IRS)

Recently, focus on wireless channel control has led to a shift in paradigm with the discovery of the intelligent reflecting surfaces (IRS) [42–44]. IRS provide an interface between traditional wireless base stations and users. Unlike conventional active relays, IRS only reflect radio signal, thus do not require the radio-frequency (RF) chains. The reflected signals are inherently free from self-interference while traveling through a conditioned wireless communication channel [45]. Current literature explores several designs to harness the intelligence of IRS for effective communication, by optimally controlling the reflection coefficients and other related established parameters, like transmit beamforming weights when multiple sources/receivers are applicable.

In wireless communication, PLS inherent desired specular reflection of the IRS system is harnessed. This property allows for maximum power transfer at the desired reflection location. It is therefore apparent to carefully design the parameters of the IRS system to manage eavesdropping.

1.4.3 Wireless Communication Sensing

Recently, due to advances in vehicular infrastructure the need for driverless vehicles has inclined studies into the feasibility of the cohabitation of various sensors using diverse spectrum bands. This is further exacerbated by the congestion of the below 6GHz spectrum band mainly used for low earth spectrum applications. A prominent

sandwich of application in most discourse is radio detection and ranging (RADAR) and wireless communication applications with critical reviews presented in [46, 47]. Spectrum users can in principle collaborate via cohabitation, co-design and cooperation [46]. However, such collaboration is usually marred by several design challenges such as interference management, varying power requirements, integration and security. For example, a typical paradigm to the design challenges suggests that RADAR systems require higher transmit power than wireless communication, but reflected RADAR signal is usually low powered which is highly susceptible to interference from communication signals. Joint sensing entails developing algorithms to enable seamless collaboration between applications sharing a particular spectrum.

1.5 Scenario Description

Consider a secure wireless communication scenario between a base station (BS) acting as a transmitting source (Alice) located at a known ground point¹ $\Omega_A = [x_A, y_A, 0]^T$ and a receiver (Bob) at a known ground point $\Omega_B = [x_B, y_B, 0]^T$ as shown in fig. 1.6. However, an eavesdropper (Eve) lurks around the area.

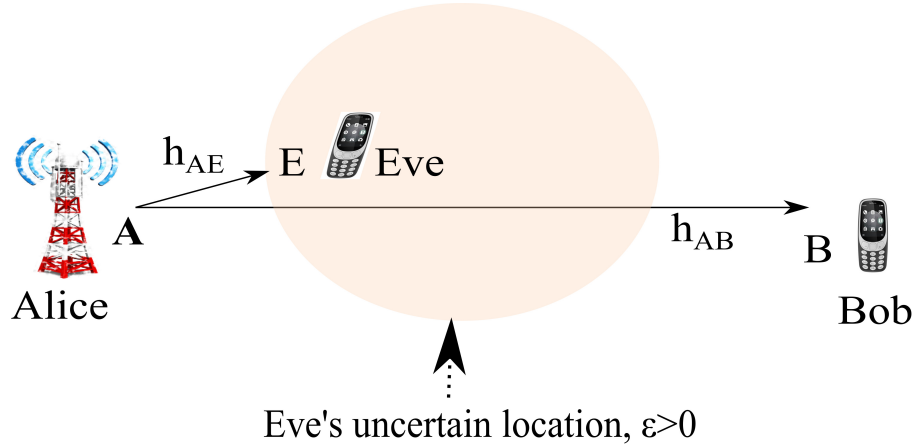


FIGURE 1.6: General thesis system model discussed.

We assume that Eve is located in a closed circular region with radius, ε , and centre at point $\Omega_E = [x_E, y_E, 0]^T$. The circular region is within the coverage region of

¹z-coordinate represents the altitude and the ground point is located at $z=0$.

Alice. This assumption is feasible given that a passive Eve will practically be within an area where it can easily purloin information without revealing its location. As $\varepsilon \rightarrow 0$, the closer we arrive at the exact location of Eve. However, since the exact position of Eve is unknown, ε must always be greater than zero and possibly can be increased to cover the entire coverage region of Alice, and thereby introducing the maximum uncertainty on Eve's location. It is also possible that the uncertain region where Eve is located can extend to the location of Bob. This will imply that Eve can possibly be co-located with Bob. In this thesis, the co-location of Eve and Bob is the worst case scenario as the schemes developed aimed to reduce the listening capacity of Eve when it is not co-located to Bob.

We note that it is assumed that the optimisations and computations carried out in this thesis were performed on a high capacity central node. This implies that memory and computing equipment are assumed to be infinity at the central processing node. Furthermore, we also assume that the computations are transferred seamlessly to the required node using a secured control signalling terminal.

1.6 Thesis Outline

In this thesis, solutions to securing communication between users (sensors) and the control stations (base stations) were presented using a combination of the technologies highlighted in section 1.4. Two main approaches were deployed: use of jamming signal; and harnessing the immanent properties of IRS and wireless sensing systems. These approaches were designed by jointly optimising the UAV trajectory and the transmit power, reflection coefficients, and beamforming vectors as applicable. It suffice to mention that the primary performance metric used to evaluate the PLS in this thesis was the average secrecy rate.

In the subsequent chapters of the thesis, complex non-convex PLS problems were reduced to sub-optimal convex problems. The problem transformation and methodological techniques were part of the novel contributions of this thesis.

Chapter 2 gave a discourse on using jamming from the UAV to guarantee positive secrecy rate for communication under passive eavesdropping. A novel expression for average secrecy rate with passive eavesdropping was derived considering that the rate of the eavesdropper was upper bound by that of the legitimate receiver. To improve on the PLS of the system, a UAV was used to deliver jamming/interfering signals in a coordinated approach to minimise interference at the legitimate receiver. Hence, an optimisation problem was formulated to design the transmit power from the transmitter, the jamming power, and the trajectory of the UAV. The solutions obtained showed that positive secrecy rate was guaranteed when the eavesdropper is passive.

Furthermore, the study of the possibilities for improving PLS with multiple UAVs were analysed following the positive single UAV observation in chapter 2. A swarm of UAVs in grid formation was deployed and optimised to improve the performance of the secrecy rate in chapter 3. The swarm design entailed the determination of their trajectory and jamming power.

Subsequently, the IRS miniaturised the swarm of UAVs while offering guaranteed positive secrecy rate in chapter 4. Hence, a single UAV solution for data collection and security optimisation using IRS was investigated. The chapter examined the reflective coefficient adjusting property of IRS as the primary variable and showed that it has the potential to aid PLS. Following the non-convex problem formulated in the chapter, two solutions were developed considering the passiveness of the eavesdropper.

In chapter 5, the role of communication sensing in enhancing PLS was examined. Using the cohabitation of wireless communication and RADAR technologies as a case study, the impact of their relationship was considered as a prerequisite for PLS guarantee. Specifically, novel autoencoder based interference and noise cancellation filter was designed to separate desired signals from the received signal. The filter is applicable where sensing is required for seamless cohabitation.

A summary of the thesis was elucidated in chapter 6 with some future prospects discussed. In addendum, appendices A and C provided proofs of different equations relating to derivations made in chapters 2 and 4 respectively. Furthermore, the signal-to-interference noise ratio (SINR) probability distribution of the aerial UAV-carried IRS system was given in Appendix B.

Parts of the chapters of this thesis were based on published peer reviewed journal or conference articles.

- (a) Chapter 2 was based in part on the journal article **Christantus O. Nnamani**, M. R. A. Khandaker, and M. Sellathurai, “UAV-aided jamming for secure ground communication with unknown eavesdropper location,” *IEEE Access*, vol. 8, pp. 72 881–72 892, Apr. 2020

It was also presented in the conference of **Christantus O. Nnamani**, M. R. A. Khandaker, and M. Sellathurai, “Maintaining secrecy in communication with UAV-to-ground jamming amidst passive eavesdropping,” in *TECHISD2020: Int. Conf. on Technol. Innovation for Holistic Sustainable Development*, Sept. 2020.

- (b) Chapter 3 followed from the conference proceedings of **Nnamani, Christantus O.**, M. R. Khandaker, and M. Sellathurai, “Secrecy rate maximization with gridded UAV swarm jamming for passive eavesdropping,” in *2021 IEEE Global Commun. Conf. (GLOBECOM)*, 2021, pp. 01–06
- (c) Chapter 4 was published in part in the journal article **Christantus O. Nnamani**, M. R. A. Khandaker, and M. Sellathurai, “Secure data collection via UAV-carried IRS,” *ICT Express, Elsevier*, 2022, Accepted
- (d) Chapter 5 has been submitted to a journal **Christantus O. Nnamani** and M. Sellathurai, “Inter-ference and noise cancellation for joint communication radar (JCR) system based on contextual information,” *IEEE*, 2022, Submitted

1.7 Notations

Throughout the chapters of this thesis, we comment that “Eve”, “Bob” and “Alice” describe the eavesdropper, the legitimate receiver and the transmitting stations respectively. The variables used in any chapter of the thesis were properly defined therein, and are exclusive for that chapter. However, the general structure of the notations employed in the thesis elucidate in this section. $\{\cdot\}^*$, $\{\cdot\}^T$ and $\{\cdot\}^H$ represent the conjugate, transpose and Hermitian of vectors/matrices, respectively, while $\hat{\mathbf{a}}_{ij} \triangleq \frac{\mathbf{a}_j - \mathbf{a}_i}{\|\mathbf{a}_j - \mathbf{a}_i\|}$ represents a normalised/unit vector along the direction of propagation from location i to j . $\text{diag}(\mathbf{x})$ is a diagonal matrix with the vector, \mathbf{x} as the main diagonal and $\mathbf{1}$ is a column vector of 1’s. Low case letters are scalars, bold-faced low case letters are vectors while bold-faced upper case letters are matrices. Furthermore, $\text{rank}(\mathbf{X})$ and $\text{Tr}(\mathbf{X})$ are the rank and trace of matrix \mathbf{X} respectively, while $\mathbb{E}[\cdot]$ is the expected value. $[a]^+$ indicates $\max(0, x)$ i.e. the maximum value between 0 and x . $\text{Re}\{x\}$ and $\text{Im}\{x\}$ represents the real and imaginary parts of the complex number, x .

Chapter 2

Physical Layer Security Optimisation for Passive Eavesdropping

In this chapter, we investigate the use of a single UAV to deliver jamming signals when an eavesdropper is passive. The design characterises the procedure to ensure that the effect on the legitimate receiver is minimum compare to the eavesdropper. The objective of this chapter is to present the formulations to reduce the amount of information obtained by an eavesdropper. Section 2.1 discusses state-of-the-art literature and the research gap filled by this chapter. In section 2.2, the system description of the model was presented leading to the problem formulation. Solution to the formulated problem was given in section 2.3. Thereafter, numerical simulations and analysis of the results were highlighted in 2.4. The chapter concluded with a recap of the main contribution of the chapter in section 2.5.

2.1 Related Works

To maximise the secrecy capacity, an on/off algorithm that regulates the power transmitted from the source depending on the channel quality of the eavesdropper

and legitimate receiver was developed in [5]. This method, referred to as the variable rate scheme, rely on the principle that the transmitter knows the channel state of the eavesdropper. This information may be based on previous channel monitoring or reliable estimation. However, when the eavesdropper is passive, as in many practical scenarios, the on/off approach become limited. This is because determining the control for the transmit power becomes difficult since channel comparison of the eavesdropper and legitimate receiver cannot be performed. In addition, the on/off approach reduces the information received at the legitimate user when both active or passive eavesdropping occur. Therefore, instead of regulating the transmit power alone, a need for other ways to augment and minimise the content of information received by the eavesdropper is necessary. Such approach requires the deliberate jamming of the eavesdropper's channel.

Jamming of illegitimate signals is a prominent brute-force methods of limiting information theft in keyless PLS. It exploits the fading characteristics of the channel as a physical layer protection strategy [10]. The jamming signals have similar characteristics to the legitimate signal received by the illegitimate listener but they do not contain information. The jamming signals cause interference of the legitimate signal at the eavesdropper. Although the jamming technique does not guarantee that there will be no information leakage, similar to other security techniques, it reduces the probability of successful interception, by increasing the signal distortions of an end-to-end communication. A form of jamming entail attaching artificial noise signal to the transmission signal and then rely on the ability of the legitimate receiver to filter out the noise. Several authors had proposed the designs at the receiver to enable it filter out the artificial noise [30, 48, 49]. Furthermore, the jamming signals can be delivered from a fixed transmitter [50, 51].

The major limitation of these jamming techniques is that the eavesdropper will usually operate at the same band as the legitimate receiver. Hence jamming the received signal at the eavesdropper will also affect the legitimate receiver. Therefore, while jamming poses to be an effective technique for improving secrecy, there are some critical design issues, such as:

- (a) The degree of transmit power required to increase the secrecy capacity without adversely degrading the information content of the desired receiver or exceeding the acceptable power threshold of wireless communication.
- (b) The transmitter's responses to the knowledge of the possible eavesdropper(s).
- (c) The optimal location or channel to deliver the jamming signals.

Researchers have since investigated these requirements independently as shown in [52]. However, the collective investigation of (a)-(c) is of practical interest due to their inter-dependency in the context of secrecy performance. While some recent studies affirm that signal jamming yields improvement in the secrecy capacity, they are mostly based on the impractical assumption that the eavesdropper location is perfectly known at the transmitter [36, 53]. However, in practice, the eavesdropper may be passive as implied in this thesis. The passiveness means that the channel statistics are unknown at the transmitter or that the location of the eavesdropper is unknown. Nevertheless, if we consider inverse-square law, then the location of the eavesdropper invariably translates to its channel quality.

With respect to the known eavesdropper location (referred as active eavesdropper in this thesis), mobile means of delivering the jamming signals have recently been investigated in the literature. Mobile jammers using vehicular ad hoc networks (VANET) was investigated in [54]. It was shown that by transmitting jamming signals periodically, communication can be jammed even with weak jamming signal. However, the influence of the jamming is reduced without clear line-of-sight (LoS). Another effective mobile methods is the use of an UAV in scenarios where the nodes under consideration (the source, the main receiver and the eavesdropper) are all ground based. The efficiency of using UAV as a mobile means to deliver jamming signals are due to its aerial radio visibility of the ground terminals, its cost efficiency and availability for low-range applications. Other applications of UAVs in communications range from their use as aerial base stations [33, 55–57], as relay nodes [58], as

access/user nodes [55, 59] to channel estimation [39], etc. Recently, with the advancement of the IoT, network of UAVs for UAV-to-UAV communications as well as for general data transmission has also been considered [60].

UAVs was deployed for secured communications between ground terminals [29, 31], and to act as both relay nodes and security agents between ground terminals [61]. In [32], the UAV was deployed with two opposing roles namely: to establish favorable channel for the legitimate receiver, and degraded eavesdropping channels. A separate jammer UAV had been considered in [62] to degrade the eavesdropping channel in addition to the cooperative UAV for the legitimate channel. Subsequently, UAVs have been used to deliver classified messages to ground terminals amidst the constraints of eavesdroppers and no-fly regions in [63]. Critical examination reveals that the methods used in [29, 31, 32, 61–63] are similar in principle since they optimise the transmitted power, the UAV jamming power and its trajectory for the corresponding scenarios. The examination also reveal that a combination of jamming and the on/off approach proposed in [5] is the bedrock of modern signal jamming techniques. However, a strong assumption made by the papers were that the location of the eavesdropper(s) was known to the source and/or the UAV(s) [29, 31, 32, 61–63]. Although this assumption simplifies the respective problem in each scenario, it is impractical. In most practical communication scenarios, even knowing that an eavesdropper is present is often very difficult, let alone knowing their exact locations or channel state information (CSI). This practical challenge motivates us to investigate secret communication with unknown eavesdropper location and CSI. We consider UAV-aided jamming technique to proactively degrade the eavesdropping channel at unknown ground point thereby, improving the achievable secrecy rate.

An attempt to introduce eavesdropper obscurity has also been made by Miao Cui, et al. in [64]. The authors in [64] considered the UAV as the information source and optimised its trajectory and transmitting power to a legitimate receiver amidst a group of eavesdroppers located within an independent small uncertainty region. The trajectory of the UAV was optimised to find the best points in the space to deliver the maximum information to the legitimate receiver while the eavesdroppers receive

minimum information. In contrast, we consider the UAV with an opposing role to degrade the eavesdropper's channel via cooperative jamming. Note that our work differs from [64] not just in terms of the UAV's role, but also in terms of guaranteed secrecy performance. In fact, the achievable secrecy performance in [64] cannot be guaranteed as the uncertainty region expands and overlaps with the certainty region of the legitimate receiver.

Furthermore, solution to a UAV networked system was considered in [65]. A UAV acts as the base station to transmit signal to other legitimate UAVs in altitude and the eavesdropper UAVs from unknown locations try to overhear the signal. The secrecy outage probability and average secrecy rate performance were analysed. Since all the nodes are at the same altitude, the gains of aerial visibility of UAV was subdued. In this chapter, we intend to explore this opportunity for ground nodes (source, legitimate receiver and eavesdropper) in order to maximise the benefits of aerial visibility of the UAV while constrained by the properties of ground propagation.

We formulate the problem of maximising the average secrecy rate under the unknown eavesdropper location assumption by jointly optimising the source transmit power, the UAV trajectory and its jamming power. The problem was non-convex due to the correlation of the optimisation variables in the problem. Therefore, we sequentially optimise the flight path of a UAV, its jamming power and the transmitted power by the source node to ensure secure communication in the considered scenario. A variable was optimised in each step while keeping the others fixed. The main contributions in this chapter are as follows:

- (a) Developing the formulation of average secrecy rate for passive eavesdropping considering variable rate scheme.
- (b) Applying the block coordinate descent method and successive convex approximation (SCA) technique with the aid of the first-order Taylor series expansion in order to solve the non-convex problem arising from the formulations.

- (c) Investigating the influence of the unknown eavesdropper's received power on the average secrecy rate between the source and the legitimate receiver.
- (d) Validating the formulations and the solutions by demonstrating the performance of the proposed algorithm against existing UAV-aided secure communication schemes through extensive numerical simulations.

2.2 System Model

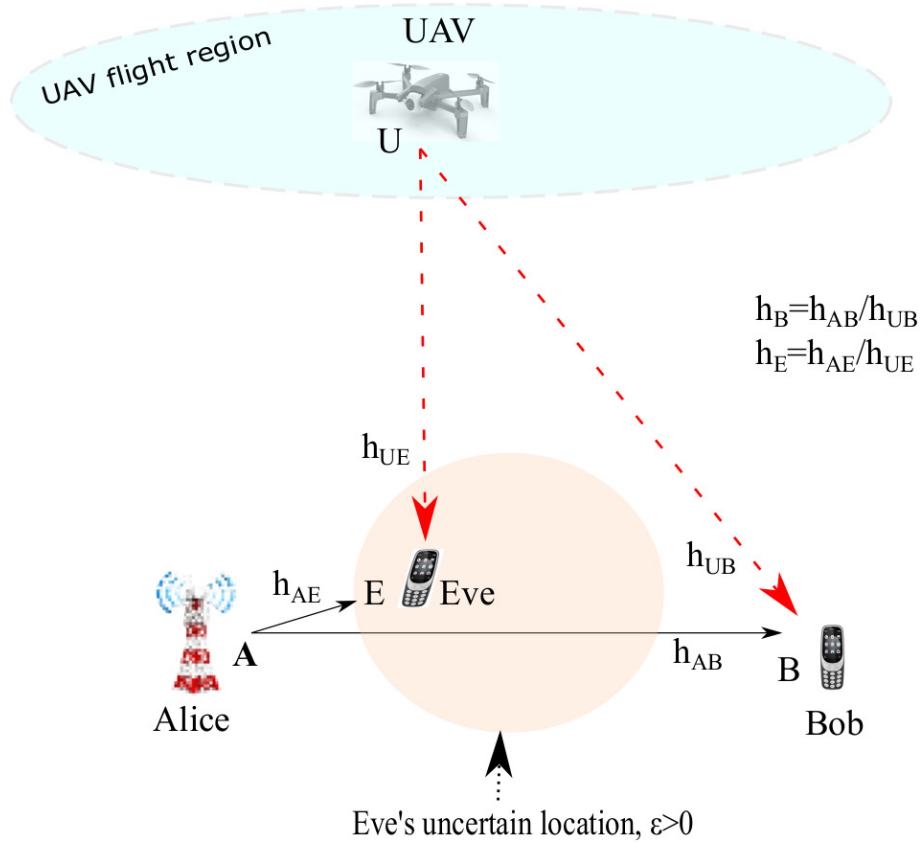


FIGURE 2.1: UAV-aided jamming for secure communication.

Let us consider the scenario described in section 1.5 where we use a UAV to deliver jamming signals to Eve. Figure 2.1 presents the pictorial description of the scenario. We discuss in this section, the analytical description of the relevant parts of the model that will enable the definition of the PLS problem. It is important to highlight that the jamming signals designed in this thesis are low powered to avoid

causing radiation injuries and manage interference. The algorithm ensures that the interference is restricted to the illegitimate receiver.

We denote the complex block-fading channels of Alice with Bob and Eve as g_B and g_E , respectively. Since Eve's location was unknown, Alice's transmission power P_A is a function of Bob's channel power gain $h_B = \mathbb{E}[|g_B|^2]$ alone; hence $P_A = P(h_B)$. This implies that Alice varies her transmission power depending on the channel state of Bob. Averaging through all fading realisations of the channels of Bob and Eve, the average secrecy rate and secrecy capacity derived from Shannon's information content are given respectively as (2.1) and (2.2) [5].

$$R_s = \int \int \underbrace{[\log_2(1 + h_B P(h_B))]}_{\text{information rate of Bob}} - \underbrace{\log_2(1 + h_E P(h_B))}_{\text{information rate of Eve}} \big]^+ f(h_B) f(h_E) dh_E dh_B, \quad (2.1)$$

$$C_s = \max_{P(h_B)} R_s, \quad (2.2)$$

where R_s , C_s , and $P(h_B)$ are the average secrecy rate¹, secrecy capacity, and transmit power from Alice, respectively. h_B , $f(h_B)$, and $h_E = \mathbb{E}[|g_E|^2]$, $f(h_E)$ are the channel power gain and probability density functions (PDF) of Bob and Eve, respectively. Note that $[\cdot]^+$ imposes a constraint such that Eve cannot receive higher information than Bob at any time during the communication. Hence, in the subsequent formulations, the $[\cdot]^+$ will be ignored since the value of the integral function is always non-negative. Accordingly, the limits of the integrals in (2.1) are defined such that when $h_E > h_B$, the mutual information between Alice and Eve is upper-bounded by $\log_2(1 + h_B P(h_B))$. This ensures that averaging the secrecy rate over all possible channel realisations of Eve is upper bounded by the channel of Bob following the variable rate scheme described in [5]. Thereby sustaining the objective of keyless PLS to ensure that (2.2) was maintained at its optimal value over the communication duration. It is desirable that the rate of Bob is as high as possible and only limited by the power constraints of Alice (transmitter). In this regard,

¹All logarithms used in this thesis are of base 2, since we refer to digital communications.

(2.1) reduces to (2.3).

$$R_s = \int_0^\infty \int_0^{h_B} [\log_2(1 + h_B P(h_B)) - \log_2(1 + h_E P(h_B))] f(h_B) f(h_E) dh_E dh_B. \quad (2.3)$$

The achievable secrecy rate in (2.3) describes the secrecy rate as the difference of the average information rates of Bob and Eve over all fading realisations. The non-negativity assumption on the secrecy rate $[\cdot]^+$ requires that the location of Eve revolves around that of Bob and not beyond the coverage region of Alice. However, in practice, Eve may even be located at positions closer to Alice than Bob and thereby receive stronger signals than Bob based on the proximity, and assuming they both share the same channel model. In such scenarios, the achievable secrecy rate would be zero as defined by the integral limits in (2.3) and proposal in [5]. This implies that the transmit power will be switched off, thereby stopping the transmission to the Bob too.

However, to ensure that even when Eve supposedly has better channel quality, that the transmission continues, we deploy a UAV that will deliver jamming signals. The jamming signals will act to reduce the information content of Eve while sustaining that obtained by Bob. Based on this functionality of the UAV, the question arises on how to design its trajectory and the power level of the jamming signal. The challenge worsens when the CSI of Eve is unknown.

If we assume that the UAV is not equipped with tracking devices, then the UAV will not be able to locate or track Eve despite having a clear LoS to all points within the coverage region of Alice due to aerial visibility. Furthermore, if the UAV flies horizontally at constant altitude from an initial point, \mathbf{q}_0 , to a final point, \mathbf{q}_f , its ascent and descent flight path to the initial and final ground points can be neglected. This means that the UAV flight displacement is preset by the start and end points. Let the UAV flight duration, T , be sampled at discrete time-stamps of N equal time slots with duration of $\delta = T/N$ [29, 55, 58]. The UAV maintains constant speed Z m/s and transmits a pulse of the jamming signal within a slot δ . The channel within the slot is assumed to vary slowly allowing for block fading within the slot. Hence, by

increasing the number of time slots, N , the UAV may be assumed to transmit almost continuously. We note that as $N \rightarrow \infty$, the UAVs are seen as following a continuous trajectory satisfying time-sharing conditions, thereby, delivering jamming signals continuously through its entire flight time [29]. For simplicity, we assume that Z m/s is constant over the entire flight duration as also assumed in [29, 55]. If the distance covered in each sample is small enough, we can assume that the UAV is stationary at each sample point. Considering a large number of sample points, the UAV, therefore, sends jamming signals continuously as it flies. These sampled points can be denoted as $\mathbf{q}[n] = [x[n], y[n], z[n]]^T$, $\forall n \in \{1, \dots, N\}$, which satisfies the constraints in (2.4).

$$\|\mathbf{q}[n+1] - \mathbf{q}[n]\|^2 \leq (Z\delta)^2 \quad (2.4a)$$

$$\|\mathbf{q}[1] - \mathbf{q}_0\|^2 \leq (Z\delta)^2 \quad (2.4b)$$

$$\mathbf{q}[N] = \mathbf{q}_f \quad (2.4c)$$

$$\|\mathbf{q}[n] - \mathbf{\Omega}_A\| + \|\mathbf{q}[n] - \mathbf{\Omega}_B\| \leq 2\varepsilon \quad (2.4d)$$

$$\mathbf{q}(x_n, y_n, z_n) = \mathbf{q}(x_n, y_n, H). \quad (2.4e)$$

Inequalities (2.4a) and (2.4b) ensure that the distance covered by the UAV within the flight samples does not exceed the parametric distance. The velocity Z m/s is chosen such that the total distance covered by the UAV through the samples will be greater than or equal to the Euclidean distance between \mathbf{q}_0 and \mathbf{q}_f , i.e., $(Z\delta) \geq \|\mathbf{q}_f - \mathbf{q}_0\|$, otherwise the system will be intractable. This ensures that the UAV travels at least in a straight path from its initial to its final points for a given total flight duration. The equality in (2.4c) ensures that the final flight point of the UAV is at an *a-priori* final destination, while (2.4d) allows the UAV to remain within the uncertainty region where the eavesdropper can be found. This region was postulated as an ellipse and physically represents a cellular coverage region of Alice. The variable, ε determines the size of the ellipse and satisfies $\{\varepsilon > \|\mathbf{\Omega}_B - \mathbf{\Omega}_A\|\}$, $\mathbf{\Omega}_A$ and $\mathbf{\Omega}_B$ are the two foci of the ellipse, ensuring that Bob is not a cell-edge user. We

note that in this chapter, $\varepsilon > 0$. However, if $\varepsilon = 0$, then the exact location of Eve is obtained. Finally, (2.4e) places the UAV to fly at constant altitude denoted by H meters.

Assuming that the ground fading channel between Alice and Bob is Rayleigh distributed, the lower bound of the channel power gain (corresponding to the worst channel condition) with the jamming signal delivered by the UAV was extracted from [31, 32, 62] and presented (2.5).

$$h_B[n] = \frac{\overbrace{\rho_0 d_{ab}^{-\psi} \mathbb{E}[\zeta]}^{\text{ground channel gain}}}{\underbrace{P_u[n] \rho_0 d_{qb}^{-2}[n] + 1}_{\text{LoS jamming signal attenuation}}}, \quad (2.5)$$

where ψ is the ground path loss component between Alice and Bob, ρ_0 represents the signal-to-noise ratio (SNR) at a reference distance ($d_0 = 1m$) of the ground channels, ζ is an exponentially distributed random variable with unit mean ($\mathbb{E}[\zeta] = 1$), d_{ab} and d_{qb} are the Euclidean distance between Alice, UAV and Bob respectively and P_u is the UAV jamming signal power.

We note that (2.5) is the upper bound of the random complex channel g_B as expressed in [32, eq. (12)]. Thus the channel power gain of Bob (h_B) has been discretised to reflect the discrete interference caused by the UAV jamming signal as represented by the N samples. We also note that the choice of integrals in (2.3) depicts averaging over all channel realisations of Bob and Eve. Clearly, $\int_0^\infty g(h_B) f(h_B) dh_B$ shows that the channel realisation of Bob, h_B , is continuous over an infinite space. However, based on the discrete-time samples of the UAV trajectory, h_B was sampled as shown in (2.5) to represent the channel of Bob under the jamming signal delivered by the UAV at each sampled slot. Hence, assuming slow fading in between slots of the UAV flight time, it is sufficient to find the average in (2.3) under the discrete-time block fading samples as (2.6).

$$R_s = \frac{1}{N} \sum_{n=1}^N \int_0^{h_B[n]} [\log_2(1 + h_B[n] P_A[n]) - \log_2(1 + h_E[n] P_A[n])] f(h_E) dh_E. \quad (2.6)$$

To ensure that the power levels of the communication is within acceptable range, P_u and P_A are subjected to average and peak power constraints described as (2.7).

$$0 \leq P_u[n] \leq P_{umax} \quad (2.7a)$$

$$\frac{1}{N} \sum_{n=1}^N P_u[n] \leq \bar{P}_{ub} \quad (2.7b)$$

$$0 \leq P_A[n] \leq P_{amax} \quad (2.7c)$$

$$\frac{1}{N} \sum_{n=1}^N P_A[n] \leq \bar{P}_{ab}. \quad (2.7d)$$

Equations (2.7a) and (2.7c) limits the power for jamming and the transmit power at each n th slot. And equations (2.7b) and (2.7d) places a limit on the total jamming and transmit power respectively. These limits are necessary to control hazardous impact of transmitting radio signals with excessive power.

2.2.1 Problem Formulation

In this section, we formulate an analytical problem that describes fig. 2.1 using the parameters defined in section 2.2. Let $\mathbf{Q} = \{\mathbf{q}[n], n \in N\}$, $\mathbf{p}_A = \{P_A[n], n \in N\}$, and $\mathbf{p}_u = \{P_u[n], n \in N\}$ be the set of UAV sample points (representing its trajectory from \mathbf{q}_0 to \mathbf{q}_f), the set of power transmitted by Alice as well as the jamming power transmitted by the UAV, respectively.

In order to solve (2.6), we need to know the possible distribution of the fading channel of Eve which can be obtained via historical measurements collected over the region covered by Alice (represented in this model as an ellipse, as in (2.4d)). If we consider that the time-varying complex channel $g_E(t)$ of Eve is normally distributed with mean zero and known variance such that $g_E(t) = g_{E,I}(t) + ig_{E,Q}(t)$, where $g_{E,I}$, $g_{E,Q} \sim \mathcal{C}(0, b_0)$ are the in-phase and quadrature components of $g_E(t)$, then its magnitude, $\alpha(t) = |g_E(t)|$, will be Rayleigh distributed with average envelop power $\mathbb{E}[\alpha^2] = 2b_0 \triangleq y_E$. The instantaneous envelop power is the squared envelop $\alpha^2(t) = |g(t)|^2 \triangleq h_E$.

and is exponentially distributed as

$$f(h_E) = \frac{1}{y_E} e^{-\left(\frac{h_E[n]}{y_E}\right)}, \quad \forall h_E \geq 0. \quad (2.8)$$

Considering block fading within a slot, the channel variations are negligible for the time in between slots, as N becomes very large. Substituting (2.8) in (2.6), we obtain

$$R_s = \frac{1}{N} \sum_{n=1}^N \log_2 (1 + h_B[n] P_A[n]) \left(1 - e^{-\left(\frac{h_E[n]}{y_E}\right)} \right) + \int_0^{h_B[n]} \log_2 (1 + h_E[n] P_A[n]) \left(\frac{1}{y_E} e^{-\left(\frac{h_E[n]}{y_E}\right)} \right) dh_E. \quad (2.9)$$

By applying integration by parts, (2.9) reduces to

$$R_s = \frac{1}{N} \sum_{n=1}^N \underbrace{\log_2(1 + h_B[n] P_A[n])}_{\text{information rate of Bob}} - \underbrace{\int_0^{h_B[n]} \frac{P_A[n] e^{-\left(\frac{h_E[n]}{y_E}\right)}}{1 + h_E[n] P_A[n]} dh_E}_{\text{information rate of Eve}}. \quad (2.10)$$

The secrecy rate in (2.10) can be further simplified with [66, eq. 3.352.1] to (2.11).

$$R_s = \frac{1}{N} \sum_{n=1}^N \log_2(1 + h_B[n] P_A[n]) - e^{\left(\frac{1}{y_E P_A[n]}\right)} \left[E_i \left(-\frac{h_B[n]}{y_E} - \frac{1}{y_E P_A[n]} \right) - E_i \left(-\frac{1}{y_E P_A[n]} \right) \right], \quad (2.11)$$

where $E_i(x) = \int_x^\infty \frac{e^{-t}}{t} dt$ is the exponential integral. We note that (2.10) is equivalent to (2.11) and they can be used interchangeably depending on the parameter been inferred. Thus we substitute the objective function in (2.2) with the elaborated form

in (2.11) to obtain the optimisation problem² as (2.12).

$$\max_{\mathbf{p}_A, \mathbf{p}_u, \mathbf{Q}} \sum_{n=1}^N \log_2(1 + h_B[n]P_A[n]) - e^{\left(\frac{1}{y_E P_A[n]}\right)} \left[E_i \left(-\frac{h_B[n]}{y_E} - \frac{1}{y_E P_A[n]} \right) - E_i \left(-\frac{1}{y_E P_A[n]} \right) \right] \quad (2.12a)$$

$$\text{s.t. } \|\mathbf{q}[n+1] - \mathbf{q}[n]\|^2 \leq (V\delta)^2 \quad (2.12b)$$

$$\|\mathbf{q}[1] - \mathbf{q}_0\|^2 \leq (V\delta)^2 \quad (2.12c)$$

$$\mathbf{q}[N] = \mathbf{q}_f \quad (2.12d)$$

$$\|\mathbf{q}[n] - \boldsymbol{\Omega}_A\| + \|\mathbf{q}[n] - \boldsymbol{\Omega}_B\| \leq 2\varepsilon \quad (2.12e)$$

$$\mathbf{q}(x_n, y_n, z_n) = \mathbf{q}(x_n, y_n, H), \quad (2.12f)$$

$$0 \leq P_u[n] \leq P_{umax} \quad (2.12g)$$

$$\frac{1}{N} \sum_{n=1}^N P_u[n] \leq \bar{P}_{ub} \quad (2.12h)$$

$$0 \leq P_A[n] \leq P_{amax} \quad (2.12i)$$

$$\frac{1}{N} \sum_{n=1}^N P_A[n] \leq \bar{P}_{ab}. \quad (2.12j)$$

Equation (2.12) entails that the secrecy capacity of the proposed system depends on the optimal transmission power of Alice, the jamming power delivered by the UAV and the UAV location. Unfortunately, (2.12) is a non-convex optimisation problem with respect to the optimisation variables $(\mathbf{p}_A, \mathbf{p}_u, \mathbf{Q})$ and cannot be easily solved directly. However, using a sequential and iterative technique under a block coordinate approach, we can obtain suboptimal solutions that satisfy the constraints in (2.4) and (2.7).

²We neglected the constant scaling factor $\frac{1}{N}$ in the objective function as this does not affect the optimal solution.

2.3 Proposed Solution

We propose solving the non-convex (2.12) in an alternating fashion. The proposed solution involves decomposing the original problem, (2.12), into three sub-problems each characterising a set of optimisation variables. In each sub-problem, we optimise one set of variables while fixing the other variables in each iteration. The results obtained from each iteration step are analysed with the objective value of (2.12) and the iteration stops at the point when the objective value (2.12) converges.

2.3.1 Optimising the Source Power (P_A)

We optimise Alice's transmit power for arbitrary initial trajectory and jamming power. Replacing the objective in (2.12) with (2.10), (2.12) can be reformulated for any given \mathbf{Q} and \mathbf{p}_u as (2.13).

$$\max_{\mathbf{p}_A} \sum_{n=1}^N \log_2 (1 + h_B[n]P_A[n]) - \int_0^{h_B[n]} \frac{P_A[n]e^{-\left(\frac{h_E[n]}{y_E}\right)}}{1 + h_E[n]P_A[n]} dh_E \quad (2.13a)$$

$$\text{s.t. (2.12i) and (2.12j).} \quad (2.13b)$$

Note that (2.13) is still non-convex over the entire domain of \mathbf{p}_A . However, for the region under peak and average power constraints, the objective can be shown to be the sum of a concave and a convex functions. The proof is relegated to Appendix A. Since the objective function of (2.13) is differentiable (as demonstrated in Appendix A), it can be solved using the Karush-Kuhn-Tucker (KKT) conditions for non-convex problems [67, section 3.2.1]. We note that the KKT solution is the optimal solution for the non-convex problem only for very large value of N . This is because the *time-sharing* conditions for non-convex problems lead to negligible duality gap only when N is very large [68]. The KKT conditions relevant to the

solution were defined as

$$\nabla f_0(x^*) + \lambda^* \nabla f_n(x^*) = 0, \quad (2.14a)$$

$$\lambda^* f_n(x^*) = 0, \quad (2.14b)$$

where f_0 is the objective in (2.13), f_n are the constraints in (2.12i) and (2.12j) and x^* is the optimal value of P_A . By solving (2.14) using [66, eq. 0.410 and 3.462.17], we obtain (2.15).

$$-\frac{1}{N} \bar{P}_{ab} - \left[\frac{h_B[n]}{1 + h_B[n] P_A[n]} - \frac{1}{y_E (P_A[n])^2} e^{\frac{1}{y_E P_A[n]}} \left[\Gamma \left(-1, \frac{1}{y_E P_A[n]} \right) - \Gamma \left(-1, \frac{h_B[n]}{y_E} + \frac{1}{y_E P_A[n]} \right) \right] \right] \sum_{n=1}^N P_A[n] = 0, \quad (2.15)$$

where $\Gamma(-i, z) = \frac{(-1)^i}{i!} (E_1(z) - e^{-z} \sum_{k=0}^{i-1} \frac{(-1)^k k!}{z^{k+1}})$ [69, eq. 8.4.15]. Solving (2.15) with a non-linear solver produces the suboptimal values of P_A .

2.3.2 Optimising the UAV Jamming Power (P_u)

To optimise the jamming power, \mathbf{p}_u delivered by the UAV, we consider \mathbf{p}_u as the optimisation variable while fixing the values of \mathbf{p}_A and \mathbf{Q} . Equation (2.12) is then reformulated while substituting for $h_B[n]$ as (2.16).

$$\max_{\mathbf{p}_u} \sum_{n=1}^N \log \left(1 + \frac{\rho_0 d_{ab}^{-\psi} P_A[n]}{P_u[n] \rho_0 d_{qb}^{-2}[n] + 1} \right) - e^{\frac{1}{y_E P_A[n]}} \left[E_i \left(-\frac{\frac{\rho_0 d_{ab}^{-\psi}}{P_u[n] \rho_0 d_{qb}^{-2}[n] + 1}}{y_E} - \frac{1}{y_E P_A[n]} \right) - E_i \left(-\frac{1}{y_E P_A[n]} \right) \right] \quad (2.16a)$$

$$\text{s.t. (2.12g) and (2.12h).} \quad (2.16b)$$

Under the constraints, the objective of (2.16) is a non-convex function with respect to \mathbf{p}_u due to the non-convexity of the information rate of the Eve. However, the information rate of Bob is concave with respect to \mathbf{p}_u . Hence, (2.16) can be solved using successive convex approximation (SCA) approach [70, 71]. Note that SCA

(also known as majorisation minimisation) is a popular optimisation approach for solving this type of problems by iteratively solving a locally tight approximation of the original optimisation problem, subject to a tight convex restriction of the constraint sets [71]. Given an initial UAV jamming power in the k -th iteration as $\mathbf{p}_u^k = \{P_u^k[n], n \in N\}$; and using first order Taylor expansion we obtain (2.17).

$$e^{\frac{1}{y_E P_A[n]}} \left[E_i \left(-\frac{\frac{\rho_0 d_{ab}^{-\psi}}{P_u[n] \rho_0 d_{qb}^{-2}[n] + 1}}{y_E} - \frac{1}{y_E P_A[n]} \right) - E_i \left(-\frac{1}{y_E P_A[n]} \right) \right] \leq G_k[n] + T_k[n](P_u[n] - P_u^k[n]), \quad (2.17)$$

where

$$G_k[n] = e^{\frac{1}{y_E P_A[n]}} \left[E_i \left(-\frac{\frac{\rho_0 d_{ab}^{-\psi}}{P_u^k[n] \rho_0 d_{qb}^{-2}[n] + 1}}{y_E} - \frac{1}{y_E P_A[n]} \right) - E_i \left(-\frac{1}{y_E P_A[n]} \right) \right]$$

and $T_k[n] = \frac{P_A[n] \rho_0^2 d_{ab}^{-\psi} d_{qb}^{-2}[n] e^{-\left(\frac{\rho_0 d_{ab}^{-\psi}}{y_E \rho_0 d_{qb}^{-2}[n] P_u^k[n] + y_E}\right)}}{(\rho_0 d_{qb}^{-2}[n] P_u^k[n] + 1)(P_A[n] \rho_0 d_{ab}^{-\psi} + \rho_0 d_{qb}^{-2}[n] P_u^k[n] + 1)}$. Taking only the non-constant terms in (2.17), (2.16) can be reformulated as (2.18).

$$\max_{\mathbf{p}_u} \sum_{n=1}^N \left[\log \left(1 + \frac{\rho_0 d_{ab}^{-\psi} P_A[n]}{P_u[n] \rho_0 d_{qb}^{-2}[n] + 1} \right) - T_k[n] P_u[n] \right] \quad (2.18a)$$

$$\text{s.t. } (2.12g) \quad \text{and} \quad (2.12h). \quad (2.18b)$$

Note that (2.18) maximises the lower bound of the original objective (2.16). Hence, it suffices that the objective value obtained by solving (2.18) is at least equal to the solution obtained by solving (2.16), using the updated P_u^k . As we iterate over k iterations, the Taylor expansion of (2.18), ensures that its objective value is the same as that of (2.16). Equation (2.18) is a convex problem within the constrained region and can be efficiently solved using interior-point method or a convex solver such as CVX [72, 73].

2.3.3 Optimising the UAV Trajectory (\mathbf{Q})

In this sub-problem, the equation (2.12) is recast to ensure that only the UAV trajectory, \mathbf{Q} is the optimisation parameter. However, the reformulated problem is non-convex in \mathbf{Q} . Hence, to reduce computational complexity, we introduce a slack variable $\mathbf{M} = \{m[n] = \|\mathbf{q}[n] - \mathbf{\Omega}_B\|^2, n \in N\}$ such that $d_{qb}^{-2}[n] = \frac{1}{m[n]}$. Thus we obtain the following optimisation problem given as (2.19).

$$\begin{aligned} \max_{\mathbf{Q}, \mathbf{M}} \quad & \sum_{n=1}^N \log \left(1 + \frac{\rho_0 d_{ab}^{-\psi} P_A[n]}{\frac{P_u[n]\rho_0}{m[n]} + 1} \right) - e^{\frac{1}{y_E P_A[n]}} \left[E_i \left(-\frac{\frac{\rho_0 d_{ab}^{-\psi}}{\frac{P_u[n]\rho_0}{m[n]} + 1}}{y_E} - \frac{1}{y_E P_A[n]} \right) \right. \\ & \left. - E_i \left(-\frac{1}{y_E P_A[n]} \right) \right] \end{aligned} \quad (2.19a)$$

$$\text{s.t. } m[n] - \|\mathbf{q}[n] - \mathbf{\Omega}_B\|^2 \leq 0, \quad (2.19b)$$

$$(2.12b) \quad \text{to} \quad (2.12f). \quad (2.19c)$$

Due to the non-convexity of problem (2.19) with respect to the trajectory, $\mathbf{q}[n]$, we reformulate the problem using successive approximation with the first order Taylor expansion. Let $\mathbf{Q}_k[n] = \{\mathbf{q}^k[n], n \in \{1, \dots, N\}\}$ denote the initial UAV trajectory for the k th iteration. Then the non-convex part of the problem given in (2.19) can be rewritten as (2.20) and (2.21) using first order Taylor's expansion.

$$\begin{aligned} e^{\frac{1}{y_E P_A[n]}} \left[E_i \left(-\frac{\frac{\rho_0 d_{ab}^{-\psi}}{\frac{P_u[n]\rho_0}{m[n]} + 1}}{y_E} - \frac{1}{y_E P_A[n]} \right) - E_i \left(-\frac{1}{y_E P_A[n]} \right) \right] \\ \leq O_k[n] + W_k[n](q[n] - q^k[n]) \end{aligned} \quad (2.20)$$

$$-\|\mathbf{q}[n] - \mathbf{\Omega}_B\|^2 \leq S^k[n], \quad (2.21)$$

where

$$O_k[n] = e^{\frac{1}{y_E P_A[n]}} \left[E_i \left(-\frac{\frac{\rho_0 d_{ab}^{-\psi}}{\frac{P_u[n]\rho_0}{m_k[n]} + 1}}{y_E} - \frac{1}{y_E P_A[n]} \right) - E_i \left(-\frac{1}{y_E P_A[n]} \right) \right],$$

$$W_k[n] = \frac{\rho_0^2 d_{ab}^{-\psi} P_u[n] e^{-\frac{\rho_0 d_{ab}^{-\psi}}{y_E \left(1 + \frac{\rho_0 P_u[n]}{m_k[n]}\right)}}}{y_E \left(-\frac{1}{y_E P_A[n]} - \frac{\rho_0 d_{ab}^{-\psi}}{y_E \left(1 + \frac{\rho_0 P_u[n]}{m_k[n]}\right)} \right) \left(1 + \frac{\rho_0 P_u[n]}{m_k[n]} \right) m_k^2[n]},$$

and $S^k[n] = \|\mathbf{q}_k[n]\|^2 - 2[\mathbf{q}_k[n] - \boldsymbol{\Omega}_B]^T \mathbf{q}[n] - \|\boldsymbol{\Omega}_B\|^2$. Under similar conditions as of explained for equation (2.16), equation (2.19) can be reformulated as (2.22).

$$\max_{\mathbf{Q}, \mathbf{M}} \sum_{n=1}^N \log \left(1 + \frac{\rho_0 d_{ab}^{-\psi} P_A[n]}{\frac{P_u[n]\rho_0}{m[n]} + 1} \right) - W_k[n]m[n] \quad (2.22a)$$

$$\text{s.t. } m[n] + S^k[n] \leq 0, \quad (2.22b)$$

$$(2.12b) \quad \text{to} \quad (2.12f). \quad (2.22c)$$

Equation (2.22) is a convex problem in \mathbf{Q} under the specified constraints and can be solved using interior-point methods or with a convex solver.

2.3.4 Overall Procedure

The overall procedure has been summarised in algorithm 1. The convergence of the algorithm 1 was depicted in fig. 2.2. The legend of fig. 2.2 defines “AA 1”, “AA 2” and “AA 3” as the simulation of algorithm 1 for UAV flight times of 300s, 350s and 400s respectively. All other parameters for the simulation was given on table 2.1. It was observed to begin to converge after three iterations for different scenarios of the UAV flight time. This corresponds to the convergence analysis of the scenario where the eavesdropper is active in [31]. Therefore algorithm 1 was guaranteed to converge for all feasible initial points.

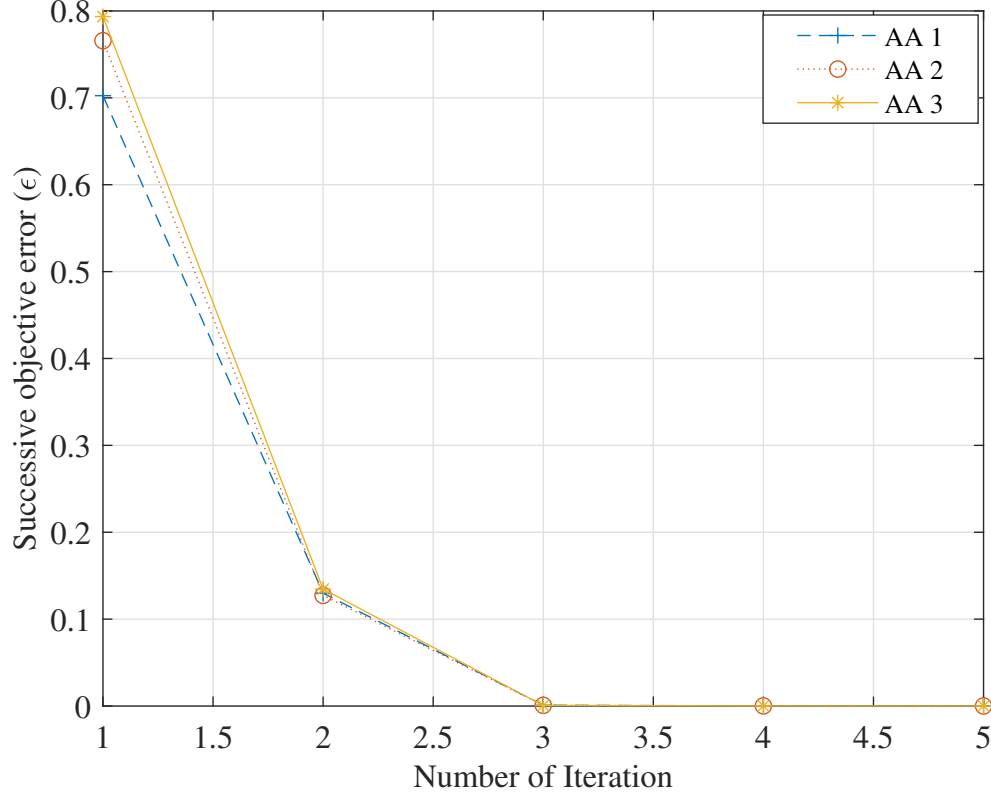


FIGURE 2.2: Convergence analysis of algorithm 1.

Algorithm 1 Iterative algorithm for solving \mathbf{p}_A , \mathbf{p}_u and \mathbf{Q}

- 1: Initialise \mathbf{p}_A^0 , \mathbf{p}_u^0 and \mathbf{Q}^0 such that the constraints in (2.7a), (2.7b) and (2.4) are satisfied.
 - 2: $m \leftarrow 1$.
 - 3: **repeat**
 - 4: Compute and update \mathbf{p}_A^m in (2.15) with given \mathbf{p}_u^{m-1} and \mathbf{Q}^{m-1} .
 - 5: Using updated \mathbf{p}_A^m and current \mathbf{Q}^{m-1} , solve (2.18) for \mathbf{p}_u^m .
 - 6: With given \mathbf{p}_A^m and \mathbf{p}_u^m , find \mathbf{Q}^m by solving problem (2.22).
 - 7: Compute R_s^m as defined in (2.11).
 - 8: $\epsilon = \left| \frac{R_s^m - R_s^{m-1}}{R_s^m} \right|$.
 - 9: $m \leftarrow m + 1$.
 - 10: **until** $\epsilon < 10^{-5}$ OR $m \geq 200$.
 - 11: **Output:** \mathbf{p}_A^m , \mathbf{p}_u^m , and \mathbf{Q}^m .
-

2.4 Simulation Results and Analysis

In this section, we evaluate the performance of the proposed solutions through numerical simulations. We implement the solution discussed in section 2.3 following the procedure described in algorithm 1. The optimisation parameters were initialised by solving the feasibility problem such that the the initial values satisfy their respective constraints. The feasibility problem was formulated by setting the objective of problem (2.12) to zero, with all the primary constraints unchanged. The solution to the variables obtained from the feasibility problem were used as the starting point to the iterative algorithm. By iteratively optimising each parameter with the knowledge of the others, we obtain the suboptimal solution to (2.12) when the error (ϵ) between steps is less than 10^{-5} or the maximum number of iterations (200) was reached.

In all the simulations, we used the parameters as described in table 2.1 unless otherwise specified in the caption of the figures. The legend used in the figures describe the various scenarios implemented as follows:

(a) For fig. 2.3, the legend is described as follows:

- (i) P_A : Refers to the optimised transmitted power from Alice (Source).
- (ii) P_u : Refers to the optimised jamming power delivered from the UAV.

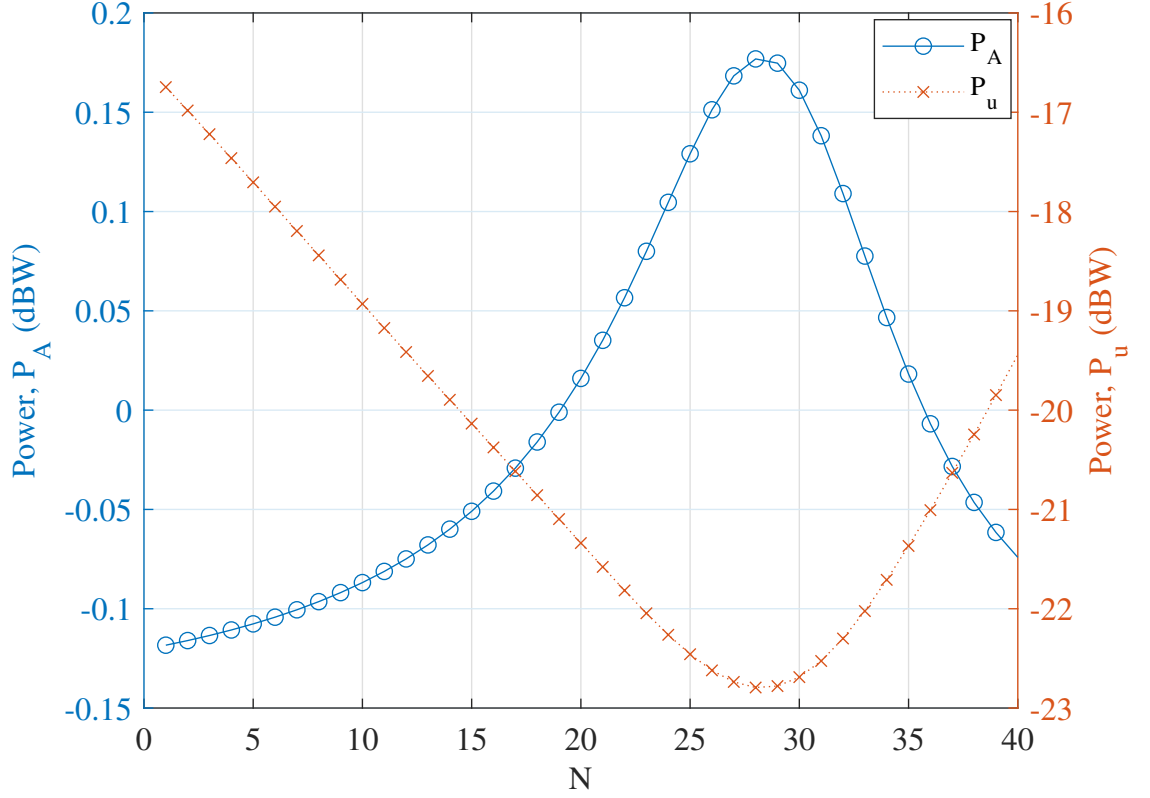
(b) For fig. 2.4, the legend is described as follows:

- (i) “AA” refers to the proposed solution to the passive eavesdropper problem with 300m Euclidean distances between Alice and Bob.
- (ii) “BB” refers to the scenario where the eavesdropper’s location was known as considered in [29]. The attached numbers represents scenarios with varying distances of Eve from Alice. We have that “BB 1”, “BB 2”, “BB 3”, “BB 4” represent the scenarios of 291.5m, 350m, 300.7m and 308.1m Euclidean distance between Alice and Eve. In these scenarios, the location of Bob fixed. The geometric locations of the eavesdropper tested for this scenario were specified in table 2.1.

- (iii) Straight refers to a straight flight of the UAV from the start to final destination (no trajectory optimisation).
- (c) From figs. 2.5 to 2.10: “AA 1”, “AA 2”, “AA 3”, “AA 4”, “AA 5” and “AA 3” refers to the simulation of proposed passive eavesdropping solution (algorithm 1) for UAV flight times of 200s, 250s, 300s, 350s, 400s and 450s respectively. The use of the legend depends on the simulated scenarios.

TABLE 2.1: Simulation parameters for jamming of obscured eavesdropper

Simulation parameter	Symbol	Value
Alice location	Ω_A	$[0, 0, 0]$
Bob location	Ω_B	$[300, 0, 0]$
Eve location	Ω_E	$[150, 250, 0], [350, 0, 0], [300, 20, 0], [300, 70, 0]$
Initial UAV location	\mathbf{q}_0	$[-100, 100, H]$
Final UAV location	\mathbf{q}_f	$[500, 100, H]$
UAV height(when fixed)	H	100m [29]
Velocity per sample(when fixed)	Z	3m/s [29]
Duration per sample(when fixed)	δ	0.5s [29]
SNR	ρ_0	90dB [29]
Average received envelop power	y_E	20dBm
Average UAV transmit power	\bar{P}_{ub}	10dBm [29]
Maximum UAV power	P_{umax}	$4\bar{P}_{ub}$ [29]
Average Source power	\bar{P}_{ab}	30dBm [29]
Maximum source power	P_{amax}	36dBm [29]
Radius of uncertainty region (when fixed)	ε	450m
Path loss for ground communication (urban area cellular radio)	ψ	3.4


 FIGURE 2.3: Comparing transmitted power from Alice and UAV for $T = 20$ s.

In the analysis of the performance of the design of the jamming parameters, we first examine the relation between the optimised transmitted powers - that is power from the source (Alice) and the UAV jammer. The transmitting power of Alice (P_A) and the UAV jamming power (P_u) were plotted in fig. 2.3. We notice from fig. 2.3 that when P_A increases, P_u decreases, and vice versa. The powers were inversely related. The UAV jammer transmits more when it is far from its optimal position. This means that it will also cause more interference at the legitimate receiver (Bob), hence, the transmitter (Alice) reduces its transmission. When the UAV hovers at the best location to deliver the jamming signals, Alice then transmits more while the jamming can be carried out with less power. The lowering of the jamming power ensures that the interference at the legitimate receiver was reduced.

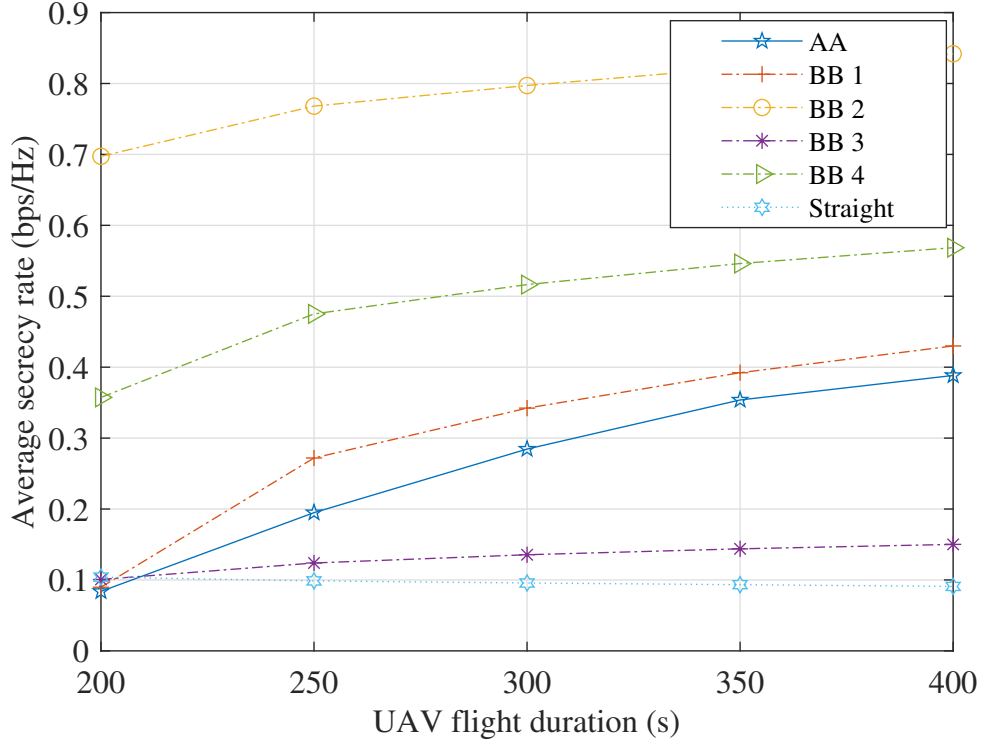


FIGURE 2.4: Average secrecy rate with ‘unknown’ as well as ‘known’ eavesdropper locations, and direct UAV flight path.

Furthermore, we analyse the secrecy rate performance of the proposed scheme and compared it with existing schemes. In fig. 2.4, the performance of the unknown Eve location scenario using the proposed joint trajectory and power optimisation algorithm (“AA”) was compared to the scenario where Eve location was known (“BB”). We also compared with a baseline scheme, referred to as “Straight”, without optimising the UAV trajectory. We make the following observations from fig. 2.4:

1. The direct flight path with constant power (Straight) scheme performs the worst in terms of the average secrecy rate. The UAV hovers at the centre of the uncertain region of the eavesdropper. Hence, the trajectory of the UAV was not optimised for this scenario causing the jamming signals to interfere with the legitimate receiver (Bob) and the eavesdropper (Eve) equally or worse for Bob depending on the unknown location of Eve.

2. When we consider the “BB” scheme where the eavesdropper’s location was known, it was observed that when the eavesdropper was close to the legitimate receiver (Bob), the secrecy rate was low (slightly above the straight scheme). However, as the eavesdropper moves away from the legitimate receiver (either towards Alice or away from Alice), an increase in the average secrecy rate was observed. This is because the UAV can track the eavesdropper and deliver the required jamming signal. Therefore for “BB 2”, we observe high secrecy rates compared to the other schemes.
3. Comparing these schemes to the scenario where the eavesdropper’s location was unknown, we see that the average secrecy rate was not dependent on the location of the eavesdropper. Furthermore, the secrecy rates were positive and higher than the “BB” schemes where the eavesdropper was close to the legitimate receiver.

It is important to note that the information rates of both Bob and Eve were affected by the jamming signal of the UAV. However, Eve was affected more, even when it has better channel condition (measured in terms of its average received envelope power). This is because the UAV regularly finds paths such that it stays further from Bob and estimates as close to Eve as possible until it flies to its final point. We show the trajectory of the UAV for the “AA” scheme in fig. 2.5.

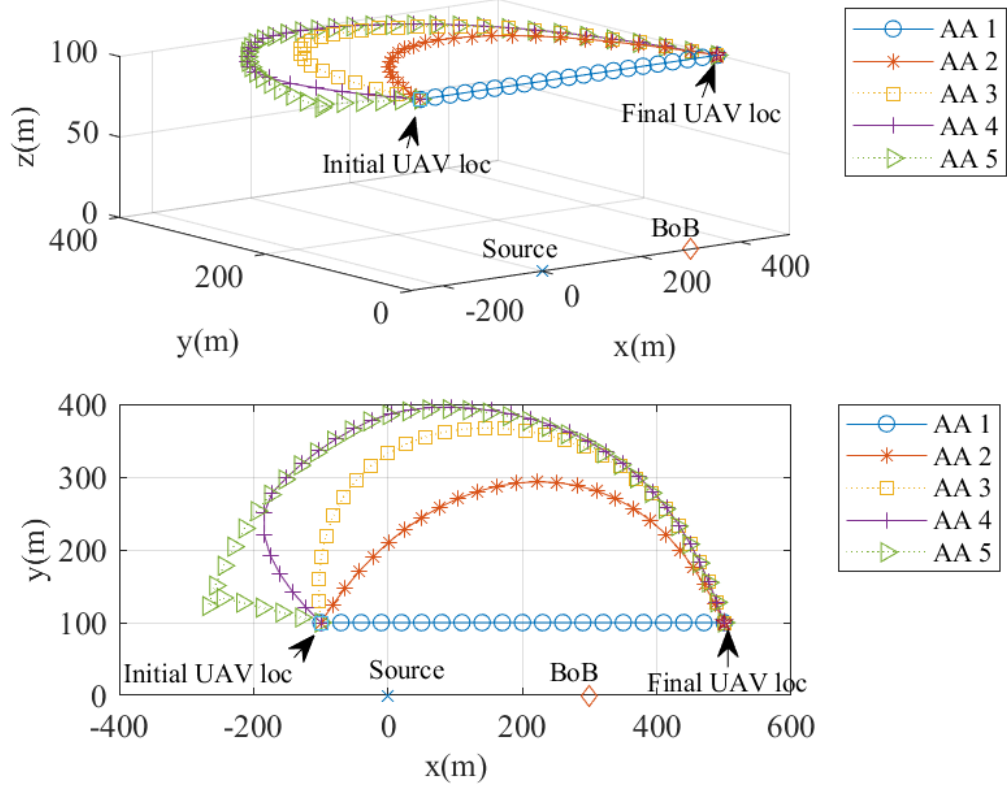


FIGURE 2.5: UAV flight trajectory in 2D and 3D view while Eve location is unknown (For clarity, we use $\delta = 10$).

The flight trajectory of the UAV with respect to Alice and Bob was shown in fig. 2.5. The 2D plot shows that from an aerial view, the trajectory of the UAV follows a given pattern bound by the uncertainty region of Eve provided it flies at a constant altitude. For clarity, the 3D plot shows that the UAV trajectory moves towards the opposite of Bob while ensuring that the jamming signal is still delivered to all points within the constrained region of Eve.

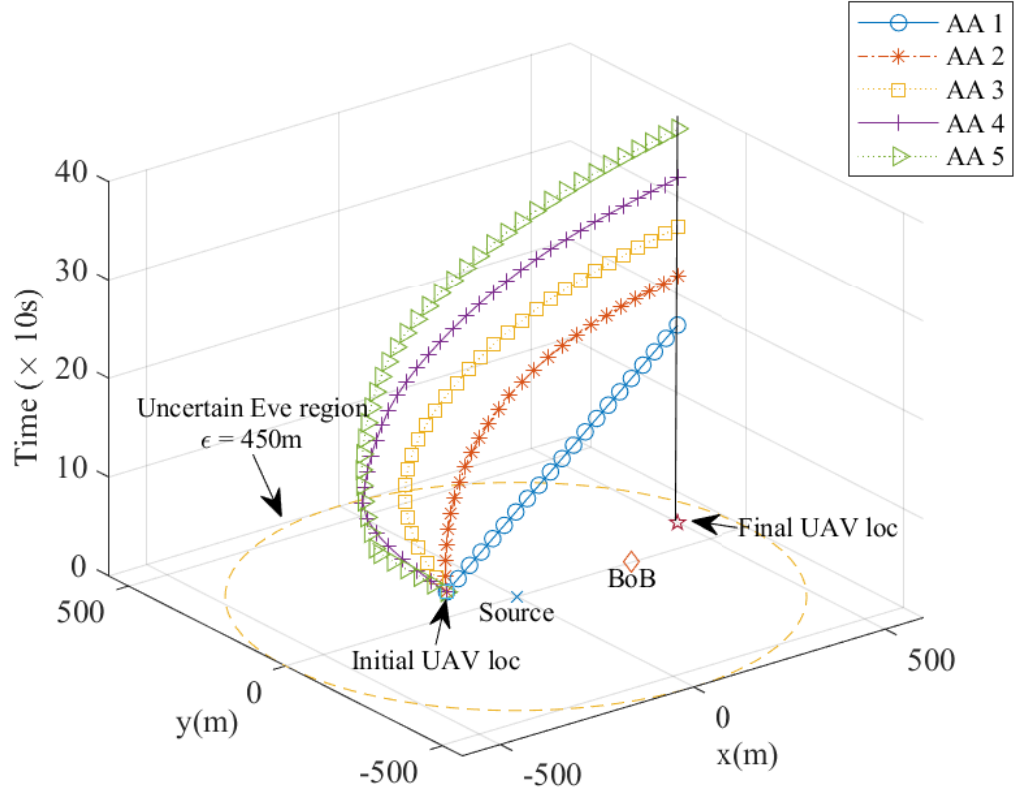


FIGURE 2.6: UAV flight trajectory as a function of time (For clarity, we use $\delta = 10$).

In fig. 2.6, the trajectory of the UAV was plotted with respect to time. It is clear from the figure that the UAV traces its path to an optimal area, and then hovers around this area until it returns to the final destination.

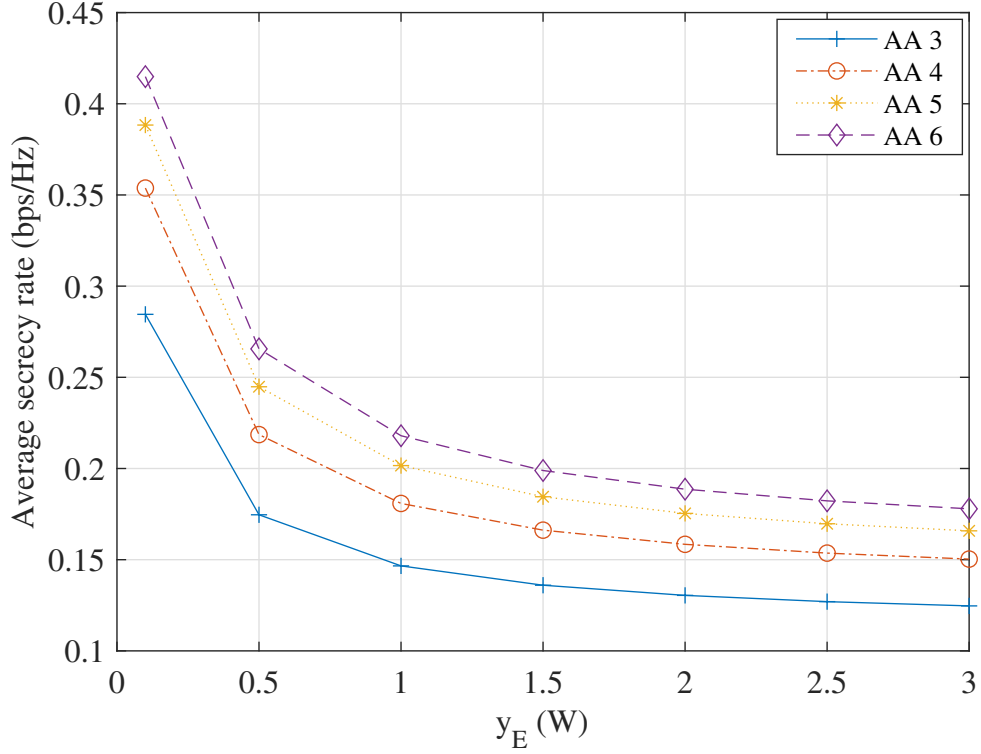


FIGURE 2.7: Effect of average received envelop power of Eve on average secrecy rate.

Figure 2.7 examines the constraints posed by the assumptions on the property of Eve's channel. We recall that the only known property of Eve is its average received envelop power, y_E . Hence fig. 2.7 presents the effect of varying y_E on the average secrecy rate. It was observed that increase in y_E decreases the average secrecy rate via a positive exponential path. Therefore, for large values of y_E , characterising Eve having better reception equipment and channel compared to Bob, the change in average secrecy rate with respect to increasing y_E becomes negligible. The optimised UAV path delivering jamming signals ensures that even when the location of Eve was unknown, the average secrecy rate of the communication between Alice and Bob was guaranteed even if Eve was supposedly receiving signals with high envelope power. While this average secrecy rate is low, it can be improved by increasing the time of flight of the UAV as shown in figs. 2.4.

Other factors that affect the average secrecy rate in the considered scenario of passive eavesdropping include the UAV height and speed, and the SNR of the environment. Figures 2.8, 2.9 and 2.10 show the average secrecy rate of the proposed system compared to the UAV altitude, speed and ground node SNR, respectively. The information rate of Eve increases with its proximity to the source. This acts as a measure of better channel quality since the channel obeys inverse square law. However, the rate is bound by the information rate of Bob as designed in the problem formulation.

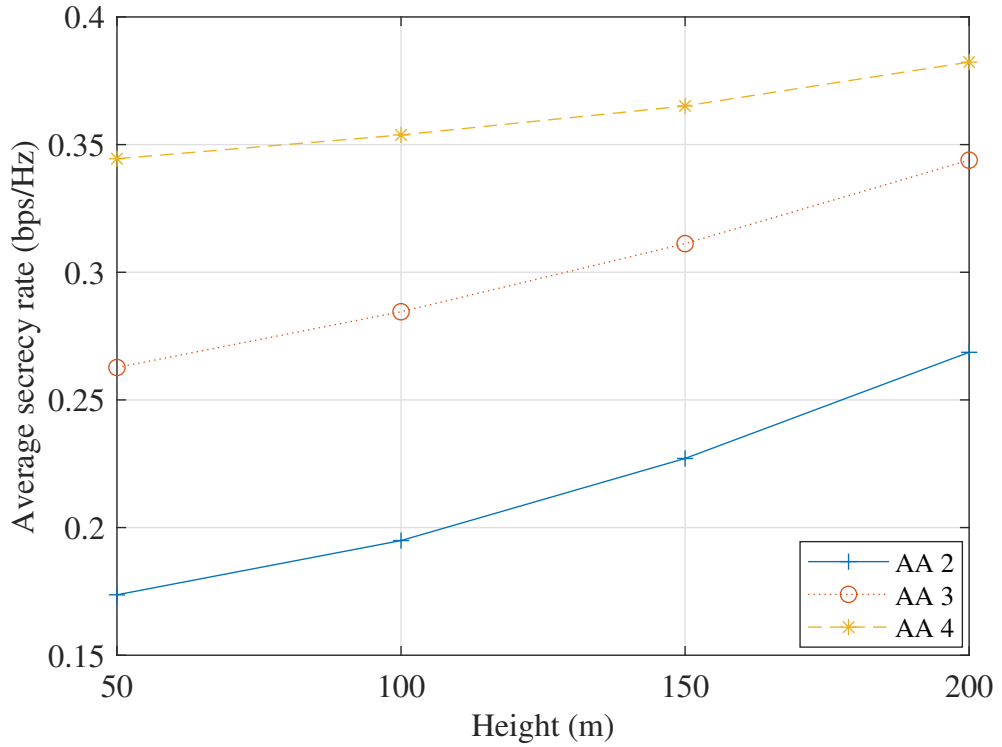


FIGURE 2.8: Influence of UAV altitude (height) on average secrecy rate under the proposed scheme.

The trend in fig. 2.8 suggests that the average secrecy rate increases with increase in the UAV altitude/height for different flight times. However, we observed from our simulations that for large values of UAV flight altitude, the trajectory optimisation problem ((2.22)) becomes infeasible. The observation follows from the LoS link established between the UAV delivering the jamming signal, and the ground nodes.

Since high altitude helps with better LoS, but too high altitude leads to connection difficulties.

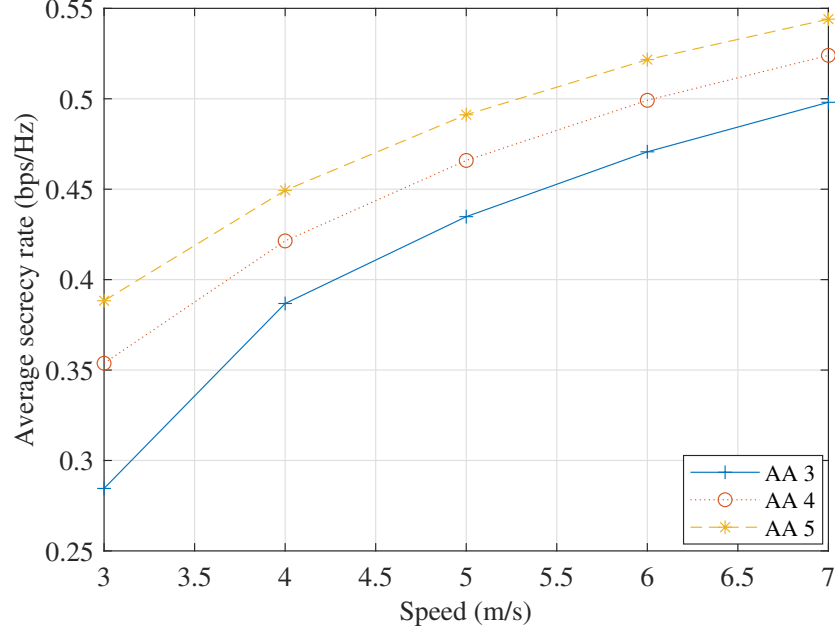


FIGURE 2.9: Influence of UAV flying speed on average secrecy rate with obscure Eve.

It was interesting to observe from fig. 2.9 that increasing the UAV speed increase the average secrecy rate. As the UAV speed increases, its sample points increase allowing it to deliver more jamming signal to Eve within its flight time. Similar to results observed in [65]. By increasing the time of flight of the UAV, with increasing speed, the average secrecy rate is higher. Recall from the trajectory of the UAV given in fig. 2.5, the UAV hovers when it gets to the point where it can deliver the jamming signals successfully. Therefore, increasing the speed of flight helps the UAV arrive at the hover point and spend more time delivering the jamming.

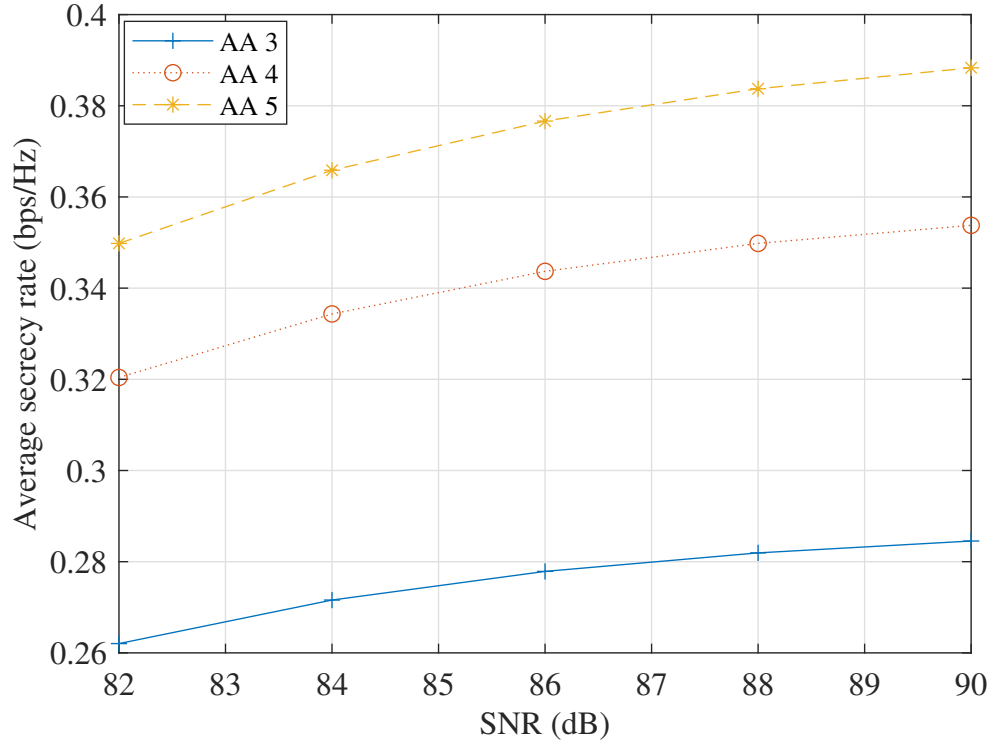


FIGURE 2.10: Average secrecy rate versus signal-noise-ratio (SNR) with obscure Eve.

Figure 2.10 examines the impact of varying the SNR of the ground nodes in the average secrecy rate. It is clear that for higher SNR, the average secrecy rate increases. We note that although the ground SNR improves the secrecy, this parameter is subject to characteristics of the environment which cannot be easily controlled.

2.5 Chapter Summary

In this chapter, a method for minimising the amount of information leaked to a passive eavesdropper was investigated using jamming signals delivered from a UAV. We first formulated a description for the average secrecy rate as a measure of PLS for the UAV-aided jammer under passive eavesdropping. Using the formulation, we defined a non-convex optimisation problem in terms of key adjustable parameters.

The solution to the formulated problem obtained the numerical values of the parameters - UAV trajectory, transmission power and UAV jamming power. These solution were obtained using an iterative sequential algorithm. When the passive eavesdropper was confined to a defined space, we showed that positive secrecy rate can be maintained. The results presented in the chapter also showed that the speed of the UAV and the length of time it is on-flight allows more delivery of the jamming signals. Therefore, both variables aids the positive average secrecy rate. We also demonstrated that even when the eavesdropper has better channel conditions depicted by the high envelop power, the jamming signal degrades the quality, thereby offering better PLS. However, the average secrecy rates were not comparable to designs where we know the location of the eavesdropper especially if the location is far from the legitimate receiver. Nevertheless, the solutions presented in this chapter shows positive average secrecy rate and inspires a search for methods to improve on it.

Chapter 3

Physical Layer Security Improvement with UAV Swarm

The chapter investigate the design of a grid structured set of UAVs in a swarm formation for maximising the secrecy rate in the presence of a passive eavesdropper. Following the possibilities observed when delivering jamming signals from a UAV in chapter 2, this chapter extends the application to the gridded swarm of UAVs. Section 3.1 describes from literature, the research contribution of the chapter. It reviews current literature leading to the system model and analytical formulation of the problem in section 3.2. The methodological approach to solving the problem was given in section 3.3. Furthermore, section 3.4 focuses on the results obtained from numerical simulation of the solution developed. The chapter concludes with a summary in section 3.5.

3.1 Existing Techniques and Discussions

Due to aerial visibility, ease of maneuvering and cost effectiveness, the UAV is rapidly becoming a preferred choice for on-demand wireless communication applications [74, 75]. The benefits accruing to the use of a single UAV as observed in several wireless communication applications can be extrapolated with the use of multiple

UAVs, popularly called UAV swarm [40, 63, 76]. For example, the use of a single UAV to deliver jamming signals studied in chapter 2 of this thesis can be extended to a swarm of UAVs.

However, the use of UAV swarm is marred by the overhead in its control logistics. The control mechanism of the UAV swarm has been discussed in [34, 38, 41, 77] for different applications in order to characterise the trade-off between design complexity and performance. In this chapter, we explore the complexity and performance trade-off for the deployment of the UAV swarm for PLS.

Let us recall from chapter 2 that PLS uses the dynamic intrinsic properties of wireless communication channels to support the legitimate receiver's signal while reducing the information content received by the eavesdropper(s) [76]. Although PLS can be traced to Shannon's theorem [18], PLS optimisation methods have been recently broadened to the use of UAVs [29, 32, 56, 65]. An elaborate discussion on the systematic research progression that established the foundation for the design for PLS was performed in [10, 13] and summarised in chapter 2.

Subsequently in chapter 2, UAV-aided jamming technique for enabling PLS in ground station with a passive eavesdropper was discussed. The unknown eavesdropper location was assumed to be within a closed path characterising the coverage region of the transmitter. Although this work guaranteed positive secrecy rate for the unknown eavesdropper CSI, the secrecy rates reported were relatively low, hence, the need for capacity improvement.

Following positive results from single UAV use-case scenarios for PLS, explorations of techniques to increase the secrecy rate led to the deployment of multiple UAVs in form of a swarm for PLS. The UAV swarm is simply a collection of independent flying UAVs that are autonomous but interact reactively to produce an aggregated behaviour [34, 41]. The theoretical framework for the relationship between the UAV swarm and the ground base station was proffered in [78]. In [40], the UAV swarm tracked the movement of the eavesdropper to jam its received signal while maximising the secrecy rate of the main receivers. The location of the eavesdropper

was assumed to be known and the formation geometry of the UAV swarm was not considered contrary to the specifications suggested in [77, 78]. However, without considering an ordered formation of the UAV swarm, the optimised beamforming weights are not guaranteed to produce a beam pattern [78, 79]. This implies that due to the sparsity of the unordered formations, coordinate beamforming that generates a single wide beam to cover the eavesdropper's region cannot be obtained. Nevertheless, distributed beamforming can be attained if the eavesdropper is active. Alternatively, deploying the unordered formed UAVs to manage a specific area within the region leads to pocket black regions where the eavesdropper can evade the jammers. Therefore, in this chapter, we considered a grid arrangement for the UAV swarm with passive eavesdropper in order to increase the secrecy rate via coordinated jamming. Simulation results demonstrate the better performance of the proposed grid-structured UAV swarm approach compared to conventional approaches. The technical contribution of this chapter can be characterised in terms of seeking the answers to the following questions:

- (a) What is the position of the each member of the UAV swarm at any given time?
- (b) How to harness the properties of the UAV swarm to improve on the average secrecy rate?

These questions as enumerated are correlated and are answered within the general principles of controlling the UAV swarm and beamforming design as discussed in this chapter.

3.2 System Model and Problem Formulation

Let us consider a scenario in which a transmitter (Alice) wants to send a confidential message to a legitimate receiver (Bob) in the presence of an eavesdropper (Eve). A group of K UAVs coordinate their jamming signals to ensure worst channel state of

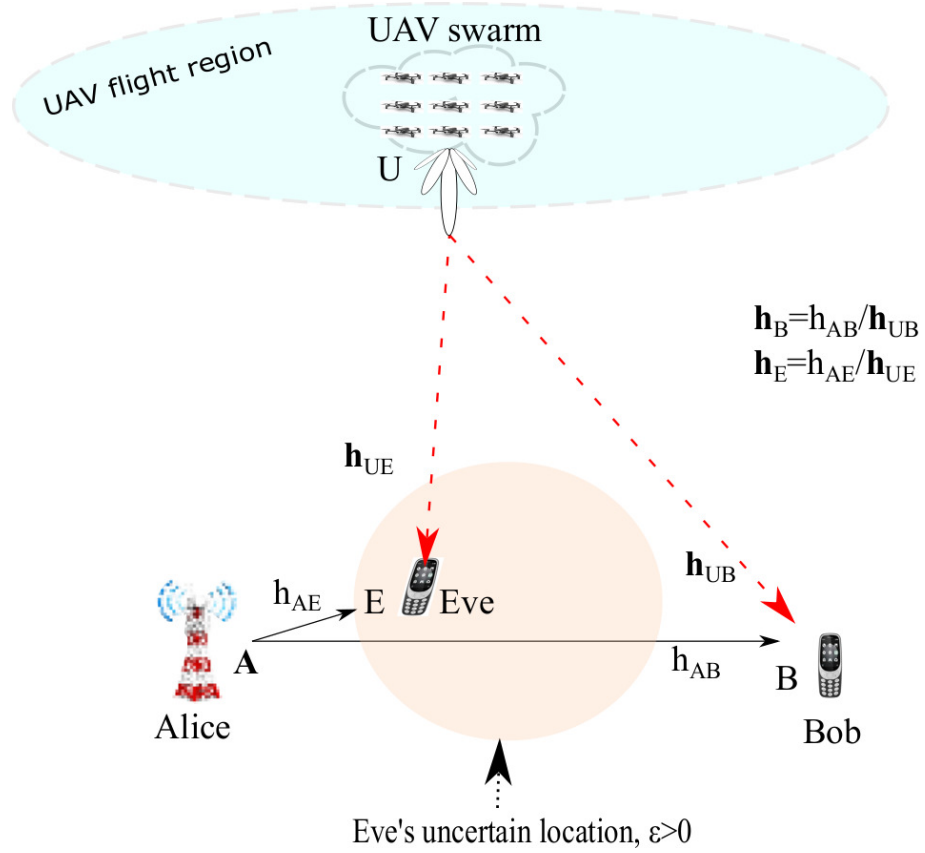


FIGURE 3.1: UAV Swarm interaction with ground stations

Eve despite its unknown location without tampering the channel of Bob. A pictorial representation is given in fig. 3.1.

Without loss of generality, we assume that the UAVs fly at constant altitude, H and with maximum speed of $Z\text{m/s}$ for each δ seconds giving rise to a trajectory represented as $\mathbf{Q} = \{\mathbf{q}_k[n], n \in N \ \& \ k \in K\}$. The received signal at Bob (B) and Eve (E) in the n -th time-slot is given by (3.1).

$$r_i[n] = h_{Ai} \underbrace{w_A s}_{x_A} + \sum_{k=1}^K (h_{ki}[n] \underbrace{w_k[n] \bar{s}[n]}_{x_k[n]}) + n_i[n], \quad \forall i \in \{B, E\}, \quad (3.1)$$

where n_i for $i \in \{B, E\}$ is an independent and identical (iid) additive Gaussian white noise (AGWN) signal received by Bob or Eve with $\sim \mathcal{C}(0, \sigma_i)$, h_{Ai} is the complex channel gain between Alice and either Bob or Eve while x_A and x_k represents the uncorrelated transmission symbols (s) and jamming signals (\bar{s}), respectively. We

also assume that $\mathbb{E}[|x_A[n]|^2] = \sigma_A^2 = 1$. This implies that the transmit power from Alice is scaled with the channel gain.

Having prior knowledge of the channel of Bob, we design the jamming signal such that Bob remains in a region free from it. This is achieved by nulling the jamming signal on the channel of Bob for each $n \in \{1, \dots, N\}$. Such that the beamforming coefficient (w_k) for each UAV was chosen to ensure that $\mathbf{h}_B^T \mathbf{w} = 0$, where $\mathbf{h}_B = [h_{1B}, \dots, h_{KB}]^T$ and $\mathbf{w} = [w_1, \dots, w_K]^T$. This ensures that \mathbf{w} lies in the null space of \mathbf{h}_B . Nevertheless, since the UAV swarm will continue to jam Eve at every possible location within the described uncertainty region, it will imply that $\mathbf{h}_E^T \mathbf{w} \neq 0$ for $\mathbf{h}_E = [h_{1E}, \dots, h_{KE}]^T$.

Furthermore, we define the channel impulse response between the k th UAV and the ground stations, $i \in \{B, E\}$ as (3.2) from [78].

$$h_{ki} = c_k e^{j\phi_k} \delta(t - \tau_k), \quad (3.2)$$

where $\phi_k = (\omega_c + \omega_d)t - \omega_d \tau_k$ is the phase shift due to Doppler effect ω_d and time delay τ_k ; c_k is the large scale channel effect due to path loss and shadowing. We assume that there is a line of sight (LoS) communication link between the UAV swarm and the ground stations (Bob and Eve), hence $c_k[n] = \rho_0 \zeta \|\mathbf{q}_k[n] - \boldsymbol{\Omega}_i\|^{-2}$, where ρ_0 represents the channel power gain at reference distance $d_0 = 1$ m and ζ is an exponential random variable with unit mean [29, 56, 76].

Assuming that $\mathbb{E}[|x_A[n]|^2] = \sigma_A^2 = 1$. The implication of this assumption is that the transmit power from Alice is fixed and will subsequently not be optimised for either Bob or Eve. Alice is considered to transmit equally in all directions using an omni-directional antenna. Since the location of Eve is unknown, varying the transmit power of Alice is not necessary in this scenario. This is because, Eve can be closer to Alice than Bob which implies that any value of the transmitting power of Alice will always contribute to improve the information content received by Eve. We note that the emphasis is to ensure that the channel quality of Eve is scrambled

such that it receives little or no information from Alice while limiting the impact of the jamming on Bob. Accordingly, the signal to interference plus noise ratio (SINR) at Bob and Eve is given by (3.3a) and (3.3b) respectively.

$$\gamma_B = \frac{|h_{AB}|^2}{\sigma_{AB}^2}, \quad (3.3a)$$

$$\gamma_E[n] = \frac{|h_{AE}|^2}{\sum_{k=1}^K (|h_{ke}[n]x_k[n]|^2) + \sigma_E^2}, \quad (3.3b)$$

where h_{Ai} is Rayleigh distributed with gain of $\mathbb{E}[|h_{Ai}[n]|^2] = \rho_0 \zeta \|\mathbf{\Omega}_A - \mathbf{\Omega}_i\|^{-\psi}$ for $i \in \{B, E\}$ and ψ is the pathloss [29]. Since Alice does not adjust its transmission rate because it is ignorant of Eve and the UAV swarm transmits in the null space of Bob, the channel between Alice and Bob was not affected by the samples of the UAV jamming signals. This is why, (3.3a) is not dependent on n .

Following the SINR given in (3.3), the average secrecy rate defined as the difference in the information rate between Bob and Eve is given in (3.4) [5, 29].

$$R_s = \frac{1}{N} \sum_{n=1}^N [\log_2(1 + \gamma_B) - \log_2(1 + \gamma_E[n])]^+, \quad (3.4)$$

The guarantee of positive secrecy was maintained by setting the power of the transmitter (Alice) to zero when the CSI of Eve is greater than the CSI of Bob. However, if we consider a more realistic scenario where Alice is ignorant of Eve, then it cannot adjust its power based on the CSI of Eve, which may invariably lead to negative secrecy rate if Eve has better CSI than Bob. Hence, the objective of this work is to ensure that the negative secrecy rate is completely mitigated even for cases when Alice is ignorant of Eve with the aid of UAV swarm jamming. If we assume that the uncorrelated jamming symbols have unity energy, we aim to maximise R_s in (3.4) by finding the appropriate \mathbf{w} and \mathbf{Q} which represents the beamforming vectors and UAV swarm trajectory respectively.

To simplify the trajectory problem, let us consider centralised grid swarm control where one element of the swarm is classified as the head of the swarm $\mathbf{q}_c = [x_c, y_c, H]$ [34]. Other elements are distributed in a grid form within a predefined width from

the head. This enables the optimisation of only the trajectory of the head of the UAV swarm through the optimisation process under the constraints in (3.5).

$$\|\mathbf{q}_c[n+1] - \mathbf{q}_c[n]\|^2 \leq (Z\delta)^2, \quad (3.5a)$$

$$\mathbf{q}_c[N] = \mathbf{q}_f. \quad (3.5b)$$

Equation (3.5a) provides the upper bound for the maximum distance covered by the UAV swarm head within a sample period, while (3.5b) constrained its final destination. The direct implication of (3.5a) ensures that the time of flight of the UAV is lower bound by $T \geq \frac{\|\mathbf{q}_f - \mathbf{q}_0\|}{Z}$, where \mathbf{q}_f and \mathbf{q}_0 represents the final and initial trajectory of the UAV head. This means that the number of discrete time-stamps, $N = \frac{T}{\delta}$, must be sufficient to allow the UAV travel at least in a straight line from its initial to its final point. However, this trajectory is not guaranteed to be optimal in terms of maximising the secrecy rate.

The UAV swarm transmit power is bound by the peak and average power constraints given in (3.6) due to the limited capability of each individual UAV payload and power.

$$\text{Tr}(\mathbf{w}[n]\mathbf{w}[n]^H) \leq \bar{P}_{\text{tot}}, \quad (3.6a)$$

$$0 \leq |\mathbf{w}_k|^2 \leq P_{\text{max}}, \quad (3.6b)$$

where P_{max} and \bar{P}_{tot} represents the maximum power transmitted by a single UAV in the swarm and the average power transmitted by the UAV swarm respectively. (3.6b) constrains the minimum and maximum value of the jamming power while (3.6a) bounds the collective power radiated from the UAV swarm at each $n \in \{1, \dots, N\}$ to minimise external interference. Subsequently, we formulate the UAV swarm problem

as (3.7).

$$\max_{\mathbf{w}, \mathbf{q}} R_s \quad (3.7a)$$

$$\text{s.t. } \mathbf{h}_B^T[n] \mathbf{w}[n] = 0, \quad (3.7b)$$

$$\text{Constraint (3.5) and (3.6).} \quad (3.7c)$$

We note that the problem in (3.7) is solvable with perfect knowledge of both the channels of Bob and Eve by solving the semi-definite program (SDP) with successive convex approximation (SCA). Nevertheless, we consider that the location of Eve is unknown but within a circular region bound by ε .

Therefore, similar to [80], we define the exact location of Eve ($\mathbf{\Omega}_E$) as a point on a circular uncertain region such that

$$\mathbf{\Omega}_E = \hat{\mathbf{\Omega}}_E \pm \Delta\mathbf{\Omega}_E, \quad (3.8a)$$

$$\|\pm \Delta\mathbf{\Omega}_E\| = \|\mathbf{\Omega}_E - \hat{\mathbf{\Omega}}_E\| \leq \varepsilon, \text{ for } \varepsilon \geq 0, \quad (3.8b)$$

$$\|\Delta\mathbf{\Omega}_E\| \leq \varepsilon, \quad (3.8c)$$

holds true, where $\hat{\mathbf{\Omega}}_E$, $\Delta\mathbf{\Omega}_E$ and ε define the estimated location of Eve, the error of the estimation and the radius of error, respectively. Hence, we can estimate the exact location of Eve with a maximum error of ε

3.3 Proposed Solution

To solve (3.7), we decompose the problem into a two sub-problems describing the beamforming vectors and the UAV swarm trajectory. The original problem (3.7) can be solved iteratively between the sub-problems to obtain the sub-optimal/near optimal results that satisfy the constraints as used in [29, 76, 81].

3.3.1 Solving for Beamforming Vectors

Since the power transmitted by the UAV swarm at each n -th sample of the trajectory is independent of other samples, the problem in (3.7) can be simplified by obtaining the values of w_k for each n . Hence, we can rewrite (3.7) for each $n \in \{1, \dots, N\}$ as (3.9), by considering only constraints that relates to beamforming vectors.

$$\max_{\mathbf{W}} \log_2 \left(1 + \left(\frac{|h_{AB}|^2}{\sigma_B^2} \right) \right) - \log_2 \left(1 + \left(\frac{\frac{1}{\sigma_E^2} |h_{AE}|^2}{\frac{1}{\sigma_E^2} (\mathbf{h}_E^T \mathbf{W} \mathbf{h}_E)[n] + 1} \right) \right), \forall n \quad (3.9a)$$

$$\text{s.t. } (\mathbf{h}_B^T \mathbf{W} \mathbf{h}_B)[n] = 0, \quad (3.9b)$$

$$\text{Tr}(\mathbf{W}[n]) \leq \bar{P}_{\text{tot}}, \quad (3.9c)$$

$$\text{diag}(\mathbf{W}[n]) \leq P_{\text{max}}, \quad (3.9d)$$

$$\text{rank}(\mathbf{W}[n]) = 1, \quad (3.9e)$$

where (3.9d) is a reformation of (3.6b) and (3.9e) is a corollary of $\mathbf{W} = \mathbf{w}\mathbf{w}^H$. Note that (3.9b) is a condition necessary to fulfil the nulling of the channel of the main receiver, Bob. Hence, we desire to find some \mathbf{w} such that (3.9b) will be satisfied. For simplicity, we satisfy this condition by obtaining a set of complex vectors, \mathbf{v} , such that $\mathbf{w} = \{\mathbf{v} | \mathbf{h}_B^H \mathbf{v} = 0\}$. \mathbf{v} becomes the projection vector onto the subspace of \mathbf{w} . Hence, $\mathbf{w} = \mathbf{H}_\perp \mathbf{v}$; where \mathbf{H}_\perp is the transformation matrix for the projection of \mathbf{v} on \mathbf{w} . It is apparent that $\mathbf{W} = \mathbf{H}_\perp \mathbf{v}(\mathbf{H}_\perp \mathbf{v})^H = \mathbf{H}_\perp \mathbf{v}\mathbf{v}^H \mathbf{H}_\perp^H$ ([82, eq. 1.9]). Let $\mathbf{V} = \mathbf{v}\mathbf{v}^H$, using [82, eq. 1.1.17] and omitting $n \in \{1, \dots, N\}$ for notational simplicity, (3.9) can be reformulated as

$$\max_{\mathbf{V}} \log_2 \left(1 + \left(\frac{|h_{AB}|^2}{\sigma_B^2} \right) \right) - \log_2 \left(1 + \left(\frac{\frac{|h_{AE}|^2}{\sigma_E^2}}{\frac{1}{\sigma_E^2} \text{Tr}(\mathbf{h}_E \mathbf{h}_E^T \mathbf{H}_\perp \mathbf{V} \mathbf{H}_\perp^H) + 1} \right) \right), \quad (3.10a)$$

$$\text{s.t. } \text{Tr}(\mathbf{H}_\perp \mathbf{V} \mathbf{H}_\perp^H) \leq \bar{P}_{\text{tot}}, \quad (3.10b)$$

$$\text{diag}(\mathbf{H}_\perp \mathbf{V} \mathbf{H}_\perp^H) \leq P_{\text{max}}, \quad (3.10c)$$

$$\text{rank}(\mathbf{V}) = 1. \quad (3.10d)$$

The problem in (3.10) is a non-convex SDP problem [83]. Hence, using the method for solving an SDP problem obtained in [28], we omit the rank constraint. We note that due to the grid formation of the swarm, \mathbf{V} is symmetric and represents the tensors (outer product) of \mathbf{v} and \mathbf{v}^H , the $\text{rank}(\mathbf{V}) = 1$ is guaranteed provided that the \mathbf{v} is a non-zero vector [84]. Since Alice is assumed ignorant of Eve and subsequently transmit continuously through the flight of the UAV swarm, the UAV swarm will continually send jamming signal through out the entire flight duration. This ensures that the vector, \mathbf{v} is not zero for each n -th sample. Hence, we can neglect the constant terms of (3.10) and reformulate as (3.11).

$$\max_{\mathbf{V}} \text{Tr}(\mathbf{h}_E \mathbf{h}_E^T \mathbf{H}_\perp \mathbf{V} \mathbf{H}_\perp^H) + 1, \forall n \quad (3.11a)$$

$$\text{s.t. } \text{Tr}(\mathbf{H}_\perp \mathbf{V} \mathbf{H}_\perp^H) \leq \bar{P}_{\text{tot}}, \quad (3.11b)$$

$$\text{diag}(\mathbf{H}_\perp \mathbf{V} \mathbf{H}_\perp^H) \leq P_{\text{max}}. \quad (3.11c)$$

We note that the solution obtained in (3.11) is sufficient to characterise the sub-optimal solution of (3.10). Equation (3.11) is a convex SDP problem that can be efficiently solved using SDPT3 solvers [72].

3.3.2 Solving for Trajectory of the UAV Swarm

To obtain the trajectory of the UAV swarm, we optimise the trajectory of the head of the swarm then we derive the trajectory of other members of the UAV swarm in relation to the head since they are in grid formation with fixed spacing. If we consider the scenario when the location of Eve is unknown but can be estimated to exist within (3.8). Problem (3.7) can be reformulated in terms of trajectory of the

head UAV swarm as given in (3.12).

$$\max_{\mathbf{Q}_c} \sum_{n=1}^N \left[\log_2 \left(1 + \left(\frac{|h_{AB}|^2}{\sigma_B^2} \right) \right) - \log_2 \left(1 + \left(\frac{\gamma_0 \|\mathbf{\Omega}_A - (\hat{\mathbf{\Omega}}_E - \Delta\mathbf{\Omega}_E)\|^{-\psi}}{\frac{\gamma_0 p_u[n]}{\|\mathbf{q}_c[n] - (\hat{\mathbf{\Omega}}_E - \Delta\mathbf{\Omega}_E)\|^2} + 1} \right) \right) \right], \quad (3.12a)$$

$$\text{s.t. Constraint (3.5),} \quad (3.12b)$$

where $\gamma_0[n] = \frac{\rho_0}{\sigma_E^2[n]}$, and $p_u = |w_k|^2$ represents the signal to noise ratio at reference distance $d = 1m$ and the transmit power from swarm head. Since the locations of Alice and Bob are fixed, we assume that the noise variation is the same for each $n \in N$. Using triangular inequality for $\mathbf{x} \in \{\mathbf{q}_c[n], \mathbf{\Omega}_A\}$, and substituting (3.8), we defined the distance between point \mathbf{x} and Eve as (3.13).

$$\|\mathbf{x} - (\hat{\mathbf{\Omega}}_E - \Delta\mathbf{\Omega}_E)\| \leq \|\mathbf{x} - \hat{\mathbf{\Omega}}_E\| + \varepsilon. \quad (3.13)$$

The right hand side is a lower bound to Euclidean distance between the UAV swarm head and the centre of the circular region¹ in which Eve is located. The lower bound represents the best case scenario since the influence of the jamming signal of the swarm will be greater if it is close to Eve. On the contrary, the lower bound represents the worst case scenario for the transmitter (Alice), since it gives the closest Euclidean distance between Alice and Eve. If Eve is close to Alice the likelihood of it to purloin information increases. Following these estimation, (3.12) can be rewritten with bounds as in (3.14)

$$\max_{\mathbf{Q}_c} \sum_{n=1}^N \left[\log_2 \left(1 + \left(\frac{|h_{AB}|^2}{\sigma_B^2} \right) \right) - \log_2 \left(1 + \left(\frac{\gamma_0 (\|\mathbf{\Omega}_A - \hat{\mathbf{\Omega}}_E\| + \varepsilon)^{-\psi}}{\frac{\gamma_0 p_u[n]}{(\|\mathbf{q}_c[n] - \hat{\mathbf{\Omega}}_E\| + \varepsilon)^2} + 1} \right) \right) \right], \quad (3.14a)$$

$$\text{s.t. Constraint (3.5).} \quad (3.14b)$$

¹Due to the approximation of (3.13), $\varepsilon = 0$ does not represent the case for when the exact location of Eve is known, however, it gives an insight into the goodness of the estimator. If $\varepsilon \rightarrow 0$, then Eve is bound to be located at the centre of the region of uncertainty.

Note that (3.14) is non-convex due to (3.14a) but it can be solved by introducing slack variable, $M = \{m[n] = (\|\mathbf{q}_c[n] - \hat{\mathbf{\Omega}}_E\| + \varepsilon)^2, n \in \{1, \dots, N\}\}$ to characterise the separation between the UAV and Eve.

$$\max_{\mathbf{Q}_c, \mathbf{M}} \sum_{n=1}^N \left[\log_2 \left(1 + \left(\frac{|h_{AB}|^2}{\sigma_B^2} \right) \right) - \log_2 \left(1 + \left(\frac{\gamma_0 (\|\mathbf{\Omega}_A - \hat{\mathbf{\Omega}}_E\| + \varepsilon)^{-\psi}}{\frac{\gamma_0 p_u[n]}{m[n]} + 1} \right) \right) \right], \quad (3.15a)$$

$$\text{s.t. } (\|\mathbf{q}_c[n] - \hat{\mathbf{\Omega}}_E\| + \varepsilon)^2 - m[n] \leq 0, \quad (3.15b)$$

$$\text{Constraint (3.5)}. \quad (3.15c)$$

Equation (3.15) is still non-convex because we are trying to maximise a convex function of (3.15a). However, it can be solved using SCA technique given in [70]. This allows to solve a local tight approximation under tight constraints and relax gradually until the original problem is solved. Hence, given a predefined initial feasible trajectory, $\mathbf{Q}_c^l[n] = \{\mathbf{q}_c^l[n], n \in \{1, \dots, N\}\}$ for the l -th iteration, the non-constant term of the objective of (3.15) can be approximated with the first order Taylor expansion as given in (3.16).

$$\log_2 \left(1 + \left(\frac{\gamma_0 (\|\mathbf{\Omega}_A - \hat{\mathbf{\Omega}}_E\| + \varepsilon)^{-\psi}}{\frac{\gamma_0 p_u[n]}{m^l[n]} + 1} \right) \right) \leq F^l[n](m[n] - m^l[n]) + G^l[n], \quad (3.16)$$

where

$$\begin{aligned} F^l[n] &= [\gamma_0^2 (\|\mathbf{\Omega}_A - \hat{\mathbf{\Omega}}_E\| + \varepsilon)^{-\psi} p_u[n]] \times [(m^l[n] + \gamma_0 p_u[n]) (\gamma_0 (\|\mathbf{\Omega}_A \\ &\quad - \hat{\mathbf{\Omega}}_E\| + \varepsilon)^{-\psi} + 1) m^l[n] + \gamma_0 p_u[n]]^{-1}, \\ m^l[n] &= (\|\mathbf{q}_c^l[n] - \hat{\mathbf{\Omega}}_E\| + \varepsilon)^2, \\ G^l[n] &= \log_2 \left(1 + \frac{\gamma_0 (\|\mathbf{\Omega}_A - \hat{\mathbf{\Omega}}_E\| + \varepsilon)^{-\psi} m^l[n]}{m^l[n] + \gamma_0 p_u[n]} \right). \end{aligned}$$

Neglecting all constant terms in (3.16), (3.15) can be reformulated as

$$\max_{\mathbf{Q}_c, \mathbf{M}} \log_2 \left(1 + \left(\frac{|h_{AB}|^2}{\sigma_B^2} \right) \right) - F^l[n]m[n], \quad (3.18a)$$

$$\text{s.t. } (\|\mathbf{q}_c[n] - \hat{\boldsymbol{\Omega}}_E\| + \varepsilon)^2 - m[n] \leq 0, \quad (3.18b)$$

$$\text{Constraint (3.5)}. \quad (3.18c)$$

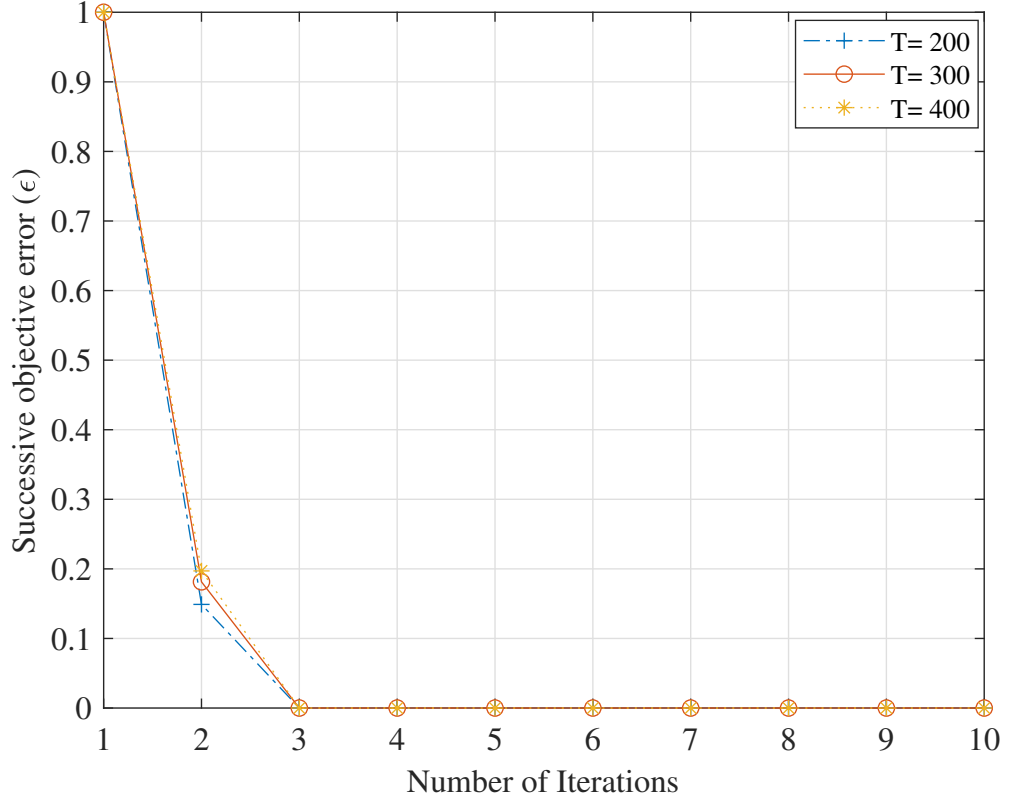
Now, (3.18) is convex and can be efficiently solved using interior point method with tools in cvx [72]. Since (3.18) maximises the lower bound of (3.15), the objective value obtained is at least equal to (3.15) using the updated trajectory, $\mathbf{Q}^l[n]$. Having obtained the trajectory of the head of the UAV swarm, the trajectory of other UAV swarm members are easily determined following the grid parameters.

3.3.3 Overall Solution

The combined solution to (3.7) was presented in algorithm 2. The proof for the convergence of algorithm 2 was shown in fig 3.2 by plotting the error of the objective function to the formulated problem after successive iterations. The algorithm begins to converge on an average of 3 iterations as depicted in fig. 3.2.

Algorithm 2 Iterative algorithm for solving \mathbf{w} , and \mathbf{Q}

- 1: Initialise \mathbf{w}^0 and \mathbf{Q}^0 with \mathbf{Q}_c^0 such that the constraints in (3.6) and (3.5) are satisfied and calculate R_s^0 with (3.4).
 - 2: $m \leftarrow 1$.
 - 3: **repeat**
 - 4: Compute and update \mathbf{w}^m with \mathbf{Q}^{m-1} by solving (3.11).
 - 5: Using updated \mathbf{w}^m , solve (3.18) to update \mathbf{Q}_c^m .
 - 6: Using the grid parameters, construct the location of all the other K UAVs in the swarm, giving rise to \mathbf{Q}^m .
 - 7: Determine the channel impulse response between the UAV swarm and the ground nodes from (3.2).
 - 8: Compute R_s^m as defined in (3.4).
 - 9: $\epsilon = \left| \frac{R_s^m - R_s^{m-1}}{R_s^m} \right|$.
 - 10: $m \leftarrow m + 1$.
 - 11: **until** $\epsilon < 10^{-5}$ OR $m \geq 200$.
 - 12: **Output:** \mathbf{w}^m and \mathbf{Q}^m .
-

FIGURE 3.2: Convergence analysis of algorithm 2 with $K = 9$.

3.4 Results and Analysis

In this section, we evaluate the performance of the UAV swarm to deliver the jamming signals with algorithm 2. The parameters used in the numerical simulations set were presented in table 3.1 unless otherwise stated. The initial values of the optimisation parameters satisfying respective constraints were obtained via feasibility analysis. The UAV swarm beamforming vectors and its trajectory were solved by iteratively optimising each parameter with the knowledge of the others, until the error (ϵ) between steps was less than 10^{-5} or 200 maximum number of iterations was reached.

TABLE 3.1: Parameters for simulating the UAV swarm problem

Simulation parameter	Symbol	Value
Alice location	Ω_A	$[0, 0, 0]$
Bob location	Ω_B	$[1000, 0, 0]$
Eve location	Ω_E	$[500, 250, 0]$
Initial UAV location	\mathbf{q}_0	$[-100, 100, H]$
Final UAV location	\mathbf{q}_f	$[1500, 100, H]$
UAV height(when fixed)	H	100m
Velocity per sample(when fixed)	Z	3m/s
Duration per sample(when fixed)	δ	1s
Signal-to-noise ratio	ρ_0	90dB
Average UAV transmit power	\bar{P}_{tot}	20dBm
Maximum UAV power	P_{max}	26dBm
Average Source power	\bar{P}_{ab}	30dBm
Maximum source power	P_{amax}	36dBm
Path loss for ground communication (urban area cellular radio)	ψ	3.1 (outdoor)
Grid gutter		10λ
Grid cell		3

In the legends in figs. 3.3 - 3.7; T , K , and ϵ represents the UAV swarm flight time, the number of UAVs and the radius (ϵ) of the location of Eve respectively. While “Unknown Eve” and “known Eve” scenarios represents the trajectory plots when Eve location is unknown and when it is known respectively.

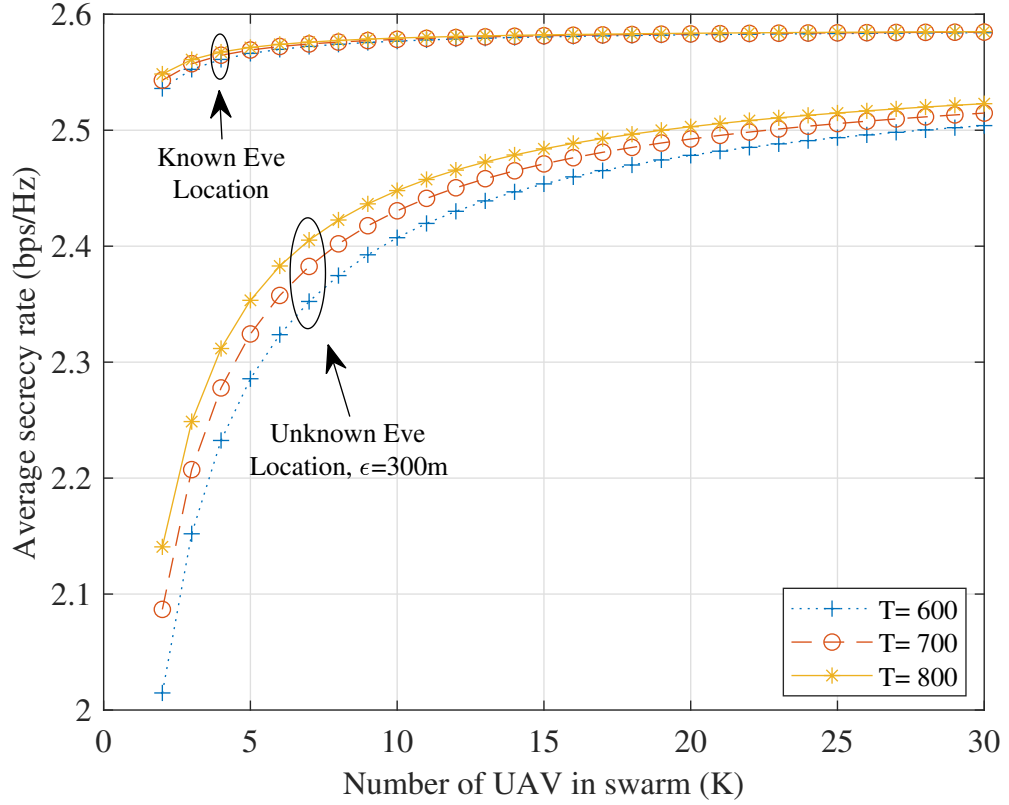


FIGURE 3.3: Comparative performance of the UAV Swarm on average secrecy rate when the eavesdropper location is known and unknown.

The performance of the UAV swarm in relation to PLS for different flight times was given in fig. 3.3. The figure also showed that as the number of UAVs in the swarm was increased, beyond some critical number the improvement on the average secrecy rate becomes insignificant. Consider that an increase in the number of UAV swarm elements leads to a large grid. The large grid causes the collaboration of the UAV elements to lower as some elements become redundant. From fig. 3.3, it is easy to see that such inflection point for the “Unknown Eve” scenario occurs when the number of UAVs was 9. However, the effect of K is minimal when the exact position Eve is known. Furthermore, as the number of UAVs making up the swarm increases, with higher flight times, improved average secrecy rate performance was observed.

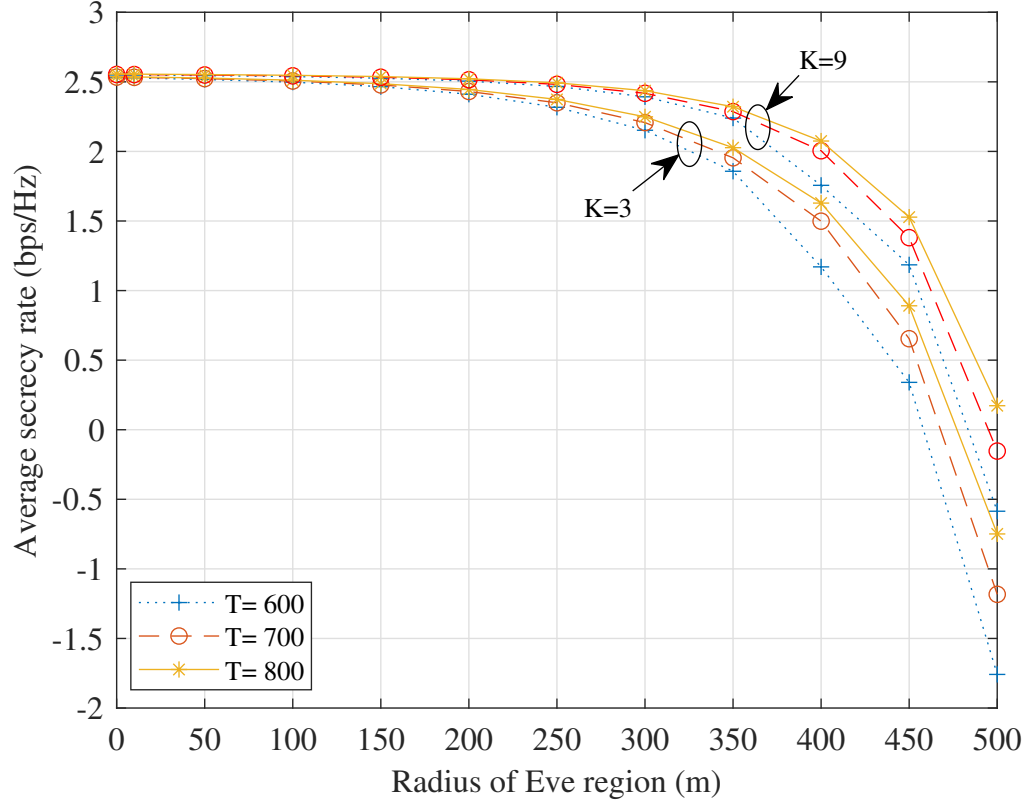


FIGURE 3.4: Effect of radius of Eve region on average secrecy.

Further observation on fig. 3.4 presents the limit to the uncertainty location area of Eve at different flight times. As the radius where Eve is located increases, the impact of the UAV swarm jamming signal becomes less significant as the average secrecy rate reduces. Negative average secrecy rate is obtained once Eve has better CSI than Bob and the UAV swarm do not provide enough jamming power as shown in fig. 3.4. The influence of the UAV swarm flight time is further increased at larger radius. Nevertheless, the characterisation of the maximum tolerable error radius in the position of Eve will guide the design of its location estimators. For example for 9 UAVs forming the swarm, the tolerable error region is 300m while for 3 UAVs, we have 200m.

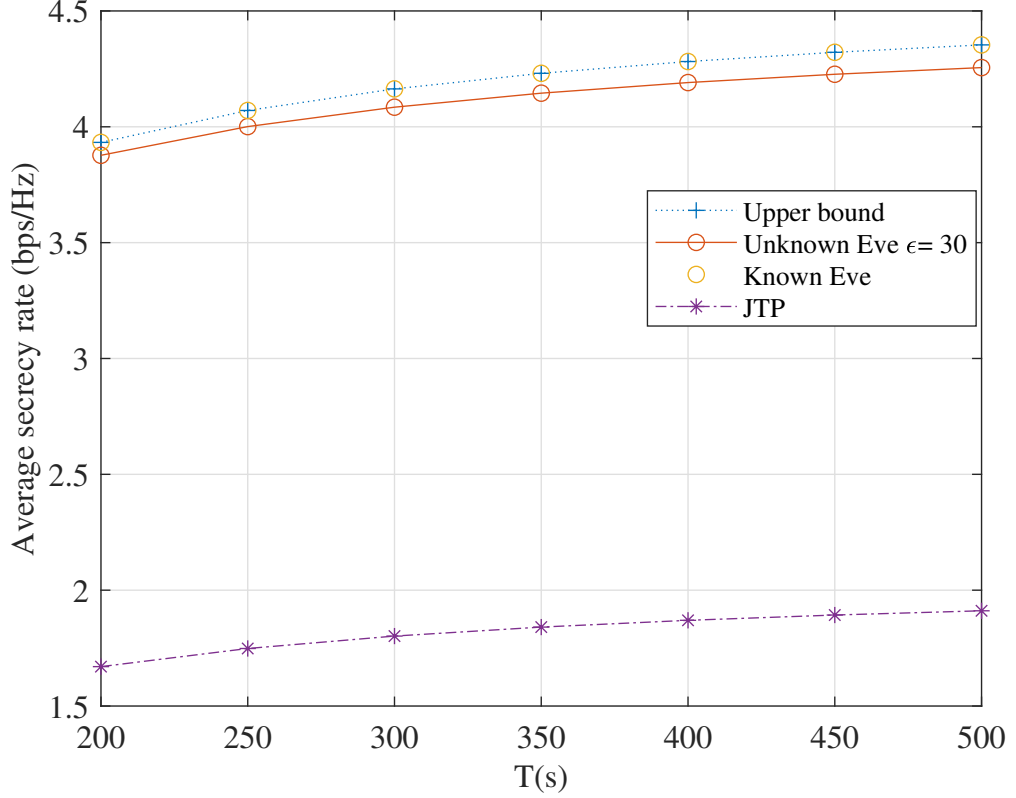


FIGURE 3.5: Comparative performance of the average secrecy rate of the UAV Swarm and single UAV jammer for $K = 9$, $\mathbf{\Omega}_b = [200, 0, 0]^T$, $\hat{\mathbf{\Omega}}_e = [200, 150, 0]^T$, $\mathbf{q}_f = [150, 100, 100]^T$.

In fig. 3.5, the average secrecy rate performance analysis of the UAV swarm joint trajectory and beamforming optimisation for known and unknown Eve's location are compared with known Eve location scenario considered in [29] (referred to as JTP in the legend) under similar power constraint. It is evident from the figure that the application of the UAV swarm out-performs the baseline scheme of a single UAV jamming model. It can be further observed that the longer time of flight of the UAVs ensures better secrecy performance. This is intuitively, and correlates with similar results presented in [29, 31, 32], since the UAVs delivers more jamming power during the communication with longer duration of flight time. When the radius of error ϵ is approximately zero, the unknown location of Eve relaxes to a single point which then acts as the known Eve's location. When that happens, we define the scenario as the upper bound of the optimisation as it gives the best case scenario

to the performance of the scenarios where $\varepsilon > 0$. In practice, as $\varepsilon > 0$, the average secrecy rate reduces (as also presented in fig. 3.4).

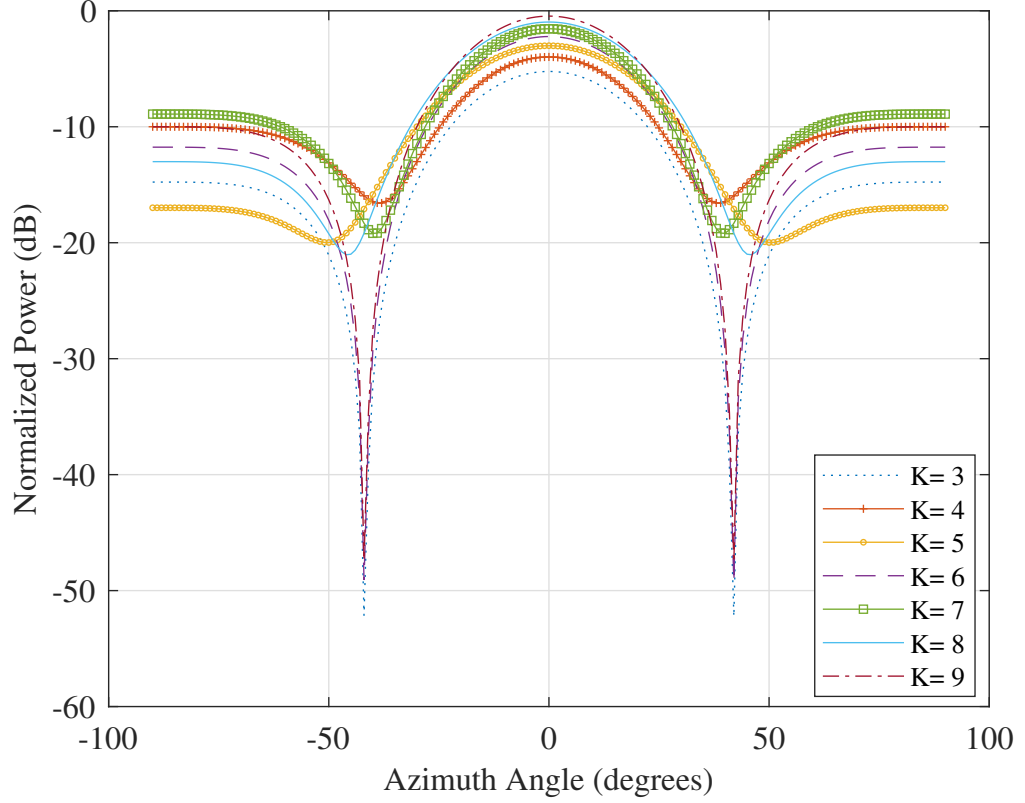


FIGURE 3.6: Beam Pattern at $T = 600$ and $\varepsilon = 300m$.

Examining the radiation pattern generated by the UAV swarm, as presented in fig. 3.6, it was observed that for K values that did not complete a quadrilateral formation of the grid ($K = 4, 5, 7, 8$), the null depth is shallow compared to values where the grid quadrilateral is complete ($K = 3, 6, 9$). The implication is that little spurious jamming signal from the UAV swarm has greater tendencies of leaking to Bob when the grid formation is incomplete. Despite the observation that higher values of K gives higher power in the main lobe, it is apparent that even when multiple UAVs are available, a selection needs to be made to ensure the grid quadrilateral is complete with recourse to the minimum number required to achieve maximum average secrecy rate as shown in fig. 3.3. However, for all values of K , side lobes with high power levels were observed. Although in conventional beamforming, the aim is

to minimise the side lobes, however, since the exact position of Eve is unknown and Bob is at the null of the jamming signal, the jamming power radiated from the side lobes will further reduce the information content received by Eve, especially where multiple Eve exist.

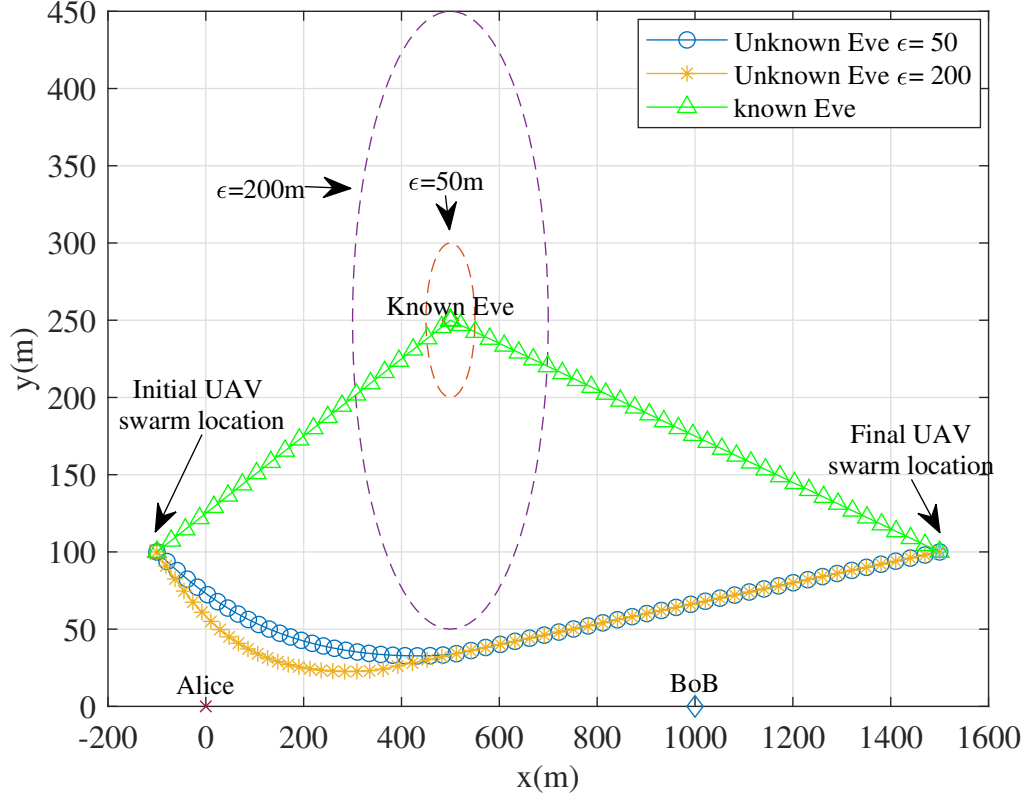


FIGURE 3.7: The UAV swarm trajectory for $T = 600s$.

The trajectory of the swarm in fig. 3.7, shows that the optimal trajectory when Eve's location is unknown follows a path close to Alice and Bob. Since the channel models are distance dependent, if Eve enjoys better channel quality than Bob then the zero or negative average secrecy rate ensues. The UAV prioritises sending higher jamming signal to Eve when it is closer to Alice. Since it cannot determine the exact location of Eve, following this trajectory ensures that the channel for Eve is always degraded despite its proximity to the transmitter (Alice). On the contrary, when the location of Eve is known (known Eve in fig. 3.7), the swarm flies directly above it and jams the signal.

3.5 Chapter Summary

In this chapter, grid formation of UAV swarm was exploited to collaboratively jam a passive eavesdropper. The passive eavesdropper was bound within a predefined region. An optimisation problem characterising the UAV swarm jammer problem was formulated and solved by finding the trajectory of the UAVs and their corresponding jamming signal power. By performing the coordinated jamming, the PLS, measured as the average secrecy rate, was increased compared to the use of a single UAV application. Considering that physical spacing between the UAV member of the swarm is larger, a barrier to increasing their number was observed from the results. Other analysis in relation to the average secrecy rate examines the impact of varying the total time of flight, and changing the radius of the uncertain region of the eavesdropper.

Chapter 4

Physical Layer Security with UAV-Carried IRS

Replacing the UAV swarm, discussed in chapter 3, with an IRS system, we explore the inherent properties of the IRS system to guarantee PLS. This is necessary to reduce the computational cost and logistic of synchronizing multiple UAVs to act as a single unit. Secondly, the IRS system is a passive device with little contribution to power consumption of the model. Therefore, in this chapter a UAV-carried IRS for secure data collection in wireless sensor networks was investigated. The goal of this chapter is to ascertain the performance of aerial based IRS system on PLS when an eavesdropper is passive. The related literature was discussed in section 4.1. Thereafter the model was described and mathematical formulation of the model was given in section 4.2. Having formulated the problem, section 4.3 provided a method to solve the problem. Numerical simulations were carried out and the discussions on the results were presented in section 4.4. Section 4.5 summarised the contribution of the chapter.

4.1 Overview of IRS on PLS

Next generation networks will be equipped with more active and passive communication nodes to improve on coverage and capacity by accommodating the use of higher frequency spectrum (e.g. millimeter wave) and massive multiple-input multiple-output (M-MIMO) technology [45, 74, 85]. Nevertheless, these expectations foretell several logistic and environmental drawbacks ranging from increased communication cost in terms of energy, space and finance, to lower security guarantees. In recent times, secure, high capacity, energy efficient and cost effective communication systems have been the paramount facet in developing technologies for the next generation of wireless communication systems [74, 81]. These next generation technologies ensure ultra-reliable connection to massive end user nodes, amidst rapid time varying channels due to fast mobility and complex inter-connection [74]. On its part, traditional communications technologies were rapidly been upgraded to support growing demands. But these upgrades only act as a conduit since they will eventually be overwhelmed in due time, especially with full deployment of the next generation systems. Several cost effective wireless communication technologies have been proposed in recent times such as lens MIMO, hybrid beamforming, unmanned aerial vehicle (UAV)/drone communications, advanced analog to digital converters (ADCs), etc. One of the primary goal of these technologies is to maximise the utilisation of the wireless communication channel.

A shift in paradigm in the wireless channel control occurred with the discovery of the intelligent reflecting surface (IRS) [42–44]. The IRS was pitched to provide an interface between the traditional wireless base stations and the users. Unlike the conventional active relays, radio signal reflected by IRS are free from self-interference [45]. The IRS system acts as a collection of small passive “mirrors” that reflects the signals by performing passive beamforming. An overview of IRS with the technicalities of the physical implementation have been studied in [42, 43, 45]. Several literature continue to explore novel designs to harness the intelligence and capacity of the IRS for effective communication. These works develop methods to optimally modelling

the reflection coefficient and other related established parameters like beamforming weights.

For specific IoT applications, a joint optimisation of the transmit beamforming and the reflection coefficients of the IRS system serving as relay between multiple antenna access point (AP) and a single antenna user was investigated in [86]. Further research used the IRS to extend the coverage region of a base station by constructively reflecting its impinging signal to desired locations either terrestrial [87] or aerial [88]. Furthermore, the IRS-enabled programmable wireless channels is a promising technology to promote PLS due to its inherent property of configuring transmission to desired users [75, 89, 90]. Literally, this manipulates the wireless channel to be favourable at desired location and adverse at another.

One key feature of the IRS system is that the reflected signal can be possibly made to constructively sum at the legitimate receiver while destructively combined at the undesired location (eavesdropper). However, the combination of the IRS reflected signals are not perfect. It is possible that the imperfection in the destructive summation can compromise the PLS of the communication with an IRS system. The authors in [91] showed analytically that the imperfection arise due to the beamwidth dependence of the reflected signal on wavelength and IRS size. The beamwidth is inversely proportional to the IRS size but proportional to wavelength [91]. The proportionality on wavelength implies that for fixed size, wider beams are generated in the radio spectrum. However, a narrow beam (more specular reflection) can be obtained when visible light is reflected with the same IRS. Therefore, IRS was described as an “anomalous” radio spectrum reflector [89, 91]. Further assertion relates the mismatch of the IRS reflected signals to the placement of the IRS system [92]. Most of the existing works on IRS-aided communication focus on fixed terrestrial IRS deployment (on facades of buildings or indoor walls/ceilings). This fixed deployment does not provide adaptability to mobile users and does not reap the full potential of IRS in terms of information rate and PLS.

Therefore, it is desirable to allow mobility of the IRS system possibly by mounting it on a UAV or other aerial devices [92, 93]. The choice of aerial mobility system will

also aid exploitation of aerial visibility for the IRS line-of-sight (LoS) application. One major drawback of aerial IRS is that more malicious users can easily establish LoS link to the aerial IRS system. Relying on the non-specular nature of the reflected radio signal, the PLS of the communication can be compromised. It is therefore the goal of this chapter to investigate the design of an IRS system mounted on a UAV. The UAV-carried IRS system will seek optimal placement while ensuring that the spurious signals received at illegitimate locations are of low quality.

Another objective of this chapter is to secure data transmission with a UAV-carried IRS system in a noisy multi-sensory scenario. By maximising the achievable secrecy rate under total transmit power constraint, we optimise the transmit beamforming weights, IRS reflection coefficients and the location of the IRS system aided by the mobility of the UAV. We assume that there were no direct link between the sensors/transmitters and the receivers, therefore the communication link was established only through the UAV-carried IRS system. By this assumption, we model the transmitter, Alice to be located in a blackout remote region where the only possible access is through the UAV-IRS system. In practise, the assumption supports remote infrastructure monitoring facilities e.g. monitoring a remote pipeline with a group of low-powered sensors. The assumption can be guaranteed in practise considering that the very large distance between the transmitters and receivers may be due to natural barriers like mountains and rivers. We note that if this assumption fails, then the solution developed in this chapter will not be applicable.

Therefore, having examined the literature alluding to the scope of the models, we can highlight the major contributions of this chapter as follows:

- (a) Designing the IRS reflection coefficients, beamforming weights and UAV trajectory considering when passive eavesdropping.
- (b) Considering a noisy environment, we proposed an analytical derivation of the SNR at the main receiver and at the eavesdropper.

4.2 System Model and Problem Formulation

Let us consider that an IRS was carried by a UAV tracing a path such that the reflected signals from transmitter (Alice) were received at a base station (Bob) which are physically incommunicado as shown in fig. 4.1. Since the radio signals from the IRS are not specularly reflected especially in noisy environment, (i.e. the reflection is not mirror-like [91]), an eavesdropper (Eve) lurking around Alice can receive an out-of-phase version of the reflected signals. Invariably, the secrecy of the communication between Alice and Bob can be compromised, especially if Eve has access to advanced signal reconstruction technologies.

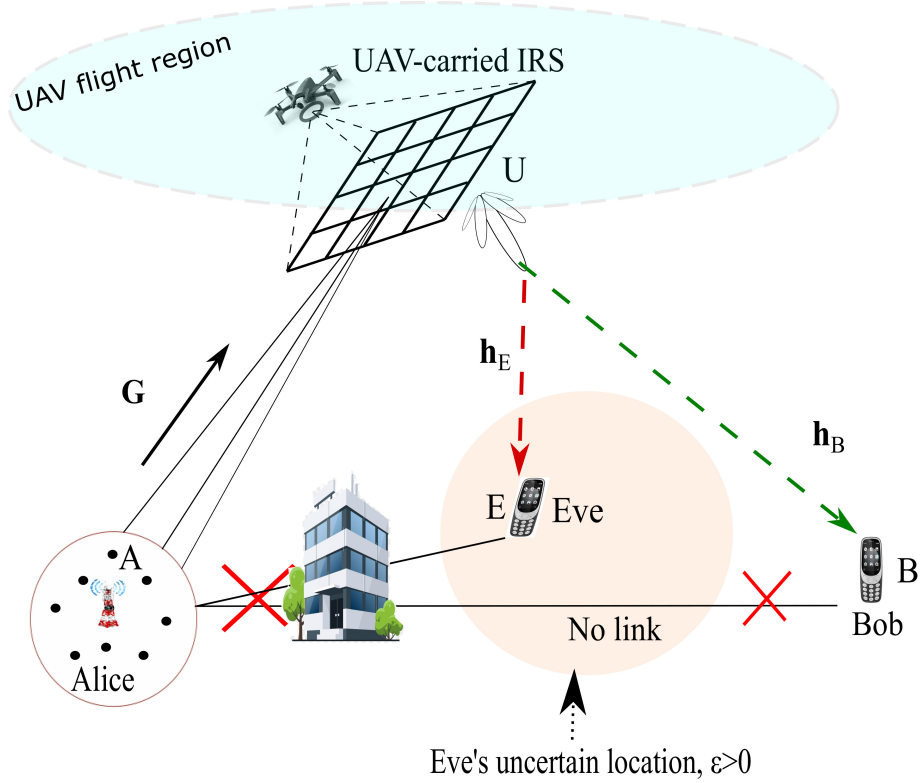


FIGURE 4.1: Schematic of the UAV-IRS interaction with ground nodes

Let us consider that Alice comprise of closely packed M sensor nodes at the ground level within an area of radius, r , collaboratively beamforming a unique symbol to Bob through the IRS. Similar to the defined notations, let the 3D location of Bob, Eve, and the centre of Alice be Ω_B , Ω_E , Ω_A , respectively. We note that Bob and Eve are in the far-field of the IRS system as required practically. The channels within the slot

relating to the UAV-IRS system are assumed to vary slowly allowing for block fading within the slot. For ease of computation, the IRS are placed on the UAV such that, for each $n \in \{1, \dots, N\}$, the location of the first IRS element, which we consider as the reference element, is the same as the location of the UAV ($\mathbf{q}_R[n] = \mathbf{q}[n]$). Given that λ is the carrier wavelength, all other adjacent elements of the IRS are separated by a fixed distance such that $d_x < \frac{\lambda}{2}$ and $d_y < \frac{\lambda}{2}$ [92]. This implies that $d_x = \frac{\lambda}{z_x}$ and $d_y = \frac{\lambda}{z_y}$, where $z_x > 2$ and $z_y > 2$. Hence we define the location of the n th IRS element such that $\mathbf{Q}_{\text{IRS}}[n] = (\mathbf{q}_{\text{Rx}}[n] + (k_x - 1)d_x, \mathbf{q}_{\text{Ry}}[n] + (k_y - 1)d_y, H)$, $n \in \{1, \dots, N\}$, $k_x \in [1, \dots, K_x]$, $k_y \in [1, \dots, K_y]$; where K_x and K_y define the number of IRS elements along the x- and y-directions of the grid, respectively. Since, the total number of IRS elements is given as $K = K_x K_y$, a compressed form of IRS element location can be written as $\mathbf{Q}_{\text{IRS}}[n] = \{\mathbf{q}_k[n], \forall n \in [1, \dots, N], \& \forall k \in [1, \dots, K]\}$. We further assume that the IRS element are arranged in a planar form.

Following the convention as in [94], we assume that the sensors in Alice collaboratively transmits a unique symbol $s(t)$ with $\mathbb{E}\{|s(t)|^2\} = 1$ giving rise to a passband signal of $x(t) = s(t) \exp(j\omega_c t)$. The incident signal on the IRS elements from the m th sensor of Alice during an n th sampling period is (4.1).

$$\mathbf{r}[n] = \mathbf{g}_m[n] w_m[n] x(t)[n] + \mathbf{n}_m[n], \quad (4.1)$$

where $\mathbf{g}_m = [g_{m1}, g_{m2}, \dots, g_{mK}]^T$ and $\mathbf{n}_m \sim \mathcal{C}^{K \times 1}$ denote the IRS to the m th sensor complex channel vector and the independent and identically distributed (i.i.d.) white Gaussian noise vector due to the LoS link between the IRS elements and the m th sensor, respectively. The symbol w_m represents the beamforming weight of the m th antenna element of Alice ($\forall m = 1, \dots, M$). Thus, the complex channel matrix between the IRS elements and all the sensors on Alice is given by

$$\mathbf{G} = [\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_M] \in \mathcal{C}^{K \times M}.$$

The UAV's continuous flight trajectory causes the reflected signals from the IRS to undergo Doppler shift and time variation at the receiver ground receivers (Bob and

Eve). However, since all the IRS elements are fixed on the UAV and travelling at the same velocity, the Doppler shift due to the respective position of the elements will be uniform. Furthermore, we note that we can eliminate the Doppler effect, by carefully compensating the Doppler phase shifts through the IRS reflection coefficients as discussed in [95, 96]. This can be justified for the model of this chapter because

- (a) there are no direct transmission link between the Alice and the ground receivers (Bob and Eve) which cannot be influenced by the IRS and
- (b) for large N leading to continuous trajectory, the coherence time of the channels is relatively low.

Invariably, considering the interaction between the k th IRS element and the m th sensor, we have that the incident signal in (4.1) can be expanded to (4.2).

$$g_{mk}[n]w_m[n]x(t)[n] = \text{Re}\{w_m[n]\sqrt{c_{mk}[n]}s(t - \tau_{mk}[n])\exp(j\omega_c(t - \tau_{mk}[n]))\}, \quad (4.2)$$

where $\tau_{mk}[n] \triangleq \frac{\|\mathbf{q}_k[n] - \Omega_m\| \mathbf{a}_{mk}}{c}$ defines the coordinate spatial frequency between the k th IRS element and the m th antenna element and g_{mk} follows an exponential distribution with channel power gain, $c_{mk}[n] \triangleq \frac{\rho_0 \varsigma_k}{\|\mathbf{q}_k[n] - \Omega_m\|^\mu}$ for ρ_0 and ς_k representing the channel power gain at reference distance $d_0 = 1\text{m}$ from the the centre of Alice and an exponentially distributed random variable with unit mean, respectively [29, 56, 76]. Note that ρ_0 determines the quality of the channel which is then scaled randomly by ς_G via the inverse distance square. Furthermore $\mu = 2$ represents the LoS path loss exponent between the IRS and the ground nodes [93, 97]. We assume that the LoS is the main component of the channel link. Contrarily to [94], we note that although the distance between the IRS elements and the distance inbetween the sensors nodes are less than the distance between the UAV and Alice (that is $\|\mathbf{q}_k[n] - \mathbf{q}_{k\pm 1}[n]\| \ll \|\mathbf{q}_R[n] - \Omega_A\|$ and $\|\Omega_m - \Omega_{m\pm 1}\| \ll \|\mathbf{q}_R[n] - \Omega_A\|$), the independent sensor to IRS element variations cannot be ignored since the separation between sensors can be significant when deployed in multi-faceted environment. Nevertheless, we assume that the beam from the sensors is directed to the UAV carrying the IRS and not necessarily each IRS element, therefore the phase direction is

towards the UAV. Equation (4.2) can then be modified for each $n \in \{1, \dots, N\}$ as

$$g_{mk}w_m\mathbf{x}(t) = \text{Re}\{w_m\sqrt{c_{mR}} \exp(-j\phi_{mk}\hat{\mathbf{a}}_{mR})\delta\left(t - \frac{\phi_{mk}}{\omega_c}\right)s(t) \exp(j\omega_c t)\}, \quad (4.3)$$

where $\phi_{mk} \triangleq \omega_c \tau_{mk}$ characterises the phase shift due to the k th IRS element location relative to the m th sensor and $\hat{\mathbf{a}}_{mR}$ is the normalised unit vector from m to UAV(R). By implication of the distance between the IRS being far less than the distance between the UAV and Alice, the phase shift for each $n \in \{1, \dots, N\}$ can be approximated as

$$\phi_{mk}\hat{\mathbf{a}}_{mR} \approx \underbrace{\frac{2\pi}{\lambda}\|\mathbf{q}_R - \boldsymbol{\Omega}_m\|}_{\phi_{mR}^a} + \underbrace{\frac{2\pi\hat{\mathbf{a}}_{mR}}{\lambda}\|\mathbf{q}_k - \mathbf{q}_R\|\hat{\mathbf{a}}_{Rk}}_{\phi_{mk}^b}. \quad (4.4)$$

It is imperative, then, that from (4.4), the phase shift is comprised of two distinct parts; based on i) fixed phase: the position of the UAV (ϕ_{mR}^a) and ii) variable phase: the k th IRS element response (ϕ_{mk}^b) to the signal from the m th sensor in Alice. In component form, the k th IRS element response phase can be written as (4.5).

$$\phi_{mk}^b = [(k_x - 1)\bar{d}_x, (k_y - 1)\bar{d}_y, 0] \cdot [\hat{a}_{mR}^x, \hat{a}_{mR}^y, \hat{a}_{mR}^z]^T, \quad (4.5)$$

where $\bar{d}_x = \frac{2\pi d_x}{\lambda}$ and $\bar{d}_y = \frac{2\pi d_y}{\lambda}$. It is easy to deduce that the IRS array response to all the sensor nodes can be represented with a $K \times M$ matrix, $\boldsymbol{\Phi}_G$, whose elements are given in (4.5).

$$\boldsymbol{\Phi}_G = \begin{bmatrix} \phi_{11}^b & \dots & \phi_{1K}^b \\ \vdots & \ddots & \vdots \\ \phi_{M1}^b & \dots & \phi_{MK}^b \end{bmatrix}^T$$

The $\text{rank}\{\boldsymbol{\Phi}_G\} \geq 1$ depends on the value of the radius of Alice (r). For $r > 0$ increases the possibility of large distance between the M sensors, thereby causing significant variations for the elements in $\boldsymbol{\Phi}_G$.

By extracting the complex channel coefficients from (4.3) for each $n \in \{1, \dots, N\}$,

the complex channel between the k th IRS element and the m th sensor node in Alice is thus presented as (4.6).

$$g_{mk} = \sqrt{c_{mR}} \exp(-j\phi_{mR}^a) \exp(-j\phi_{mk}^b) \delta\left(t - \frac{\phi_{mk}}{\omega_c}\right), \quad (4.6)$$

where $\exp(-j\phi_{mk}^b)$ elucidates the k th IRS elements response to the incident signal from the m th sensor. Recalling that $\mathbf{g}_m = [g_{m1}, g_{m2}, \dots, g_{mK}]^T$, (4.6) describes the elements of \mathbf{g}_m .

Alternatively, the combined IRS response to the incident signal from the m th sensor in Alice can be rewritten as (4.7). This is obtained by substituting (4.5) into $\mathbf{j}^b = \exp(-j\phi_{mk}^b)$. The \mathbf{j}^b presented in (4.7) shows the influence of the IRS formation on the incident signal.

$$\mathbf{j}^b = [1, \dots, \exp(-j(K_x - 1)\bar{d}_x \hat{a}_{mR}^x)]^T + [1, \dots, \exp(-j(K_y - 1)\bar{d}_y \hat{a}_{mR}^y)]^T. \quad (4.7)$$

Therefore, the channel vector between all the IRS elements and the m th sensor can be presented as

$$\mathbf{g}_m = \sqrt{c_{mR}} \exp(-j\phi_{mR}^a) \mathbf{j}^b \circ \delta\left(t - \frac{\phi_{mR}^a + \mathbf{j}^b}{\omega_c}\right), \quad (4.8)$$

where \circ is the Hadamard product. Although equations (4.6) and (4.8) are different representations of \mathbf{g}_m , we continue the derivations in this chapter with (4.6) because it is a simpler expression.

Similarly, for each $n \in [1, \dots, N]$, the complex channel between the IRS and the ground nodes (that is $\mathbf{h}_i = [h_{1i}, \dots, h_{Ki}]^T \in \mathcal{C}^{K \times 1}, \forall i \in \{B, E\}$), was obtained by updating the direction of the reflected signal given in (4.9).

$$h_{ki} = \sqrt{c_{Ri}} \exp(-j\phi_{Ri}^a) \exp(-j\phi_{ki}^b) \delta\left(t - \frac{\phi_{ki}}{\omega_c}\right), \quad (4.9)$$

where $\phi_{ki}^b = [(k_x - 1)\bar{d}_x, (k_y - 1)\bar{d}_y, 0] \times [\hat{a}_{Ri}^x, \hat{a}_{Ri}^y, \hat{a}_{Ri}^z]^T$. It is imperative that the generalised IRS array response to the ground node can be presented as a $K \times 1$

vector, \mathbf{u}_i with elements given as ϕ_{ki}^b . Note that $c_{ki}[n] \approx c_{\text{Ri}}[n] \triangleq \frac{\rho_0 \varsigma_i}{\|\mathbf{q}_{\text{R}}[n] - \Omega_i\|^2}$, $\phi_{\text{Ri}}^a = \frac{2\pi}{\lambda} \|\Omega_i - \mathbf{q}_{\text{R}}\|$ and $\tau_{ki} \triangleq \frac{\|\Omega_i - \mathbf{q}_{\text{R}}\|}{c}$. Therefore, having defined the channel parameters, the coherently received signal at the ground nodes (Bob and Eve) during the n th sample is given by

$$y_i = \mathbf{h}_i^H \Theta \mathbf{G} \mathbf{w} x(t) + \eta_i, \quad (4.10)$$

where $i \in \{\text{B}, \text{E}\}$, $\mathbf{w} = [w_1, \dots, w_M]^T$ is the beamforming weights of the M sensors, $\Theta = \text{diag}(\exp(j\theta_1), \exp(j\theta_2), \dots, \exp(j\theta_K))$ represents the reflection coefficients of the IRS elements and $\eta_i \sim \mathcal{CN}(0, \sigma_i^2)$ presents an independent and identically distributed (i.i.d.) additive white Gaussian noise (AWGN) at the corresponding receiver¹. Note that at the ground receiver nodes, (Bob and Eve), the reflected signals from all the IRS elements are superimposed coherently [90, 92]. It is intended that such coherent superimposition will maximise the received signal power at the Bob while limiting the signal power at Eve.

Our design objective is explored under these sub-headings.

1. **Generic model:** Given the channel information of Bob and Eve, we aim to maximise the secrecy rate of the communication by choosing the optimal beamforming weight, trajectory of the UAV and the reflection coefficients of the IRS. Accordingly, we formulate the optimisation problem of (4.11).

$$\max_{\mathbf{w}, \mathbf{Q}, \Theta} \frac{1}{N} \sum_{n=1}^N \left[\log_2 \left(\frac{1 + \gamma_{\text{B}}[n]}{1 + \gamma_{\text{E}}[n]} \right) \right]^+, \quad (4.11a)$$

$$\text{s.t. } 0 \leq \theta_k[n] \leq 2\pi, \quad (4.11b)$$

$$\|\mathbf{q}[n] - \mathbf{q}[n-1]\|^2 \leq (Z\alpha)^2, \quad (4.11c)$$

$$\mathbf{w}[n]^H \mathbf{w}[n] \leq P, \quad (4.11d)$$

¹By setting σ_i^2 to high value, we ensure that the communication channel is noisy.

where $[x]^+ = \max\{x, 0\}$ ², $\gamma_i[n] = \frac{1}{\sigma_i^2} |\mathbf{h}_i^H[n] \mathbf{\Theta}[n] \mathbf{G}[n] \mathbf{w}[n]|^2$, $i \in \{B, E\}$ represents the signal to noise ratio at Bob and Eve. γ_i is the SNR at the i th receiver with its probability density function (PDF) given in Appendix B. The constraint in (4.11b) ensures that the principal argument of the reflection coefficient from the k th IRS was maintained while (4.11c) limits the distance covered by the UAV between sampling points. Equation (4.11d) constrains the power transmitted from the sensors.

2. **Modified model:** Given that the presences of Eve in the system model is unknown, we aim to maximise the rate achieved at Bob by solving (4.12). Furthermore, we examined the impact of this rate maximisation on a passive Eve located within the system.

$$\max_{\mathbf{w}, \mathbf{Q}, \mathbf{\Theta}} \frac{1}{N} \sum_{n=1}^N [\log_2 1 + \gamma_B[n]]^+, \quad (4.12a)$$

$$\text{s.t. } 0 \leq \theta_k[n] \leq 2\pi, \quad (4.12b)$$

$$\|\mathbf{q}[n] - \mathbf{q}[n-1]\|^2 \leq (Z\alpha)^2 \quad (4.12c)$$

$$\mathbf{w}[n]^H \mathbf{w}[n] \leq P, \quad (4.12d)$$

4.3 Proposed Solution

Equation (4.11) is a non-convex multi-variable optimisation problem that is difficult to solve directly due to the inter-dependence of the varriables and the non-convexity of the objective function. Hence, we sub-divide the problem by creating distinct sub-optimal problems from (4.11) [76, 90, 92]. The idea is to solve the sub-optimal problems iteratively until a change in the objective value of (4.11) is insignificant.

²Note that $[x]^+$ imposes a constraint that the information received at Eve will always be less than that at Bob else no message is transmitted. However, since there are no direct path between the transmitter (Alice) and the ground nodes (Bob and Eve), the received signals will always be from the IRS reflected path. The reflection coefficients ensures that the reflection is maximum at target location (Bob) [91]. This means that the eavesdropper receives only the non-specular weak reflected signal. Therefore, negative objective will not arise in this model, hence, we ignore this constraint in the subsequent derivations. If there are a direct communication link between the transmitter and the ground nodes (Bob and Eve), then negative secrecy will be possible.

However, we see from the subsequent sections that by designing the reflection coefficient in terms of the main receiver, Bob, the sub-optimal problems arising from (4.12) was solved using non-iterative means.

We note that the UAV and the sensors have limited power, therefore, they may not be equipped to support the computational overhead presented in this section. We assume that the channel of the main receiver (Bob) is perfectly known at a central control node that performs these computations. This central node is responsible for communicating the beamforming weights to the transmitter (Alice), the trajectory to the UAV and the reflection coefficients to the IRS. This communication takes place via the control signaling channel.

4.3.1 Solving for Θ

In this section, we discussed the possible procedures to obtain the reflection coefficients (Θ) based on specific information at the IRS control. We note that since the IRS are passive elements, they do not alter the signal power. Therefore, the magnitude of the reflection coefficient is always 1 while the procedure described in the section obtained its phase.

4.3.1.1 Generic Model

This method depends on knowledge of the beamforming vectors and the trajectory of the UAV. Given that the sub-problem from (4.11) in relation to Θ is (4.13).

$$\max_{\Theta} \frac{1}{N} \sum_{n=1}^N \left[\log_2 \left(\frac{1 + \gamma_B[n]}{1 + \gamma_E[n]} \right) \right], \quad (4.13a)$$

$$\text{s.t. } 0 \leq \theta_k[n] \leq 2\pi. \quad (4.13b)$$

Recalling (4.10) and applying some matrix manipulations, it is known that

$$\gamma_i = \left| \frac{1}{\sigma_i^2} \mathbf{h}_i^H \Theta \mathbf{G} \mathbf{w} \right|^2 = \left| \frac{1}{\sigma_i^2} \hat{\boldsymbol{\theta}}^H \mathbf{H}_i \mathbf{G} \mathbf{w} \right|^2 \quad \forall i \in \{B, E\},$$

where $\hat{\boldsymbol{\theta}} = [\exp(j\theta_1), \dots, \exp(j\theta_K)]^H$ and $\mathbf{H}_i = \text{diag}(\mathbf{h}_i^H)$. Since the problem defined in (4.13) is not dependent on the n th sample, we can reformulate it as given in (4.14) for each $n \in \{1, \dots, N\}$.

$$\max_{\hat{\boldsymbol{\theta}}} \left(\frac{1 + |\frac{1}{\sigma_B^2} \hat{\boldsymbol{\theta}}^H \mathbf{H}_B \mathbf{G} \mathbf{w}|^2}{1 + |\frac{1}{\sigma_E^2} \hat{\boldsymbol{\theta}}^H \mathbf{H}_E \mathbf{G} \mathbf{w}|^2} \right), \quad (4.14a)$$

$$\text{s.t. } |\exp(j\theta_k)|^2 = 1 \quad \forall k \in \{1, \dots, K\}. \quad (4.14b)$$

The constraint in (4.13b) has been rewritten for tractability as (4.14b) since the square magnitude of a complex exponent is 1. Equation (4.14) can further be simplified to (4.15).

$$\max_{\hat{\boldsymbol{\Theta}}} \left(\frac{1 + \text{Tr}(\mathbf{A} \hat{\boldsymbol{\Theta}})}{1 + \text{Tr}(\mathbf{B} \hat{\boldsymbol{\Theta}})} \right), \quad (4.15a)$$

$$\text{s.t. } \text{diag}(\hat{\boldsymbol{\Theta}}) = 1, \quad (4.15b)$$

$$\text{rank}(\hat{\boldsymbol{\Theta}}) = 1, \quad (4.15c)$$

where $\hat{\boldsymbol{\Theta}} = \hat{\boldsymbol{\theta}} \hat{\boldsymbol{\theta}}^H$, $\mathbf{A} = |\frac{1}{\sigma_B^2}|^2 \mathbf{H}_B \mathbf{G} \mathbf{w} \mathbf{w}^H \mathbf{G}^H \mathbf{H}_B^H$, $\mathbf{B} = |\frac{1}{\sigma_E^2}|^2 \mathbf{H}_E \mathbf{G} \mathbf{w} \mathbf{w}^H \mathbf{G}^H \mathbf{H}_E^H$. (4.15c) is due to $\hat{\boldsymbol{\Theta}} = \hat{\boldsymbol{\theta}} \hat{\boldsymbol{\theta}}^H$. The problem given in (4.15) is a semi-definite programming (SDP) problem which is non-convex due to the rank constraint. Using standard procedure of solving SDP, we solve the problem while ignoring the rank constraint and obtain a rank 1 approximation using randomised rank approximation technique as given in [86]. By ignoring the rank constraint, the problem reduces to a linear-fractional programming problem which can be effectively solved with Charnes-Cooper transformation. Therefore, let $u = \frac{1}{1 + \text{Tr}(\mathbf{B} \hat{\boldsymbol{\Theta}})}$ and $\hat{\mathbf{U}} = u \hat{\boldsymbol{\Theta}}$, we reformulate convex problem in (4.16) that can be efficiently solved with cvx [72].

$$\max_{\hat{\mathbf{U}} \succeq 0, u \geq 0} u + \text{Tr}(\mathbf{A} \hat{\mathbf{U}}), \quad (4.16a)$$

$$\text{s.t. } u + \text{Tr}(\mathbf{B} \hat{\mathbf{U}}) = 1, \quad (4.16b)$$

$$\text{diag}(\hat{\mathbf{U}}) = u. \quad (4.16c)$$

4.3.1.2 Modified Approach

In order to reduce the channel overhead and considering that the eavesdropper is sometimes passive, we offer an alternative approach that relies on the channel information of the main receiver, Bob. Since the IRS elements can effectively reflect signals along the desired direction, we aim to design the optimal reflection coefficients such that the signals contribute to Bob's reception constructively. An excerpt from the discussions on the relationship between the squared magnitude of the scattered field of IRS and observation angle as given Lemma 1 in [91] alludes that maximum received power occurs at the specular reflected path of the IRS signal which by design is at Bob. This non-specular nature of the reflections allows us to consider the possibility of eavesdropping at Eve. However, since maximum power is obtained at the specular direction which is the design parameter Θ that reflects the signal to Bob. Intuitively, we can design Θ to maximise reflection at Bob as this not only simplifies the problem, it is easily tractable.

Since we know that the channels from the IRS to Bob and Eve are independent of each other but dependent on reflection coefficients, it is sufficient to optimise the reflection coefficients based on Bob's channel only. Accordingly, we design the reflection coefficients Θ , for a given trajectory \mathbf{Q} , and beamforming vector \mathbf{w} , such that it is not influenced by Eve's channel condition. It is therefore, apparent that the optimal Θ can be determined for maximising Bob's SNR γ_B . This can be done by extracting the following sub-problem from the original problem in (4.12):

$$\max_{\Theta} \gamma_B[n], \quad (4.17a)$$

$$\text{s.t. } 0 \leq \theta_k[n] \leq 2\pi. \quad (4.17b)$$

The solution obtained from solving (4.17) eventually maximises the information rate received by Bob ($\log_2(1 + \gamma_B[n])$). For each $n \in \{1, \dots, N\}$, the solution to (4.17) ensures the maximum objective value since the signals from the IRS elements are added constructively. Recall that, by examining (4.4), it is clear that the phase of the channel response linking the ground nodes ($i \in \{B, E\}$) to the UAV-carried

IRS system is subdivided into 2 parts - fixed phase (due to the relative position of the UAV) and variable phase (due to the IRS response). While the fixed phase accounts for Doppler distortions, the variable phase presents the IRS reflected system response. The variable phase can be modified to constructively combine the received reflected signals from the IRS elements. Therefore, by expanding $\mathbf{h}_B^H \mathbf{\Theta} \mathbf{G} \mathbf{w}$, we construct the reflection coefficient to maximise the received signal at Bob as given in (4.18).

Following similar derivation as in [87, 92], it is easy to see that for each $n \in \{1, \dots, N\}$, the solution to (4.17) was given by

$$\boldsymbol{\theta} = \theta_{\text{com}} - \mathbf{u}_B + \mathbf{u}_G, \quad (4.18)$$

where $\boldsymbol{\theta} = [\theta_1, \dots, \theta_K]^T$, $\mathbf{u}_B = [\phi_{1B}^b, \dots, \phi_{KB}^b]^T$ and \mathbf{u}_G is the maximum left singular vector corresponding to the rank-1 (low rank) approximation of $\mathbf{\Phi}_G$. θ_{com} is an arbitrary phase common to all elements of the IRS. This phase allows for the cancellation of unscrupulous phase elements at the receiver arising from the direct link between the Alice and Bob [45, 92]. However, since there are no direct paths between the Alice and the ground receiver nodes as described in Section 4.2, θ_{com} can be set to zero without loss of generality.

By the definition of $\mathbf{\Theta}$ given in (4.18) and the knowledge of the channel matrices, we define Proposition 4.1 at Bob and Eve for each $n \in \{1, \dots, N\}$ as:

Proposition 4.1: $\mathbf{h}_i^H \mathbf{\Theta} \mathbf{G} = \boldsymbol{\chi}_i$, where the elements of $\boldsymbol{\chi}_i = [\chi_{1i}, \dots, \chi_{Mi}]$ are presented in (4.19a) and (4.19b) for $i \in \{B, E\}$, respectively:

$$\chi_{mB} = K \sqrt{c_{RB} c_{mR}} \exp(-j(\phi_{mR}^a + \phi_{RB}^a - \theta_{\text{com}})), \quad (4.19a)$$

$$\begin{aligned} \chi_{mE} = & \sqrt{c_{RE}c_{mR}} \exp(-j(\phi_{RE}^a + \phi_{mR}^a - \theta_{com})) \\ & \times \left(\sum_{k_x=1}^{K_x} \sum_{k_y=1}^{K_y} \exp \left(-j \left[(k_x - 1)\bar{d}_x(-\hat{\mathbf{a}}_{RE}^x + \hat{\mathbf{a}}_{RB}^x - \hat{\mathbf{a}}_{mR}^x) \right. \right. \right. \\ & \left. \left. \left. + (k_y - 1)\bar{d}_y(-\hat{\mathbf{a}}_{RE}^y + \hat{\mathbf{a}}_{RB}^y - \hat{\mathbf{a}}_{mR}^y) + u_G^{k_x, k_y} \right] \right) \right), \quad (4.19b) \end{aligned}$$

where $u_G^{k_x, k_y}$ is the k th element of u_G .

Proof: By substituting and simplifying the expressions for \mathbf{h}_i , $\mathbf{\Theta}$, and, \mathbf{G} given in equations (4.9), (4.18) and (4.6) respectively, it is easy to see that \mathbf{u}_G in (4.18) is designed as a rank-1 approximation to cancel out the variations of the columns of matrix $\mathbf{\Phi}_G$. However, we know that the rank-1 approximation error of \mathbf{u}_G increases as $r > 0$ since the sensor are randomly placed over large area, hence $|\mathbf{u}_G - \mathbf{\Phi}_G(:, m)| \geq 0$. However, from experimentation, for small values of r , $|\mathbf{u}_G - \mathbf{\Phi}_G(:, m)| \approx 0$ allowing the cancellation of $\mathbf{\Phi}_G$. This completes the proof of the proposition. ■

Using exponential sum formulas, (4.19b) can be further simplified as

$$\begin{aligned} \chi_{mE} = & \sqrt{c_{RE}c_{mR}} \exp \left(-j \left(\frac{2\pi}{\lambda} (d_{RE} + d_{mR}) \right) \right) f(K_x, K_y) \\ & \times \exp \left(j \left(\theta_{com} + \frac{A_x(K_x - 1)}{2} + \frac{A_y(K_y - 1)}{2} \right) \right), \quad (4.20) \end{aligned}$$

where $f(K_x, K_y) = \frac{\sin(\frac{1}{2}K_x A_x) \sin(\frac{1}{2}K_y A_y)}{\sin(\frac{1}{2}A_x) \sin(\frac{1}{2}A_y)}$, $A_x = \bar{d}_x(\hat{\mathbf{a}}_{RE}^x + \hat{\mathbf{a}}_{RB}^x - \hat{\mathbf{a}}_{mR}^x)$ and $A_y = \bar{d}_y(\hat{\mathbf{a}}_{RE}^y + \hat{\mathbf{a}}_{RB}^y - \hat{\mathbf{a}}_{mR}^y)$. It is easily observed that the number of IRS elements on the UAV will affect the SNR received at Bob and Eve differently. While all choices on the number IRS elements is guaranteed to improve on the SNR at the Bob (refer to (4.19a), especially as the number increases to infinity, the reverse is not obtained at Eve due to the function $f(K_x, K_y)$. Hence, the selection of the number of IRS element must be made to ensure that the SNR at Eve is minimised with largest phase distortion possible.

Following Proposition 4.1, we infer that the maximum SNR values at Bob and Eve are

$$\gamma_B \leq \sum_{m=1}^M \frac{\bar{P} \varsigma_B \varsigma_k (\rho_0 K)^2}{d_{RB}^2 d_{mR}^2}, \quad (4.21a)$$

$$\gamma_E \leq \sum_{m=1}^M \frac{\bar{P} \varsigma_E \varsigma_k (\rho_0 |\zeta|)^2}{d_{RE}^2 d_{mR}^2}, \quad (4.21b)$$

respectively, where $\bar{P} = \frac{P}{\sigma_i^2}$ and

$$|\zeta|^2 = \sum_{k_x=1}^{K_x} \sum_{k_y=1}^{K_y} \exp \left(j \left[(k_x - 1) \bar{d}_x (\hat{\mathbf{a}}_{RE}^x + \hat{\mathbf{a}}_{RB}^x - \hat{\mathbf{a}}_{mR}^x) + (k_y - 1) \bar{d}_y (\hat{\mathbf{a}}_{RE}^y + \hat{\mathbf{a}}_{RB}^y - \hat{\mathbf{a}}_{mR}^y) + u_G^{k_x, k_y} \right] \right) \stackrel{(a)}{\leq} K. \quad (4.22)$$

Note that the SNR bounds in (4.21) invariably define the worse case of the average secrecy rate. From (4.22), the equality in (a) represents the worst-case scenario and arises when the channel of Bob and Eve are highly correlated. This may occur in the unlucky event when Eve is located at the exact position of Bob (e.g. an application in the device of Bob becoming the potential Eve).

4.3.2 Solving for \mathbf{w}

We adopt two different design strategies for the beamforming weights \mathbf{w} , with known trajectory, \mathbf{Q} , and reflection coefficients, Θ .

4.3.2.1 Generic Approach

Taking the eavesdropper's information into consideration, we reformulate (4.11) as

$$\max_{\mathbf{w}} \left(\frac{1 + \mathbf{w}^H \mathbf{A} \mathbf{w}}{1 + \mathbf{w}^H \mathbf{B} \mathbf{w}} \right), \quad (4.23a)$$

$$\text{s.t. } \mathbf{w}^H \mathbf{w} \leq P, \quad (4.23b)$$

where $\mathbf{A} = \frac{1}{\sigma_B^2}(\mathbf{h}_B^H \boldsymbol{\Theta} \mathbf{G})^H (\mathbf{h}_B^H \boldsymbol{\Theta} \mathbf{G})$, $\mathbf{B} = \frac{1}{\sigma_E^2}(\mathbf{h}_E^H \boldsymbol{\Theta} \mathbf{G})^H (\mathbf{h}_E^H \boldsymbol{\Theta} \mathbf{G})$. This implies that by considering the presence of both Bob and Eve, the optimal $\mathbf{w}^* = \sqrt{P} \mathbf{u}_{\max}$, where \mathbf{u}_{\max} is the eigenvector corresponding to the maximum eigenvalue of the matrix $(\mathbf{B} + \frac{1}{P} \mathbf{I}_M)^{-1} (\mathbf{A} + \frac{1}{P} \mathbf{I}_M)$ [90, 98].

4.3.2.2 Modified Approach

Since the IRS can direct signals to specific targets, we consider transmission to Bob only ignoring the presence of Eve. Then the (4.12) reduces to

$$\max_{\mathbf{w}} (1 + \mathbf{w}^H \mathbf{A} \mathbf{w}), \quad (4.24a)$$

$$\text{s.t. } \mathbf{w}^H \mathbf{w} \leq P, \quad (4.24b)$$

where $\mathbf{A} = \frac{1}{\sigma_B^2}(\mathbf{h}_B^H \boldsymbol{\Theta} \mathbf{G})^H (\mathbf{h}_B^H \boldsymbol{\Theta} \mathbf{G})$. It is known that the optimal $\mathbf{w}^* = \sqrt{P} \mathbf{u}_{\max}$ is a maximum ratio transmission (MRT) beamformer towards the UAV, where \mathbf{u}_{\max} is the eigenvector corresponding to the maximum eigenvalue of the channel matrix $\frac{1}{\sigma_B^2}(\mathbf{h}_B^H \boldsymbol{\Theta} \mathbf{G})^H (\mathbf{h}_B^H \boldsymbol{\Theta} \mathbf{G})$ [92, 94]. This solution ensures that the determination of the weights are independent of the presence of Eve. In this work, we examine the performance characteristics of both schemes in order to determine their impact on the average secrecy rate.

4.3.3 Solving for Q

In this subsection, we investigate methods to obtain the trajectory of the UAV carrying the IRS system for both: i) known eavesdropper's location and ii) unknown eavesdropper's location.

4.3.3.1 Generic Approach

Now, to obtain the trajectory of the UAV for known IRS reflection coefficients, $(\boldsymbol{\Theta})$ and beamforming vectors, \mathbf{w} with knowledge of the location of Eve, (4.11) was

reformulated as (4.25):

$$\max_{\mathbf{Q}} \sum_{n=1}^N \left[\log_2 \left(\frac{1 + \gamma_B[n]}{1 + \gamma_E[n]} \right) \right] \quad (4.25a)$$

$$\text{s.t. } \|\mathbf{q}[n] - \mathbf{q}[n-1]\|^2 \leq (Z\alpha)^2. \quad (4.25b)$$

Note that the (4.25) is non-convex due to the fractional objective. Equation (4.25) was solved by introducing an auxiliary variable, β limiting the maximum achievable rate by Eve. Furthermore, considering that the distance between the sensors in Alice is very small compared to the distance, between Alice and the UAV-carried IRS, we can assume for simplification that the UAV trajectory is determined in respect to Alice rather than the individual sensors, ($d_{mR} \approx d_{AR}$). Therefore, we reformulate the trajectory problem as (4.26) by expanding γ_i from (4.21).

$$\max_{\mathbf{Q}, \beta} \sum_{n=1}^N \left[\log_2 \left(\frac{1 + \left(\frac{\bar{P}M(\rho_{0SE}K)^2}{d_{RB}^2 d_{AR}^2} \right) [n]}{\beta[n]} \right) \right], \quad (4.26a)$$

$$\text{s.t. } 1 + \left(\frac{\bar{P}M(\rho_{0SE}K)^2}{d_{RB}^2 d_{AR}^2} \right) [n] \leq \beta[n] \quad (4.26b)$$

$$\|\mathbf{q}[n] - \mathbf{q}[n-1]\|^2 \leq (Z\alpha)^2. \quad (4.26c)$$

Equation (4.26) can be solved using Karush-Kuhn-Tucker (KKT) conditions to obtain the optimal trajectory of the UAV as defined in Proposition 4.2. A detailed proof is relegated to Appendix C.

Proposition 4.2: Given the maximum achievable rate at Eve is β , the optimal location of the UAV during the n th sample ($n \in [1, \dots, N]$) can be obtained by solving

$$q_x^2[n] + q_y^2[n] = (\varepsilon[n] \|\Omega_A\|)^2 - H^2, \quad (4.27)$$

where the closed form expression of ε is given in (4.28).

Proof: See Appendix C. ■

$$\varepsilon[n] = \frac{\frac{1}{3\sqrt[3]{2}} \sqrt[3]{2b^3 + 3\sqrt{3}\sqrt{-4b^3d - b^2c^2 + 18bcd + 4c^3 + 27d^2} - 9bc - 27d - \sqrt[3]{2}(3c - b^2)}}{3\sqrt[3]{2b^3 + 3\sqrt{3}\sqrt{-4b^3d - b^2c^2 + 18bcd + 4c^3 + 27d^2} - 9bc - 27d} + \frac{b}{3}} \quad (4.28)$$

$$\text{where } b = \frac{\|\mathbf{\Omega}_B\|}{2\|\mathbf{\Omega}_A\|} + 2\frac{\|\mathbf{q}[n-1]\|}{\|\mathbf{\Omega}_A\|} + \frac{1}{2}, \quad c = \frac{\|\mathbf{\Omega}_B\|\|\mathbf{q}[n-1]\| + \|\mathbf{q}[n-1]\|^2}{\|\mathbf{\Omega}_A\|^2} - \frac{\|\mathbf{q}[n-1]\|}{\|\mathbf{\Omega}_A\|},$$

$$d = \frac{\|\mathbf{\Omega}_B\|}{2\|\mathbf{\Omega}_A\|} \frac{\|\mathbf{q}[n-1]\|^2}{\|\mathbf{\Omega}_A\|^2} + \frac{\|\mathbf{q}[n-1]\|^2}{2\|\mathbf{\Omega}_A\|^2} - \frac{(Z\alpha)^2}{2\|\mathbf{\Omega}_A\|^2}$$

The solution to (4.27) can easily be obtained by a linear search algorithm that seeks for pairs of points that satisfy the trajectory constraint in (4.26c). We recall that the trajectory is related to the solution of (4.27) by $\mathbf{Q} = \{\mathbf{q}[n] = [q_x[n], q_y[n], H]^T, n \in \{1, \dots, N\}\}$. It can be deduced from Proposition 4.2 that the trajectory of the UAV is not dependent on the knowledge of the rate received at Eve or Bob but on the exact location of Bob, Alice and the distance covered by the UAV during the n th sample. This ensures that the rate regulation (varying β) for Eve is insignificant in determining all the possible locations of the UAV for $n \in \{1, \dots, N\}$. However, while conducting the linear search to obtain the optimal location among the possible locations, the knowledge of the location of Eve influences the choice leading to the trajectory of the UAV as obtained in fig. 4.3.

4.3.3.2 Modified Approach

We now assume that the location of the eavesdropper is unknown. Therefore, we cannot access the channel information of the eavesdropper. The best thing we can do is to find the optimal UAV trajectory based on the legitimate channel only. Therefore, (4.11) can be presented in terms of the trajectory as (4.29):

$$\max_{\mathbf{Q}} \sum_{n=1}^N [\log_2(1 + \gamma_B[n])] \quad (4.29a)$$

$$\text{s.t. } \|\mathbf{q}[n] - \mathbf{q}[n-1]\|^2 \leq (Z\alpha)^2. \quad (4.29b)$$

The solution to (4.29) was obtained from its KKT solution by solving (4.27) with the definition for ε as:

$$\varepsilon = \frac{\|\mathbf{q}_R[n-1]\| \pm Z\alpha}{\|\boldsymbol{\Omega}_A\|}.$$

A linear search method as described in section 4.3.3.1 is employed until the points maximising the objective function in (4.29) was obtained.

4.3.4 Overall Iterative and Non-iterative Algorithm

The overall iterative and non-iterative algorithm is presented in algorithm 3 and 4 respectively. The convergence of the iterative algorithm (algorithm 3) was presented in fig. 4.2. A fast convergence of the iterative process of was observed through numerical simulations for different $n \in \{1, \dots, N\}$ samples.

Algorithm 3 Generic model iterative algorithm for solving $\boldsymbol{\Theta}$, \mathbf{w} , and \mathbf{Q}

- 1: Initialise \mathbf{w}^0 and \mathbf{q}^0 such that the constraints in (4.11d) and (4.11c) are respectively satisfied. Then solve the objective value defined in (4.11a) as R_s^0
 - 2: $m \leftarrow 1$.
 - 3: **repeat**
 - 4: Solve (4.26) and update \mathbf{q}^m .
 - 5: Using the grid cell, \mathbf{q}^m , d_x , and d_y , compute the locations of the IRS elements, \mathbf{Q}^m .
 - 6: Determine the channel impulse responses using the definitions in (4.6) and (4.9).
 - 7: For each $n \in \{1, \dots, N\}$, solve (4.16) to obtain $\boldsymbol{\Theta}^m$.
 - 8: Compute and update \mathbf{w}^m with solutions described in 4.3.2.
 - 9: Compute R_s^m as defined in (4.11a).
 - 10: Compute $\epsilon = \left| \frac{R_s^m - R_s^{m-1}}{R_s^m} \right|$.
 - 11: $m \leftarrow m + 1$.
 - 12: **until** $\epsilon \leq 10^{-5}$ OR $m \geq 200$.
 - 13: **Output:** $\boldsymbol{\Theta}^m$, \mathbf{w}^m and \mathbf{Q}^m .
-

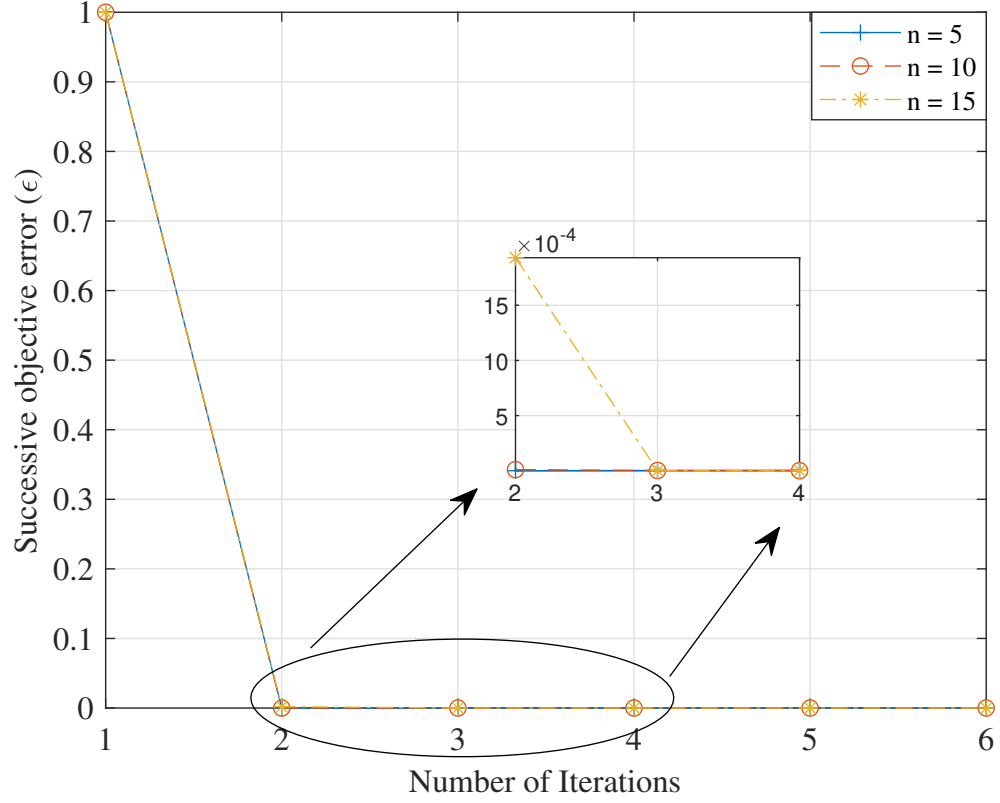


FIGURE 4.2: Convergence on iterative algorithm 3

Algorithm 4 Non-Iterative algorithm for solving Θ, \mathbf{w} , and \mathbf{Q}

- 1: Solve (4.27) and update \mathbf{q} .
 - 2: Using the grid cell, \mathbf{q} , d_x , and d_y , compute the locations of the IRS elements, \mathbf{Q} .
 - 3: Determine the channel impulse responses using the definitions in (4.6) and (4.9).
 - 4: For each $n \in \{1, \dots, N\}$, solve (4.18) to obtain Θ .
 - 5: Compute and update \mathbf{w} with solutions described in 4.3.2.
 - 6: Compute R_s as defined in (4.11a).
 - 7: **Output:** Θ , \mathbf{w} and \mathbf{Q} .
-

4.4 Results and Discussions

In this section, we evaluate the performance of the proposed algorithm via numerical simulations and compare with baseline schemes. The parametric settings of the simulation environment were given in table 4.1 except where explicitly stated.

TABLE 4.1: Parameters for UAV-carried IRS simulation

Simulation parameter	Symbol	Value
Number of sensors	M	4
Centre of Alice	Ω_A	$[0, -100, 0]^T$
Bob location	Ω_B	$[80, 100, 0]^T$
Eve location	Ω_E	$[-100, 50, 0]^T$ (Uncorrelated) $[75, 100, 0]^T$ (Correlated)
Fixed IRS location	Ω_{fixIRS}	$[50, 0, 20]^T$
Initial UAV location	\mathbf{q}_o	$[-100, 100, H]^T$
UAV flight altitude	H	100m
UAV time of flight	T	300s
Velocity per sample	Z	3m/s
Duration per sample	α	0.5s
Transmission frequency	f	900 MHz
Number of IRS elements	K	16
IRS separation	$d_x = d_y$	$\frac{\lambda}{4}$
Noise	$\sigma_B^2 = \sigma_E^2$	30dBm
Signal-to-noise ratio at reference distance of 1m	ρ_o	60dBm (Strong), 30dBm (Weak)

We use the methods summarised in algorithms 3 and 4 to optimise the parameters. The initial values of the iterative method in algorithm 3, satisfies the feasibility problem³ of (4.11). The legend of the figures describe the various scenarios implemented

³The feasibility problem was obtained by setting the objective value to 0 and solving the optimisation problem. This gives the initial values to the parameters used to start the iteration.

as:

1. Scheme 1: Refers to the UAV-carried IRS scenario where the knowledge of the channel characteristics of the eavesdropper (Eve) is unknown.
2. Scheme 2: Refers to the UAV-carried IRS scenario where the knowledge of the channel characteristics of the eavesdropper (Eve) is known.
3. Fixed: Refers to the algorithm 1 given in [90]. To adapt the algorithm to the scenario described herein, we replaced the structured transmit antenna at the AP with a sensor network, set the direct link between Alice and Bob/Eve to 0 and defined the channel as explained in this chapter.

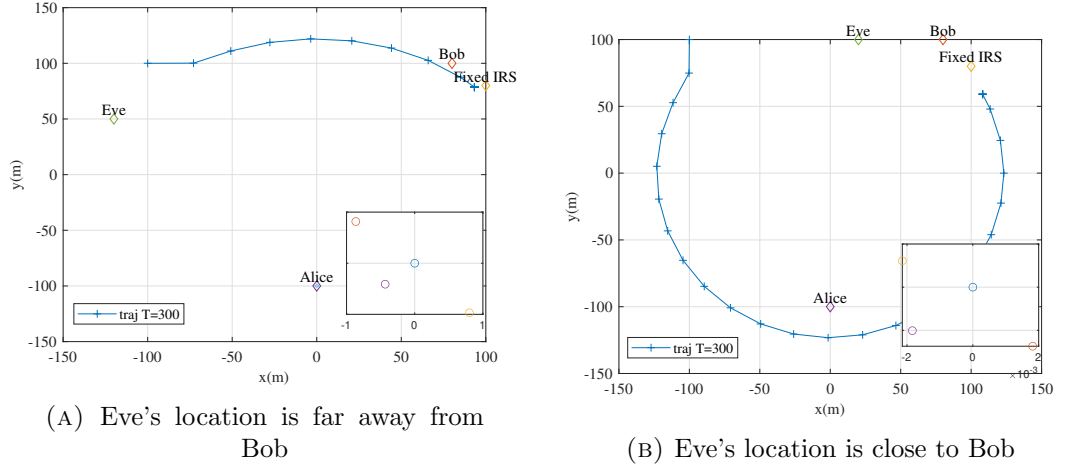


FIGURE 4.3: UAV trajectory for different locations of Eve.

Figure 4.3 presents the trajectory of the UAV as we change the location of Eve. We consider when Eve location is far away from Bob and when it is close to Bob in the sub-figures. The UAV attempts to find paths that are as far from Eve as possible while maintaining reasonable distance between Alice and the Bob to ensure the transmitted signals are received and reflected. When a safe distance was obtained, the UAV hovers around that location until the end of the simulation. This behaviour of the UAV is similar at different scheduled flight times. Intuitively, since the IRS use passive beamforming, the distance travelled by the reflected signal is required to be small while maintaining LoS with Alice. The active beamforming at the Alice

ensures that the transmitted signal were directed to the IRS on the UAV, since it can adjust the transmitted power where necessary. The trajectory of the UAV collaborates the conclusion in [91] having shown that the received signal power at Bob is proportional to the square of the IRS area and inverse square propagation distance, $\frac{1}{(d_{AR}d_{RB})^2}$. Therefore, the optimal IRS placement should aim to minimise $d_{AR}d_{RB}$ as obtained via the UAV. Furthermore, the position of Eve determines the trajectory while the position of the main receiver (Bob) determines the optimal location for the UAV-carried IRS system.

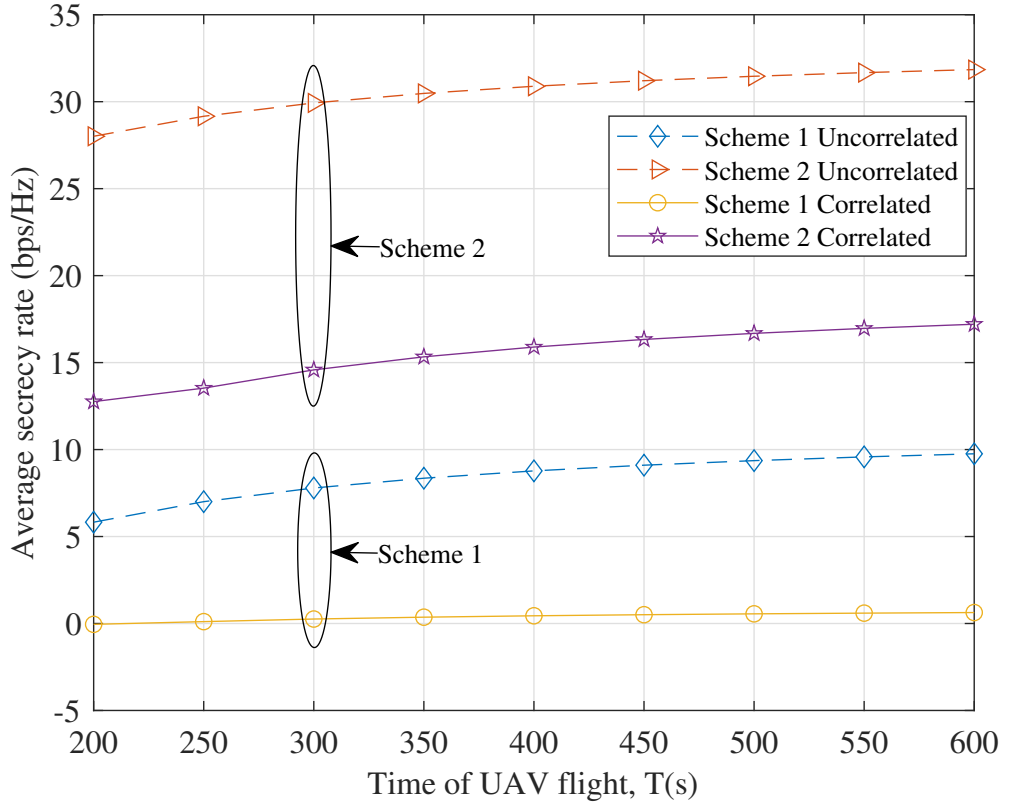


FIGURE 4.4: Average secrecy versus time of flight (T) for different transmit power (dBm) for $K = 16$, $r = 1\text{m}$, $\rho_0 = 120\text{dBm}$, and $P = 1\text{dBm}$

Following the trajectory presented in fig. 4.3, it was observed in fig. 4.4 that the longer the UAV flies with the IRS for a given communication, the better the average secrecy rate for both beamforming weight schemes under consideration. It has been established in [92] that for aerial IRS, the SNR increases with higher transmit power. However, due to the IRS, we showed that the SNR for Eve declines leading to an

increase in the average secrecy rate as observed in the rate of the Eve in fig. 4.6. Similar performance was observed in the fixed IRS scenario as reported in [90]. Figure 4.4 also provides an insight that scheme 2 performs better than scheme 1 when the channels of Bob and Eve are correlated and uncorrelated in terms of average secrecy rate.

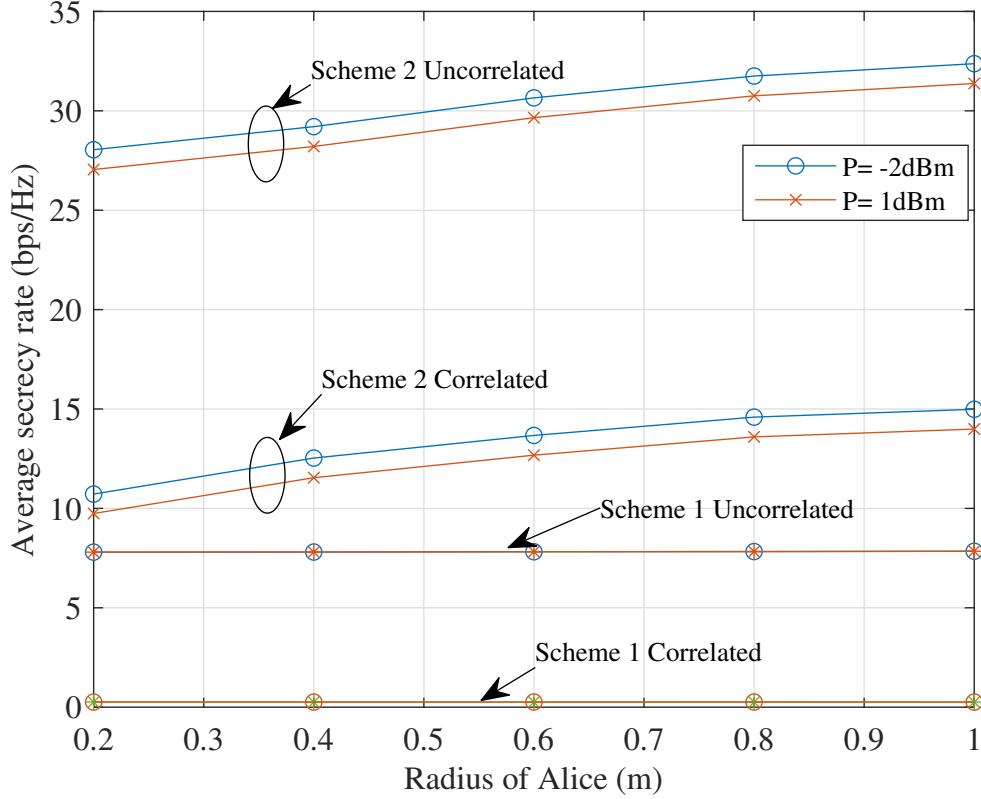


FIGURE 4.5: Average secrecy rate versus Radius of sensor location for $K = 16$ and $T = 300s$

In fig. 4.5, the density of the sensors that acted collaboratively to transmit via the UAV-IRS system was varied by increasing their location area. It was observed that varying the radius of the area led to increased average secrecy rate performance. This is primarily because increase in the radius allows the sensors to be scattered over a larger area ensuring that the Φ_G is not rank 1 and introducing greater variability for the eavesdropper (Eve). We note that since the design of the reflection coefficients, Θ , focused on maximising the quality of signal received at Bob, the impact of the

variations obtained given that the rank of Φ_G is not 1 at Bob was reduced by the design of Θ .

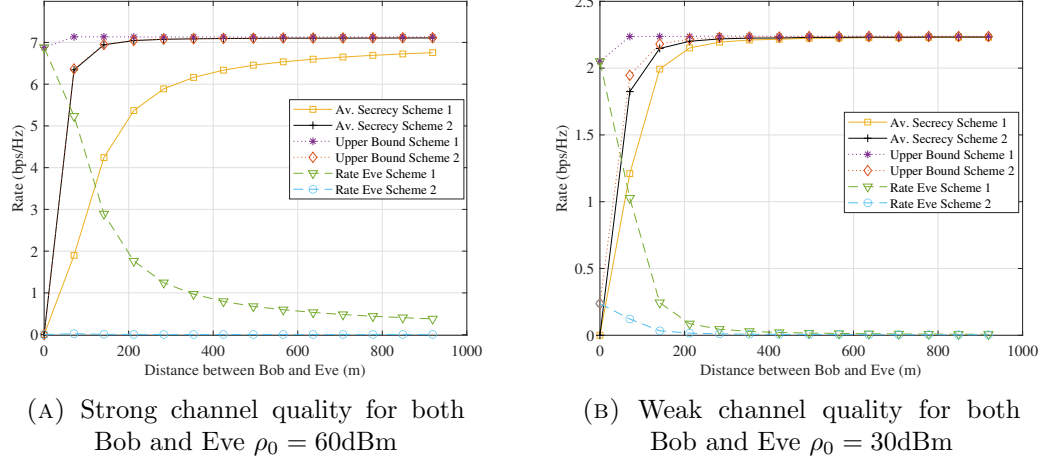


FIGURE 4.6: Average secrecy rate versus distance between Bob and Eve for $K = 16$, $r = 1\text{m}$, $P = 10\text{dBm}$ and $T = 300\text{s}$.

Furthermore, we test the effect of varying the distance⁴ between the eavesdropper and the legitimate receiver in fig. 4.6. The plots of the upper bounds of the the average secrecy rate which was obtained by setting the eavesdropper's reception to zero was used in the figure to evaluate the performances. First, we observe that the rates of the eavesdropper in Scheme 2 is almost zero regardless of the channel quality of the legitimate receiver. However, as the distance between Bob and Eve increases, the rates received by Eve tends to gradually fall to zero in Scheme 1. Following these variations in the rates received by Eve, the average secrecy rates tends to the upper bound faster with Scheme 2 than Scheme 1 as the distances increase. The deduction from fig. 4.6 presents that when the eavesdropper is passive as with Scheme 1, the designs of the trajectory, beamforming and reflection coefficients are more stringent compared with Scheme 2. Nevertheless, the trade-off in the lower performance of Scheme 1 compensates for the removal of the assumption about the knowledge of the channel information of the eavesdropper.

⁴Since the channels in this chapter were modeled as a function of distance, the distance between Bob and Eve = $\|\mathbf{\Omega}_B - \mathbf{\Omega}_E\|$ examines the similarity between Bob and Eve in terms of their proximity. Lower values indicate highly correlation while higher values indicate highly uncorrelated [99, 100].

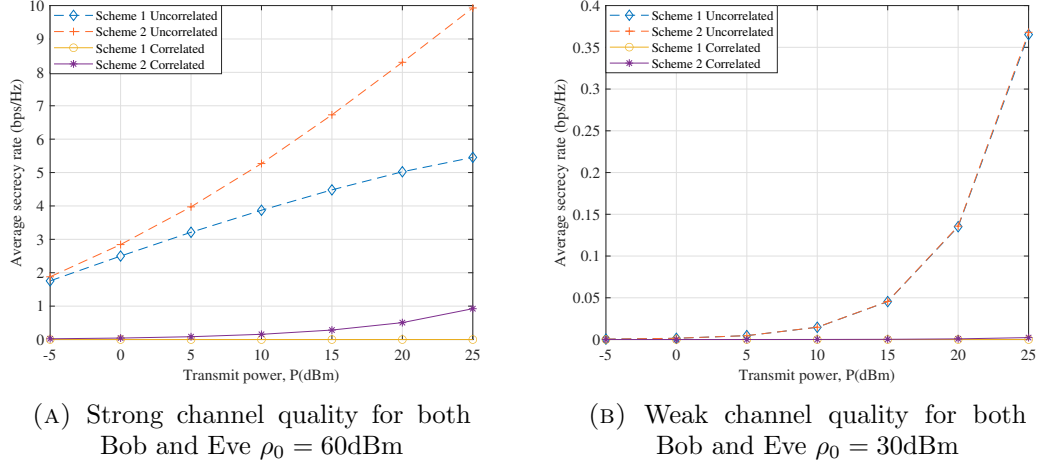


FIGURE 4.7: Average secrecy rate versus transmit power for $K = 16$, $r = 1\text{m}$ and $T = 300\text{s}$.

In fig. 4.7, the impact of transmit power on the average secrecy rate of the system was presented. By comparing the sub-figures, scheme 2 out-performs scheme 1 when the channel quality of Bob and Eve are strong (represented by different values of ρ_0) and highly uncorrelated. Similar assertion was observed in fig. 4.6 while examining the influence of distance between Bob and Eve representing correlation. In fig. 4.6a and fig. 4.7a, we note that scheme 2 was designed with the perfect knowledge of Eve, therefore, the information rate received by Eve is only maximum when the correlation between the channels of Bob and Eve is highest and declines rapidly as the distance between Bob and Eve increases. A combination of the benefits of the beamforming weights in scheme 2 and the optimised reflection coefficients easily cause its average secrecy rate to the upper bound, which is the rate of Bob. Nevertheless, since the beamforming weights for scheme 1 was designed ignorant of Eve, the information rate received at Eve was influenced only by the reflection coefficients. In contrast to these observations, figs. 4.6b and 4.7b, elucidates that the performance in terms of both schemes 1 and 2 are similar when the channel quality of Bob and Eve are poor and uncorrelated. This is an interesting result as it provides reasonable justification deploying scheme 1 especially when the exact location of Eve is unknown under noisy channel conditions.

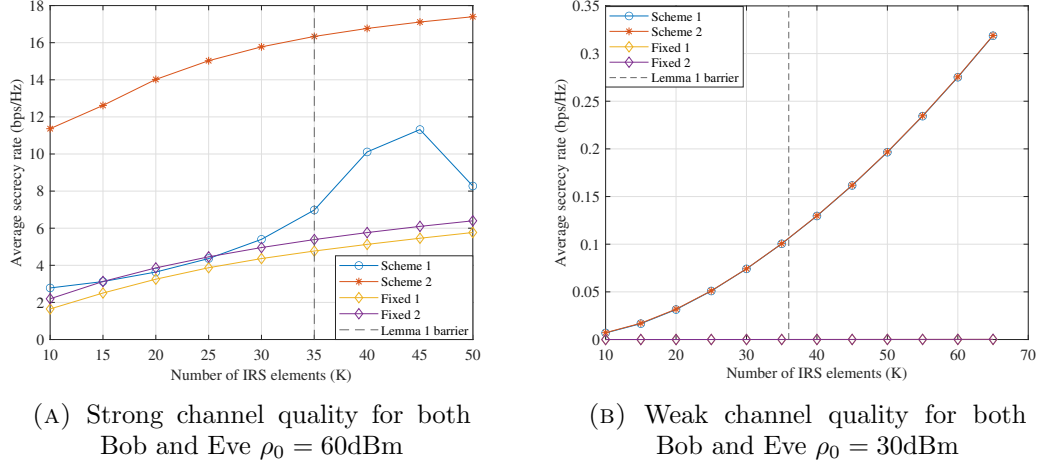


FIGURE 4.8: Influence of the number of IRS on Average secrecy rate at uncorrelated formation of Eve and Bob channel ($r = 1\text{m}$ and $P = 10\text{dBm}$, $T = 300\text{s}$).

In fig. 4.8, the number of IRS elements mounted on the UAV was varied to observe its effect on the average secrecy rate. Scheme 1 and 2 were compared to legacy IRS system where the IRS system was mounted on a fixed position. The observations showed that optimising the location of the IRS using the UAV produced better average secrecy rates despite the quality of the channel of the main receiver as shown in figs. 4.8a and 4.8b. Similar to previous reports in figs. 4.6 and 4.7, Scheme 2 out performs Scheme 1 when the channel qualities are strong. But both schemes are fairly the same with low channel quality.

Furthermore, with the 2D separation between the elements of the IRS system in horizontal and vertical directions as d_x and d_y respectively, we define Lemma 1 to determine the maximum number of IRS elements (K) to guarantee the average secrecy rate defined in the objective of (4.11). Lemma 1 was stated as a consequence of the dependent of the beamwidth on the size of the IRS [91]. Considering PLS and noisy channel environment, the effect of the Lemma was shown in fig. 4.8.

Lemma 1: For a noisy channel, given that d_x and d_y are fractions of λ , such that $d_x = \frac{\lambda}{z_x}$ and $d_y = \frac{\lambda}{z_y}$, then it holds that $K_x \leq z_x$ and $K_y \leq z_y$

Proof: It is known that for IRS plate width larger than λ , the required local phase is coarsely quantised and will cause a mismatch between the desired reflection angle

and the IRS array response in its far field [91]. It is apparent, then, to constrain the width of the entire IRS system within the bound of λ such that $d_x K_x \leq \lambda$ and $d_y K_y \leq \lambda$ in order to minimise reflection mismatch. Simplifying the relations, completes the proof of Lemma 1. From the Lemma 1, it is easy to see that $K \leq z_x z_y$ and the area of the entire IRS plate is upper bound by λ^2 . ■

Due to the inverse relation between the beamwidth and the IRS plate width as given in [91], we know that provided the bound of Lemma 1 is sustained, the beamwidth reflected from the IRS will be smaller for increasing number of IRS elements, K . This implies that the average secrecy rate of the system will increase for large values of K since the reflected beam will be focused on Bob, thereby increasing its signal quality. This invariably increases the average secrecy rate as shown in fig. 4.8. However, fig. 4.8a shows that when Lemma 1 is not satisfied, the increased number of IRS elements do not guarantee improved average secrecy rate. This is because the reflected beamwidth is larger leading to dependency on the correlation of the eavesdropper's channel to the legitimate channel. Since there are mismatch between the reflection angle and the IRS array response, the eavesdropper has greater chance of receiving signal that can sum constructively. Interestingly, it was observed that for weak channel shown in fig. 4.8b, Schemes 1 and 2 performance are similar without dependence on Lemma 1.

Based on the observations recorded in figs. 4.6, 4.7 and 4.8, we assert that the use of the non-iterative algorithm given in Algorithm 4 and represented as Scheme 1 in the figures is best suited for PLS with poor channel conditions. Also, Scheme 1 is also valuable when the knowledge of information about the eavesdropper's channel is unavailable, considering that positive secrecy rates that were higher than the fixed IRS scheme were obtained.

4.5 Chapter Summary

In this chapter, an IRS system was carried on a UAV. The setup was used to reflect data to desired receiver while eluding the passive eavesdropper. Since the IRS causes maximum power transfer at the legitimate receiver, the PLS of the system was guaranteed provided there were no direct link between the transmitters and receivers. The IRS causes the passively beamformed signal to be destructive at illegitimate receivers. The problem described was reduced to its analytical formulations in the chapter and solutions were obtained to define key adjustable parameters of the scenario. The parameters include the UAV trajectory, transmit beamforming weights and the reflection coefficients of the IRS. Based on the formulated problem and the results obtained via numerical simulations, the optimal solution to the parameters were obtained by using iterative means. In the chapter, we further proposed a non-iterative means to obtain the solution as a low complex alternative to the iterative means. The non-iterative approach considers that the eavesdropper is passive and is best suited with poor channel quality of the receivers.

Chapter 5

Physical Layer Security for Joint Wireless Communications and Sensing

Consider a typical sandwich of RADAR and wireless communication application, traditionally operating diverse spectrum bands but requiring cohabitation to maximise spectrum usage. The postulate of this chapter seeks to enhance the security challenge (in terms of PLS) of the cohabitation by harnessing the interference and power requirements. We note that in chapters [2](#) and [3](#) of the thesis, jamming signals were externally introduced as interfering signal to improve the PLS of the wireless communication model. In this chapter, the interfering signals due to the cohabitation was harnessed as a tool to improve on PLS. The RADAR signal interferes with the wireless communication signal creating pseudo interference signal that can be harnessed for jamming. Therefore, in this chapter, wireless communication receiver sensing was explored as a means of enhancing PLS. An example of communication sensing was shown with cohabiting RADAR and wireless communication signals in the presence of a passive eavesdropper. The background and prospect of wireless communication sensing were established in section [5.1](#). Thereafter, section [5.2](#)

reviewed the related works on wireless communication sensing and RADAR cohabitation as a case study. Based on the review, the system model and problems were formulated for the chapter in section 5.3. Section 5.4 discussed the solutions to the problems using conventional optimisation tools and autoencoders for passive eavesdropper. The solution focused on mitigating the impact of the interference on the legitimate receivers to improve on PLS. The numerical solutions to the models were simulated and results discussed in section 5.5. The chapter summary was presented in section 5.6 to conclude the chapter.

5.1 Prospects of Communication Sensing

In order to avoid interference and efficiently utilise the limited radio resources, standardisation bodies in different countries/regions adopted a fixed frequency allocation scheme [101, 102] popularly referred to as fixed spectrum allocation (FSA). The scheme allowed various services requiring radio resources to be statically classified, and definite frequency range ascribed to the classification. Such services include various generations of wireless communications, RADAR, microwave, scientific and medical applications, etc. However, the fixed structure increasingly began to pose several bottlenecks as new radio resource use-cases increased. That was because some allocated frequency bands were increasingly been over utilised or under-utilised depending on geographical region, time, and circumstances. As a means for efficient utilisation, flexible radio resource allocation schemes were exploited and referred to as dynamic spectrum allocation (DSA).

The DSA techniques can be classified as cooperative and non-cooperative schemes [47]. The former considers that agreements were reached by users to mitigate interference but the latter emphasise that users act independently but conscious of minimising interference. A general classification model were discussed in [101, 102] and summarised herein.

1. Exclusive model: This scheme statically allocates frequency bands for different applications use real-time measures to determine users exclusive rights. Although applications maintain allotted frequency bands, the bands can change depending on agreed measure like traffic pattern or size.
2. Spectrum commons model: All users are allowed to compete equally for available resources with or without some restrictions. While the former was referred to as managed commons, the latter was termed open sharing model. A typical example is the unlicensed industrial, scientific, and medical (ISM) bands.
3. Hierarchical access model: In this model, spectrum roles are assigned to users depending on user rights priority. Such roles are for primary users roles (highest priority), secondary users roles and dual roles (priority change due to circumstances) [47]. Frequency bands are allotted to primary users but they are open to sharing by secondary users provided that the interference by the secondary users are relatively low, usually below a set threshold. To maintain the interference levels, 3 distinct approaches are readily available:
 - a) Spectrum underlay: The secondary users have low range requiring low transmission power but can transmit simultaneously with the primary users. In this case, strict constraints are placed on the transmission power in order to minimise the interference level.
 - b) Spectrum overlay: In this setup, the secondary users can transmit simultaneously with the primary users on the same channel provided it acts as a relay for the primary users.
 - c) Spectrum interweave: This requires the secondary users to observe the spectrum in order to find transmission opportunities, usually when the primary users are absent. These opportunities must ensure minimum interference levels to the primary users. This category leads to the concept of spectrum sensing or referred in some literature as opportunistic spectrum access. A typical example is the functionality of cognitive radios [102].

Spectrum sensing can be conducted by observing the energy of the channels (primary users increase energy level of the channel), or the signal pattern (specific signal properties like headers and/or trailers are sought after) or waveform (regular patterned waveform indicate presence of a primary user) [102].

Due to recent advances in vehicular infrastructure, and the prospects of beyond 5G communications, emphasis is arising for studies into the feasibility of the collaboration between various applications using diverse spectrum bands [46, 47]. The requirement for collaboration was exacerbated by the congestion of the below 6GHz spectrum band mainly used for low earth spectrum applications. Spectrum users of diverse bands, in principle, can collaborate via cohabitation, co-design and cooperation [46]. This collaboration usually explores co-design and cooperation perspective. It places the burden of the collaboration on the transmission of the signals as evident with the classification of DSA. However, with the prospects of beyond 5G applications, this chapter propose to emphasise on the cohabitation of applications with traditional diverse spectrum.

In collaboration due to the cohabiting of applications, all applications use the spectrum band at the same time without priorities. The transmitting and receiving stations share the burden of the collaboration. Hence, sensing arise from the transmitters and receivers. However, several challenges mar the discourse on cohabiting collaboration. Such challenges include: interference management, varying power requirements, integration and security guarantees [46, 103]. For example, a typical paradigm to these challenges suggests that RADAR systems require high transmit power than wireless communication, but the reflected RADAR signal is usually low powered which is highly susceptible to interference from the wireless communication signals. Such exemplar describes the need for cohabitation of applications to optimise the usage of the available spectrum.

5.2 Cohabiting Collaboration: A Case Study of Joint Communication and RADAR (JCR)

Cohabitation of RADAR and wireless communication signals are broadly discussed under the dual-function RADAR communication (DFRC) and joint communication and RADAR (JCR) models using multiple input multiple output (MIMO) systems [104, 105]. While the latter presents complementary roles for both signals, the former describes a waveform that inseparably represents both signals. Overviews of the coexistence of communication and RADAR systems were presented in [106, part 1], [104, 105].

A trade-off analysis for conflicting requirements of power and signal space for a JCR half-duplex system was addressed in [107]. In [106, part 2], a scheme that estimates the communication channel while conducting RADAR target detection was proposed. The scheme use hybrid-analog-digital (HAD) beamformer to transmit pilot signals for channel estimation and target searching. Similarly, an interweave full-duplex co-existence scheme was presented in [108], where the RADAR signal was projected onto the null space of the channel matrix between the RADAR and wireless communication signals. Soft PLS guarantees cannot be obtained for the JCR systems due to the exposure of the communication signals to the RADAR target(s) and receivers. This has prioritised the exploration of DFRC schemes for PLS cohabitation. PLS of cohabiting RADAR and wireless communication systems consider that the RADAR targets and/or receivers may likely be unintended receivers of the wireless communication signals.

In the DFRC, embedded wireless communication signals can be performed on the beamforming weights or on the orthogonal waveform or vice versa [109]. Emphasising on maintaining power levels and maximising SINR, the beam pattern obtained from the co-variance matrix of the RADAR signal can be used to obtain the transmit beamforming through zero-forcing precoding [110]. Therefore, beamforming designs for full and/or half-duplex transmit and receive communication mitigates the interference between RADAR and communications signals at the expense of the PLS

of the wireless communication signals. However, to ameliorate the PLS concerns, the wireless communication signal and some artificial noise (AN) were embedded onto the beamforming weights of the RADAR transmission [111]. Furthermore, the DFRC system was implemented by using the main lobe for RADAR and the sidelobes for communication transmissions [112]. The wireless communication signals were embedded in the signal waveforms determined by 2 different beamforming weights (representing 0 and 1). Although attempts were made by [111] and [112] to incorporate PLS in DFRC system, they were transmission-centred, based on statistical knowledge of the channel impulse and required handshake between the communication transmitter and genuine receivers.

Nevertheless, if real-time channel information or noise impact were unavailable PLS and interference management challenges become exacerbated. This is further worsened when the establishment of communication handshake is impossible. Considering autonomous multi-application domain, it is apparent that the receiver systems become equipped with interference cancellation abilities to maximise the quality of received signal and improve on the PLS of the wireless communication. Therefore, in this chapter, the designs of a PLS receiver based on interference cancellation algorithm were presented. The key contributions are enumerated.

1. We first evaluate the performance of the communication and RADAR cohabiting system when its design allow for the cancellation of the interfering signals to both receivers. This was achieved by assuming the channel information are available and nulling the interfering transmissions with beamforming weights.
2. Furthermore, relaxing the assumption on the channel information (i.e. by considered that the channel information are unknown), this chapter proposes an interference mitigation scheme implemented with autoencoders. We focus on separating transmitted wireless communication and RADAR signals at the receiver of the legitimate communication user and the RADAR receiver system using novel noise and interference cancellation filter. Our novel approach entails the use of autoencoders at the receivers to filter out the interfering and

noise signals. We note that the proposed method curtails the requirement for spectrum sensing at the transmitter. By limiting the spurious interfering wireless communication signal impinging on the legitimate receivers while confusing the eavesdroppers, PLS performance was improved. Similarly, by reducing the RADAR interference, the wireless communication transmission rate was also improved.

In practice, an application of the proposed noise and interference cancellation filter aids autonomous vehicular RADAR impact on wireless communication infrastructure. Although it minimises the impact of the DFRC or JCR constraints, we focus on the cohabiting of JCR system without loss of generalisation. We emphasise that the overall objective entails the cancellation of interference at legitimate receivers based on previously acquired contextual information of the system's reaction to cohabitation. Such contextual information as applicable to RADAR tracking system using neural networks [113] were implemented. Specifically, the contextual information is obtained from an *a priori* knowledge of observations of the JCR system with pilot/test sample signals.

5.3 System Model of a Communication/RADAR Cohabiting Scenario

Consider a MIMO communication system with N_A transmit and N_B receive antennas operating on the RADAR spectrum. Let the wireless communication system cohabit with MIMO RADAR systems with N_C transmit and N_D receive antennas. For computational simplicity, we assume that the transmit and receive RADAR systems are located at the same place such that they share the same far-field observations. However the assumption does not necessarily apply to the communication system, thereby supporting their joint action. The $N_C \times 1$ and $N_A \times 1$ passband signals of the RADAR and communication transmit antennas are presented in (5.1a) and

(5.1b) respectively.

$$\mathbf{s}_k(t) = \mathbf{w}_k^* \psi_k(t), \forall k = \{1, \dots, K\} \quad (5.1a)$$

$$\mathbf{s}_{AB}(t) = \mathbf{w}_{AB}^* \varphi(t), \forall t = \{1, \dots, T\}. \quad (5.1b)$$

where \mathbf{w}_k represent the $N_C \times 1$ transmit beamforming vector of the k th orthogonal waveform ($\psi_k(t)$). \mathbf{w}_{AB} the $N_A \times 1$ is the transmit weight vector of the communication systems. K is the total number of orthogonal waveforms radiated by the RADAR system (for simplicity, $K = N_C$ implying that the RADAR transmission are orthogonal for each antenna element) and T is the total number of transmit snapshots. While $\varphi(t)$ is the baseband communication signal waveform.

If we assume frequency hopping communication transmission with quadrature phase shift keying (PSK) modulation, then $\varphi(t)$ is the same as presented in [109, eq. 9]. In the rest of this chapter, the subscripts A, B, C, D, E denotes an index of the communication transmitter, communication legitimate receiver (Bob), RADAR transmitter, RADAR receiver and communication illegitimate receiver (Eve) respectively. We note that in the context of JCR, the communication and RADAR transmit systems are usually co-located, sharing the same physical resources. However, spatial separation has been introduced in fig. 5.1 for clarity. In fig. 5.1, the notations of \mathbf{H}_{jn} ($\forall \{j \in \{A, C\} \text{ and } n \in \{B, D\}\}$) represents the forward channel response between j th transmitter and the n th receiver. The transmission from the wireless communication transmitters is the desired signal at the communication receiver and also an interfering signal at the RADAR receiver. The same description applies to the transmission from the RADAR transmitter.

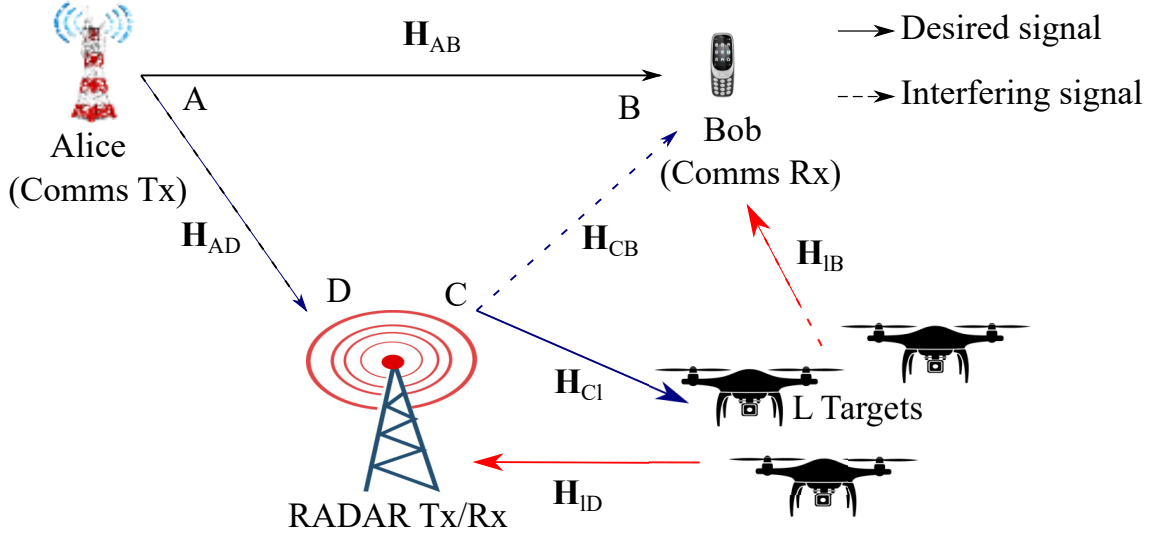


FIGURE 5.1: MIMO Communication and RADAR cohabitation system

To understand the operational requirements of the entire system model, we discuss 2 distinct role of the RADAR system in relation to the wireless communication system. The distinct roles are considered when RADAR target is absent and when it is present.

5.3.1 Case 1: No RADAR Target

In this section, we model the received signals of the wireless communications and RADAR receiver systems under JCR when there are no RADAR targets. We consider fig. 5.1 without the L RADAR targets. The received signal at the communication and the RADAR receivers were given as (5.2a) and (5.2b) respectively.

$$\mathbf{y}_i(t) = \underbrace{\mathbf{b}(\theta_{iA})\alpha_{Ai}\mathbf{a}^T(\theta_{AB})\mathbf{s}_{AB}(t)}_{\text{Comms. transmitted}} + \underbrace{\mathbf{b}(\theta_{iC})\alpha_{Ci}\mathbf{c}^T(\theta)\mathbf{s}_k(t)}_{\text{RADAR interference}} + \mathbf{n}_i, \quad \forall i \in \{B, E\} \quad (5.2a)$$

$$\mathbf{y}_D(t) = \underbrace{\mathbf{d}(\theta_{DA})\alpha_{AD}\mathbf{a}^T(\theta_{AB})\mathbf{s}_{AB}(t)}_{\text{Comms. interference}} + \mathbf{n}_D, \quad (5.2b)$$

where $\alpha_{jn} = \rho_0 \zeta \|\boldsymbol{\Omega}_j - \boldsymbol{\Omega}_n\|^{-2}$, $\forall \{j \in \{A, C\} \text{ and } n \in \{B, D\}\}$ are random channel coefficients characterising the propagation from path j to n . ρ_0 represents the

channel power gain at reference distance $d_0 = 1$ m and ζ is an exponential random variable with unit mean similar to [29, 56]. Parameters $\mathbf{a}(\theta_{AB})$ and $\mathbf{c}(\theta)$ are the transmit communication and RADAR steering vectors respectively. While $\mathbf{b}(\theta_{iA})$, $\mathbf{b}(\theta_{iC})$ and $\mathbf{d}(\theta_{DA})$ are the receive steering vectors. Note that the wireless communication receivers include the legitimate receiver (Bob) and the eavesdropper (Eve) as required. Assume that the antenna geometry on the wireless communication and RADAR systems follow a uniform linear array (ULA) configuration as postulated in [114], then the steering vectors can be generated with

$$\mathbf{x}(\theta_{jn}) = [1, e^{j\frac{2\pi}{\lambda}d_x \sin(\theta_{jn})}, \dots, e^{j\frac{2\pi}{\lambda}(N_i-1)d_x \sin(\theta_{jn})}]^T,$$

where d_x is the distance between antenna elements. Referring to (5.2), $\mathbf{n}_B \sim \mathcal{CN}(0, \sigma_B^2 \mathbf{1}_{N_B})$ and $\mathbf{n}_D \sim \mathcal{CN}(0, \sigma_D^2 \mathbf{1}_{N_C})$ are additive white Gaussian noise with variance σ_B^2 and σ_D^2 . The spatial direction of the RADAR system is focused towards a predefined sector such that $\theta = [\Theta_{\min}, \Theta_{\max}]$ where Θ_{\min} and Θ_{\max} represents the lower and upper contours of the sector. We note that θ_{jn} is the azimuth spatial direction of transmission from j to n or reception at j from n .

5.3.2 Case 2: RADAR Target Present

Consider fig. 5.1 where hypothetical L RADAR targets reflects RADAR signals. The received signal equations at the communication and RADAR receiver are given in (5.3) and (5.4) respectively.

$$\begin{aligned} \mathbf{y}_B(t) = & \mathbf{b}(\theta_{BA})\alpha_{AB}\mathbf{a}^T(\theta_{AB})\mathbf{s}_{AB}(t) + \mathbf{b}(\theta_{BC})\alpha_{CB}\mathbf{c}^T(\theta)\mathbf{s}_k(t) \\ & + \underbrace{\sum_{l=1}^L \mathbf{b}(\theta_{Bl})\alpha_{lB}\beta_l\alpha_{lr}\mathbf{c}^T(\theta)\mathbf{s}_k(t)}_{\text{target reflected(interference)}} + \mathbf{n}_B, \end{aligned} \quad (5.3)$$

$$\mathbf{y}_D(t) = \mathbf{d}(\theta_{DA})\alpha_{AD}\mathbf{a}^T(\theta_{AB})\mathbf{s}_{AB}(t) + \underbrace{\sum_{l=1}^L \mathbf{d}(\theta_{Dl})\alpha_{lD}\beta_l\alpha_{lr}\mathbf{c}^T(\theta)\mathbf{s}_k(t)}_{\text{target reflected(desired)}} + \mathbf{n}_D, \quad (5.4)$$

where β_l obeys Swerling II model and represents the reflection coefficient of the l th target. The Swerling II model imply that the reflectivity of the target may change for different pulse, but it will be constant within the duration of a single pulse duration.

In the cases described in sections 5.3.1 and 5.3.2, it is underlined that some form of cross-interference exists for the communication and RADAR systems especially when their channels are correlated. For the wireless communication signal containing relevant data, its interference on the RADAR receiver makes it susceptible to eavesdropping. By mitigating the interference, the loss of data in the physical layer domain is reduced.

5.4 Interference Mitigation

In this section, we examine the methods to mitigate the interference caused by the wireless communication transmission on the RADAR reception and vice versa. The interference mitigation approaches are discussed under two distinct generic scenarios, namely cooperative and uncooperative systems.

5.4.1 Cooperative Systems: RADAR receiver is the eavesdropper

The RADAR and wireless communication systems are said to be cooperative when the channel impulse responses between the transmitters and receivers are known by both systems. This entails that channel estimation had been carried out and updated in both systems. Using this contextual information of the *a priori* channel information, the interfering signals impact are reduced as a transmitter design

problem. We note that the wireless communication and RADAR systems are distributive and only share the contextualised information. It is easy to see that by independently optimising the transmit beamforming weights of both the wireless communication and RADAR transmissions, interference cancellation is obtained in the case discussed in section 5.3.1.

Consider equations (5.3) and (5.4) in section 5.3.2, the SINR of the wireless communication and the RADAR signals can be deduced as (5.5).

$$\gamma_B = \left(\frac{\text{Tr}(|\mathbf{H}_{AB}\mathbf{s}_{AB}(t)|^2)}{\sum_{l=1}^L \text{Tr}(|\mathbf{H}_{lB}\mathbf{s}_k(t)|^2) + \text{Tr}(|\mathbf{H}_{CB}\mathbf{s}_k(t)|^2) + \sigma_B^2} \right), \quad (5.5a)$$

$$\gamma_D = \left(\frac{\sum_{l=1}^L \text{Tr}(|\mathbf{H}_{lD}\mathbf{s}_k(t)|^2)}{\text{Tr}(|\mathbf{H}_{AD}\mathbf{s}_{AB}(t)|^2) + \sigma_D^2} \right), \quad (5.5b)$$

where $\mathbf{H}_{AB} = \mathbf{b}(\theta_{BA})\alpha_{AB}\mathbf{a}^T(\theta_{AB})$, $\mathbf{H}_{AD} = \mathbf{d}(\theta_{DA})\alpha_{AD}\mathbf{a}^T(\theta_{AB})$, $\mathbf{H}_{CB} = \mathbf{b}(\theta_{BC})\alpha_{CB}\mathbf{c}^T(\theta)$, $\mathbf{H}_{lB} = \mathbf{b}(\theta_{Bl})\alpha_{lB}\beta_l\alpha_{lr}\mathbf{c}^T(\theta)$, $\mathbf{H}_{lD} = \mathbf{d}(\theta_{Dl})\alpha_{lD}\beta_l\alpha_{lr}\mathbf{c}^T(\theta)$. We recall that when $L = 0$, the equations described in section 5.3.2 reduces to the equations given in section 5.3.1 where there are no RADAR targets.

Recall that $\text{Tr}(|\mathbf{H}_{AD}\mathbf{s}_{AB}(t)|^2)$ and $\sum_{l=1}^L \text{Tr}(|\mathbf{H}_{lB}\mathbf{s}_k(t)|^2) + \text{Tr}(|\mathbf{H}_{CB}\mathbf{s}_k(t)|^2)$ are the interfering parameters caused by the communication transmission on the RADAR receiver and the RADAR transmission on the communication receiver respectively. The objective herein is to mitigate the interfering parameters with the design of the beamforming weights $(\mathbf{w}_{AB}, \mathbf{w}_k)$ such that the impact of the interfering parameters are negligible. Hence, we formulate the rate optimisation problems in (5.6) and (5.7) constraining the interfering parameters to zero with strict equality. Since the wireless communication and RADAR transmissions are distributive, the determination of the transmit parameters are independent. Hence, (5.6) and (5.7) were independently

solved at the wireless communication and RADAR transmitters respectively.

$$\max_{\mathbf{w}_{AB}} \log_2 \left(1 + \frac{\text{Tr}(|\mathbf{H}_{AB}\mathbf{s}_{AB}(t)|^2)}{\sum_{l=1}^L \text{Tr}(|\mathbf{H}_{lB}\mathbf{s}_k(t)|^2) + \text{Tr}(|\mathbf{H}_{CB}\mathbf{s}_k(t)|^2) + \sigma_B^2} \right) \quad (5.6a)$$

$$\text{s.t. } \text{Tr}(|\mathbf{H}_{AD}\mathbf{s}_{AB}(t)|^2) = 0, \quad (5.6b)$$

$$\mathbf{w}_{AB}^H \mathbf{w}_{AB} = 1, \quad (5.6c)$$

$$\max_{\mathbf{w}_k} \log_2 \left(1 + \frac{\sum_{l=1}^L \text{Tr}(|\mathbf{H}_{lD}\mathbf{s}_k(t)|^2)}{\text{Tr}(|\mathbf{H}_{AD}\mathbf{s}_{AB}(t)|^2) + \sigma_D^2} \right) \quad (5.7a)$$

$$\text{s.t. } \sum_{l=1}^L \text{Tr}(|\mathbf{H}_{lB}\mathbf{s}_k(t)|^2) + \text{Tr}(|\mathbf{H}_{CB}\mathbf{s}_k(t)|^2) = 0, \quad (5.7b)$$

$$\mathbf{w}_k^H \mathbf{w}_k = 1. \quad (5.7c)$$

We note that $\mathbf{s}_k(t)$ and $\mathbf{s}_{AB}(t)$ are respective functions of \mathbf{w}_k and \mathbf{w}_{AB} , with expressions given in (5.1a) and (5.1b). Equations (5.6) and (5.7) are convex optimisation problems that can be easily solved using `cvx` [73]. We note that (5.6c) and (5.7c) describes the total normalised power transmitted by the wireless communication and RADAR transmitter respectively. These powers can be scaled to desired level in practice. For $L = 0$, no target reflects the RADAR signal and the solution is produced for case 5.3.1.

5.4.2 Cooperative Systems: Eavesdropper is an External Node

Consider that an eavesdropper lurks within the radio vicinity of the wireless communication signal, thereby receiving the legitimate wireless communication transmission and interference generated by the cohabiting transmission (RADAR). In this section, the characterisation of the PLS with wireless communication sensing was performed. The generic cohabitation figure presented in fig. 5.1 was expanded in

fig. 5.2 with the depiction of the passive eavesdropper location to allow for PLS analysis. We recall from section 5.3 that the notations, $\mathbf{H}_{jn}, \forall \{j \in \{A, C\} \text{ and } n \in \{B, D, E\}\}$, in fig. 5.2 represents the forward channel response between j th wireless communication and RADAR transmitter and their respective n th receiver. In fig. 5.2, the RADAR sends tracking signals which were reflected by the targets. The RADAR signal and the reflection interfere with the legitimate (Bob) and illegitimate (Eve) communication receivers. Eve was located within a closed region defined by the coverage of the communication transmitter (Alice). Furthermore, the communication transmitter transmits message intended for Bob but it was intercepted by Eve and interfered with the RADAR receiver. The interference of the wireless communication and RADAR transmissions were enabled since we assume that both systems operate on the same spectrum.

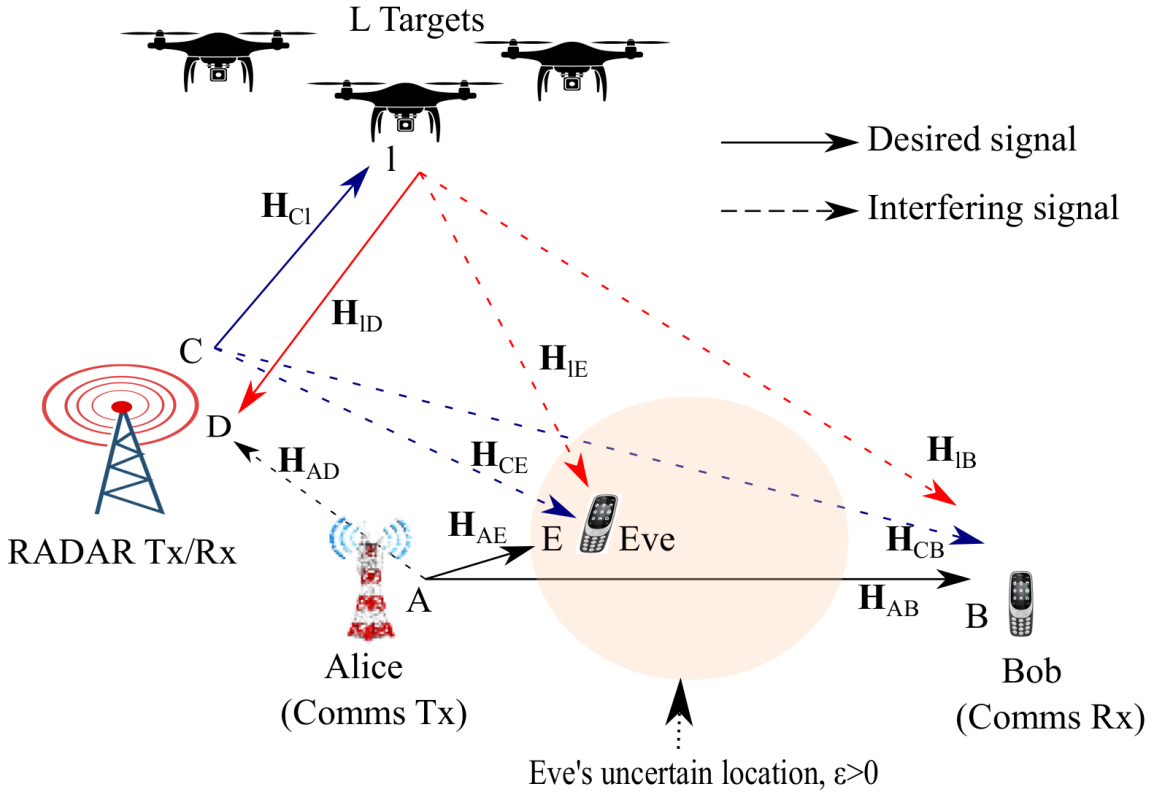


FIGURE 5.2: Signal architecture of the wireless communication and RADAR cohabitation systems with interaction from a passive eavesdropper

Since the eavesdropper is passive, its exact location or signal signature is unknown.

However, for simplicity, we assume that it is located within a circular region that spans the coverage area of the transmitters. Therefore, following the derivations in section 3.3, the exact location of Eve ($\mathbf{\Omega}_E$) was defined as a point on a circular uncertain region with the uncertainty measure defined in (5.8).

$$\mathbf{\Omega}_E = \hat{\mathbf{\Omega}}_E \pm \Delta\mathbf{\Omega}_E, \quad (5.8a)$$

$$\|\pm \Delta\mathbf{\Omega}_E\| = \|\mathbf{\Omega}_E - \hat{\mathbf{\Omega}}_E\| \leq \varepsilon, \text{ for } \varepsilon \geq 0, \quad (5.8b)$$

$$\|\Delta\mathbf{\Omega}_E\| \leq \varepsilon, \quad (5.8c)$$

holds true, where $\hat{\mathbf{\Omega}}_E$, $\Delta\mathbf{\Omega}_E$ and ε define the estimated location of Eve, the error of the estimation and the radius of error, respectively. Using triangular inequality and substituting (5.8), we have that

$$\|\mathbf{\Omega}_j - \mathbf{\Omega}_E\| = \|\mathbf{\Omega}_j - (\hat{\mathbf{\Omega}}_E \pm \Delta\mathbf{\Omega}_E)\| \leq \|\mathbf{\Omega}_j - \hat{\mathbf{\Omega}}_E\| + \varepsilon. \quad (5.9)$$

The right hand side is upper bound to Euclidean distance between the transmitters (communication, RADAR) and the centre of the circular uncertain region.

Following from the previous definition of the channel coefficient given in section 5.3.1, the channel coefficient was defined as $\alpha_{jE} = \rho_0 \zeta \|\mathbf{\Omega}_j - \mathbf{\Omega}_E\|^{-2}$, where $j \in \{A, C, I\}$ depending on the transmitter. By substituting the approximation of the upper bound of the location of Eve into the stochastic channel coefficient of Eve, we obtain an estimated value given as $\hat{\alpha}_{jE} = \rho_0 \zeta (\|\mathbf{\Omega}_j - \hat{\mathbf{\Omega}}_E\| + \varepsilon)^{-2}$. We note that the estimated location of Eve impacts the deterministic path of the channel coefficient.

Having defined the variations due to the introduction of the eavesdropper, we can consider the definition for the SINR of Bob and Eve as presented in (5.10a) and (5.10b) respectively.

$$\gamma_B = \frac{\text{Tr}(|\mathbf{H}_{AB}\mathbf{s}_{AB}(t)|^2)}{\sum_{l=1}^L \text{Tr}(|\mathbf{H}_{lB}\mathbf{s}_k(t)|^2) + \text{Tr}(|\mathbf{H}_{CB}\mathbf{s}_k(t)|^2) + \sigma_B^2}, \quad (5.10a)$$

$$\hat{\gamma}_E = \frac{\text{Tr}(|\hat{\mathbf{H}}_{AE}\mathbf{s}_{AB}(t)|^2)}{\sum_{l=1}^L \text{Tr}(|\hat{\mathbf{H}}_{lE}\mathbf{s}_k(t)|^2) + \text{Tr}(|\hat{\mathbf{H}}_{CE}\mathbf{s}_k(t)|^2) + \sigma_E^2}, \quad (5.10b)$$

where $\hat{\mathbf{H}}_{\text{AE}} = \mathbf{b}(\theta_{\text{EA}})\hat{\alpha}_{\text{AE}}\mathbf{a}^T(\theta_{\text{AB}})$, $\hat{\mathbf{H}}_{\text{IE}} = \mathbf{b}(\theta_{\text{EI}})\alpha_{\text{IE}}\beta_l\hat{\alpha}_{lr}\mathbf{c}^T(\theta)$, $\hat{\mathbf{H}}_{\text{CE}} = \mathbf{b}(\theta_{\text{EC}})\hat{\alpha}_{\text{CE}}\mathbf{c}^T(\theta)$. The other variables in the (5.10) are the same as previously defined under (5.5). With these SINR, the average secrecy rate which is the difference in the information rate of Bob and Eve can be written with (5.12a) [5, 29].

$$R_s = [\log_2(1 + \gamma_{\text{B}}) - \log_2(1 + \hat{\gamma}_{\text{E}})]^+, \quad (5.11)$$

where $[x]^+ = \max\{0, x\}$ ensures that the information rate received by Eve is not greater than that received by Bob in a variable rate scheme [5]. However, since the variable rate scheme is not the emphasis of this chapter, we focus on providing solutions that increases the interference of Eve's received signal while minimising that of Bob.

$$\max_{\mathbf{w}_{\text{AB}}, \mathbf{w}_k} R_s, \quad (5.12a)$$

$$\text{s.t. } \log_2 \left(1 + \frac{\sum_{l=1}^L \text{Tr}(|\mathbf{H}_{\text{ID}}\mathbf{s}_k(t)|^2)}{\sigma_{\text{D}}^2} \right) \geq r_{\text{th}}, \quad (5.12b)$$

$$\text{Tr}(|\mathbf{H}_{\text{AD}}\mathbf{s}_{\text{AB}}(t)|^2) = 0, \quad (5.12c)$$

$$\sum_{l=1}^L \text{Tr}(|\mathbf{H}_{\text{IB}}\mathbf{s}_k(t)|^2) + \text{Tr}(|\mathbf{H}_{\text{CB}}\mathbf{s}_k(t)|^2) = 0, \quad (5.12d)$$

$$\mathbf{w}_{\text{AB}}^H \mathbf{w}_{\text{AB}} = 1, \quad (5.12e)$$

$$\mathbf{w}_k^H \mathbf{w}_k = 1. \quad (5.12f)$$

The parameter, r_{th} , is the minimum RADAR rate required to reformulate the reflected signal from the RADAR targets. Equation (5.12b) provides the lower bound to the rate received by the RADAR receiver to reconstruct the reflected signal. Equation (5.12d) used the known CSI to cancel the interference at the legitimate receiver while (5.12c) removes the interference of the wireless communication signal at the RADAR receiver. By substituting for \mathbf{s}_{AB} and \mathbf{s}_{AB} with (5.1b) and (5.1a) respectively and expanding the objective function, (5.12) is rewritten as (5.13).

$$\begin{aligned} \max_{\mathbf{W}_{AB}, \mathbf{W}_k} \quad & \log_2 \left(1 + \frac{\text{Tr}(\mathbf{H}_{AB} \mathbf{W}_{AB} \mathbf{H}_{AB}^H)}{\sigma_B^2} \right) \\ & - \log_2 \left(1 + \frac{\text{Tr}(\hat{\mathbf{H}}_{AE} \mathbf{W}_{AB} \hat{\mathbf{H}}_{AE}^H)}{\sum_{l=1}^L \text{Tr}(\hat{\mathbf{H}}_{lE} \mathbf{W}_k \hat{\mathbf{H}}_{lE}^H) + \text{Tr}(\hat{\mathbf{H}}_{CE} \mathbf{W}_k \hat{\mathbf{H}}_{CE}^H) + \sigma_E^2} \right), \end{aligned} \quad (5.13a)$$

$$\text{s.t.} \quad \log_2 \left(1 + \frac{\sum_{l=1}^L \text{Tr}(\mathbf{H}_{lD} \mathbf{W}_k \mathbf{H}_{lD}^H)}{\sigma_D^2} \right) \geq r_{\text{th}}, \quad (5.13b)$$

$$\text{Tr}(\mathbf{H}_{AD} \mathbf{W}_{AB} \mathbf{H}_{AD}^H) = 0, \quad (5.13c)$$

$$\sum_{l=1}^L \text{Tr}(\mathbf{H}_{lB} \mathbf{W}_k \mathbf{H}_{lB}^H) + \text{Tr}(\mathbf{H}_{CB} \mathbf{W}_k \mathbf{H}_{CB}^H) = 0, \quad (5.13d)$$

$$\text{Tr}(\mathbf{W}_{AB}) = 1, \quad (5.13e)$$

$$\text{Tr}(\mathbf{W}_k) = 1 \quad (5.13f)$$

$$\text{rank}(\mathbf{W}_{AB}) = 1, \quad (5.13g)$$

$$\text{rank}(\mathbf{W}_k) = 1. \quad (5.13h)$$

Equations (5.13g) and (5.13h) were consequences of $\mathbf{W}_{AB} = \mathbf{w}_{AB} \mathbf{w}_{AB}^H$, and $\mathbf{W}_k = \mathbf{w}_k \mathbf{w}_k^H$ respectively. The SINR equation given in (5.10a), with the interference nulling performed in (5.13d), and the SINR of (5.10b) were expanded to

$$\gamma_B = \frac{\text{Tr}(\mathbf{H}_{AB} \mathbf{W}_{AB} \mathbf{H}_{AB}^H)}{\sigma_B^2}.$$

$$\hat{\gamma}_E = \frac{\text{Tr}(\hat{\mathbf{H}}_{AE} \mathbf{W}_{AB} \hat{\mathbf{H}}_{AE}^H)}{\sum_{l=1}^L \text{Tr}(\hat{\mathbf{H}}_{lE} \mathbf{W}_k \hat{\mathbf{H}}_{lE}^H) + \text{Tr}(\hat{\mathbf{H}}_{CE} \mathbf{W}_k \hat{\mathbf{H}}_{CE}^H) + \sigma_E^2}.$$

We note that (5.13) is non-convex due to the non-convexity of the objective function. However, it can be solved by applying successive convex approximation (SCA) algorithms. Recall that the SCA allows the problem to be broken into sub-optimal problems and an iterative algorithms developed to minimise the error of the objective function given in (5.13a) at each iteration step. The sub-problems and solutions arising from (5.13) were presented as (5.14) and (5.16) and the iterative algorithm was summarised in algorithm 5.

First, we present the sub-problem from (5.13) that solves for the beamforming weights parameter arising from the wireless communication transmission in (5.14).

$$\max_{\mathbf{W}_{AB}} \log_2 (1 + \bar{k}_1 \text{Tr}(\mathbf{H}_{AB} \mathbf{W}_{AB} \mathbf{H}_{AB}^H)) - \log_2 (1 + \bar{k}_2 \text{Tr}(\hat{\mathbf{H}}_{AE} \mathbf{W}_{AB} \hat{\mathbf{H}}_{AE}^H)), \quad (5.14a)$$

$$\text{s.t. } \text{Tr}(\mathbf{H}_{AD} \mathbf{W}_{AB} \mathbf{H}_{AD}^H) = 0, \quad (5.14b)$$

$$\text{Tr}(\mathbf{W}_{AB}) = 1, \quad (5.14c)$$

$$\text{rank}(\mathbf{W}_{AB}) = 1, \quad (5.14d)$$

where $\bar{k}_1 = \frac{1}{\sigma_B^2}$ and $\bar{k}_2 = \left(\sum_{l=1}^L \text{Tr}(\hat{\mathbf{H}}_{lE} \mathbf{W}_k \hat{\mathbf{H}}_{lE}^H) + \text{Tr}(\hat{\mathbf{H}}_{CE} \mathbf{W}_k \hat{\mathbf{H}}_{CE}^H) + \sigma_E^2 \right)^{-1}$. Equation (5.14) is a semi-definite programming (SDP) problem which was solved following conventional approach of neglecting the rank constraint in (5.14d). Hence, by applying logarithm law, and rewriting the trace matrix with [82, eq. 16], the objective of (5.14) was written as fractional objective. Thereby enabling the use of Charnes-Cooper's transformation of the problem to (5.15). Let $u = (1 + \text{Tr}(\hat{\mathbf{H}}_{AE}^H \hat{\mathbf{H}}_{AE} \mathbf{W}_{AB}))^{-1}$, and $\mathbf{U} = u \mathbf{W}_{AB}$, then (5.14) is equivalent to (5.15).

$$\max_{\mathbf{U}, u} (u + \text{Tr}(\bar{k}_1 \mathbf{H}_{AB}^H \mathbf{H}_{AB} \mathbf{U})), \quad (5.15a)$$

$$\text{s.t. } (u + \bar{k}_1 \text{Tr}(\bar{k}_2 \hat{\mathbf{H}}_{AE}^H \hat{\mathbf{H}}_{AE} \mathbf{U})) = 1, \quad (5.15b)$$

$$\text{Tr}(\bar{k}_2 \mathbf{H}_{AD}^H \mathbf{H}_{AD} u \mathbf{U}) = 0, \quad (5.15c)$$

$$\text{Tr}(u \mathbf{U}) = u, \quad (5.15d)$$

Equation (5.15) is convex and is easily solved with CVX [72]. We note that the rank constraint is dropped in (5.15) to allow for SDP solution. However, when the solution is obtained, the rank constraint was enforced using rank reduction technique like randomisation.

Furthermore, the sub-problem in terms of \mathbf{W}_k was presented in (5.16). This problem solves for the optimal weights of the RADAR transmitter to increase the average

secrecy capacity of the setup demonstrated in fig. 5.2.

$$\begin{aligned} \max_{\mathbf{W}_k} \quad & \log_2 \left(1 + \frac{\text{Tr}(\mathbf{H}_{AB} \mathbf{W}_{AB} \mathbf{H}_{AB}^H)}{\sigma_B^2} \right) \\ & - \log_2 \left(1 + \frac{\text{Tr}(\hat{\mathbf{H}}_{AE} \mathbf{W}_{AB} \hat{\mathbf{H}}_{AE}^H)}{\sum_{l=1}^L \text{Tr}(\hat{\mathbf{H}}_{lE} \mathbf{W}_k \hat{\mathbf{H}}_{lE}^H) + \text{Tr}(\hat{\mathbf{H}}_{CE} \mathbf{W}_k \hat{\mathbf{H}}_{CE}^H) + \sigma_E^2} \right), \end{aligned} \quad (5.16a)$$

$$\text{s.t.} \quad \log_2 \left(1 + \frac{\sum_{l=1}^L \text{Tr}(\mathbf{H}_{lD} \mathbf{W}_k \mathbf{H}_{lD}^H)}{\sigma_D^2} \right) \geq r_{\text{th}}, \quad (5.16b)$$

$$\sum_{l=1}^L \text{Tr}(\mathbf{H}_{lB} \mathbf{W}_k \mathbf{H}_{lB}^H) + \text{Tr}(\mathbf{H}_{CB} \mathbf{W}_k \mathbf{H}_{CB}^H) = 0, \quad (5.16c)$$

$$\text{Tr}(\mathbf{W}_k) = 1, \quad (5.16d)$$

$$\text{rank}(\mathbf{W}_k) = 1. \quad (5.16e)$$

If we ignore the constant terms in the objective function that do not influence the optimisation, with some mathematical manipulations, we obtain an SDP problem. The rank constraint was resolved using the technique described above. Hence, a convex equivalent of (5.16) was obtained and shown in (5.17). Equation (5.17) is convex and can be solved with CVX [72].

$$\max_{\mathbf{W}_k} \quad \log_2 \left(1 - \frac{\text{Tr}(\hat{\mathbf{H}}_{AE} \mathbf{W}_{AB} \hat{\mathbf{H}}_{AE}^H)}{z(\mathbf{W}_k)} \right), \quad (5.17a)$$

$$\text{s.t.} \quad \log_2 \left(1 + \frac{\sum_{l=1}^L \text{Tr}(\mathbf{H}_{lD} \mathbf{W}_k \mathbf{H}_{lD}^H)}{\sigma_D^2} \right) \geq r_{\text{th}}, \quad (5.17b)$$

$$\sum_{l=1}^L \text{Tr}(\mathbf{H}_{lB} \mathbf{W}_k \mathbf{H}_{lB}^H) + \text{Tr}(\mathbf{H}_{CB} \mathbf{W}_k \mathbf{H}_{CB}^H) = 0, \quad (5.17c)$$

$$\text{Tr}(\mathbf{W}_k) = 1. \quad (5.17d)$$

where $z(\mathbf{W}_k) = \sum_{l=1}^L \text{Tr}(\hat{\mathbf{H}}_{lE} \mathbf{W}_k \hat{\mathbf{H}}_{lE}^H) + \text{Tr}(\hat{\mathbf{H}}_{CE} \mathbf{W}_k \hat{\mathbf{H}}_{CE}^H) + \text{Tr}(\hat{\mathbf{H}}_{AE} \mathbf{W}_{AB} \hat{\mathbf{H}}_{AE}^H) + \sigma_E^2$. Equation (5.17) is convex and can be solved with CVX [72].

Algorithm 5 SCA Iterative algorithm for solving \mathbf{W}_{AB} , \mathbf{W}_{AB}^0 and \mathbf{W}_k

-
- 1: Initialise \mathbf{W}_{AB}^0 , \mathbf{W}_k^0 and R_s^0 such that the constraints in (5.13) were satisfied.
 - 2: $m \leftarrow 1$.
 - 3: **repeat**
 - 4: Compute and update \mathbf{W}_{AB}^m with (5.15).
 - 5: Using updated \mathbf{W}_{AB}^m , update \mathbf{W}_k^m with (5.17).
 - 6: Compute R_s^m as defined in (5.11).
 - 7: $\epsilon = \left| \frac{R_s^m - R_s^{m-1}}{R_s^m} \right|$.
 - 8: $m \leftarrow m + 1$.
 - 9: **until** $\epsilon \leq 10^{-5}$ OR $m \geq 200$.
 - 10: **Output:** $\mathbf{W}_{AB} = \mathbf{W}_{AB}^m$ and $\mathbf{W}_k = \mathbf{W}_k^m$.
-

In summary, the procedure to solve (5.13) follows algorithm 5. If the iterations terminates at the maximum number, then convergence was not obtained and the solution to the problem fails. However, it was shown in fig. 5.3 that the algorithm 5 always converge within a few number of iterations. The starting point of the iteration is a feasible but not close optimal as shown with the high error margin between the 0th and 1st iteration in fig. 5.3. Nevertheless, in subsequent iterations, the objective value begins to converge with low error between the successive objective values. The feasible starting point of the iteration can be obtained by setting the objective of (5.17) to zero and solve the feasibility problem.

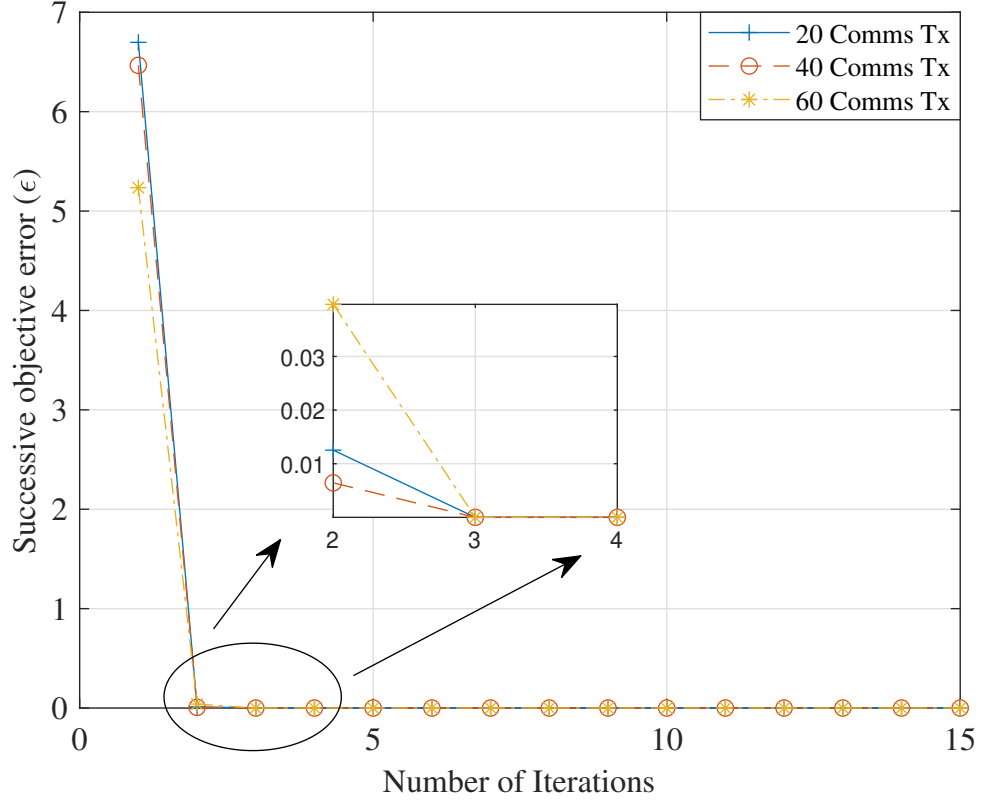


FIGURE 5.3: Convergence of the sensing algorithm 5.

5.4.3 Uncooperative Systems

When the RADAR and wireless communications systems are uncooperative, the channel impulse responses are unknown. Hence relying on beamforming weights as an interference mitigation approach is insufficient. This is because nulling the channels as carried out in (5.6b) and (5.7b) cannot be performed without knowledge of the channel impulse response. Therefore, to mitigate the cross interference of the RADAR and wireless communication systems, we implement a filter technology using autoencoder.

5.4.3.1 Autoencoder Formulation and Design

Autoencoder is a variation of an artificial neural network which use unsupervised learning approach to translate a corrupt or unrefined input data to a refined output data [115]. The output reconstructs the input data by excluding insignificant data variations. The autoencoder network typically has two sections referred to as the encoder and decoder sections. The encoder takes the corrupt data and converts it into an intermediary data which the decoder uses to estimate the refined data. Both sections contains several hidden layers used for feature extraction. Since the sections lie between the input and its output stages of the autoencoder, they are responsible for correlating the input data to produces a refined output through dimension reduction. It is desirable that the dimension of the feature space of the autoencoder is less than the dimension of the input data. This avoids the autoencoder configuring its hidden layers to an identity function, thereby, reproducing the input at its output [115]. To ensure that the requirement of the dimension of the autoencoder is less than the input data, sparse and denoise regularisation techniques are commonly used. While the sparse method switches off some hidden layers of the autoencoder, the denoising method maps the input data to a stochastic process. Several applications of autoencoders ranging from image processing [116, 117], feature extraction [117] and direction of arrival estimation under low SNR [118] has been explored in literature.

In this section, autoencoder was used for feature extraction to learn the variability of a multi-dimensional noisy data. The extraction was used to determine the noiseless version of the input data. The noisy data referred to in this work include the desired signals, cross interfering signals and AGWN.

The schematics of the autoencoder network deployed herein was presented in fig. 5.4. From fig. 5.4, the input and output data are represented as χ and χ' respectively, while ζ gives the data exchanged between the encoder and decoder. ϕ and Ψ are the encoder and decoder activation function respectively. The activation function refers to the drivers of a group of neurons classified as hidden layers of the autoencoder.

The encoder comprise of $1000 \times 800 \times 300 \times 100$ hidden layers where the numbers refer to the number of neurons. Similarly, the decoder comprise of $300 \times 800 \times 1000$ hidden layers. In artificial neural network, there are no standard methods to accurately predict the optimal number of neurons and hidden layers required for a set of non-linear problems [115]. However, in this chapter, the number of neurons and hidden layers used to construct the autoencoder were obtained by a brute pruning method. The pruning method allows for evaluation of the weights after training a small data set and eliminating neurons with little or no contribution to the learning process.

Each hidden layer of the encoder and decoder were activated with a rectified linear unit (ReLU) function. The neurons of the layers were also assigned a pair of weight and bias to characterise the feature impact ascribed to the neuron. The relation between the output of the autoencoder through the hidden layers of the encoder and decoder sections are given in (5.18) [115, 119].

$$\chi' = \Psi(\mathbf{W}'\phi(\mathbf{W}\chi + \mathbf{b}) + \mathbf{b}'). \quad (5.18)$$

We note that $\{\mathbf{W}, \mathbf{b}\}$ and $\{\mathbf{W}', \mathbf{b}'\}$ are the pair weights and biases for the encoder and decoder parts of the autoencoder respectively. The weights and biases were constantly updated during the training phase to construct the network for feature extraction of the test data.

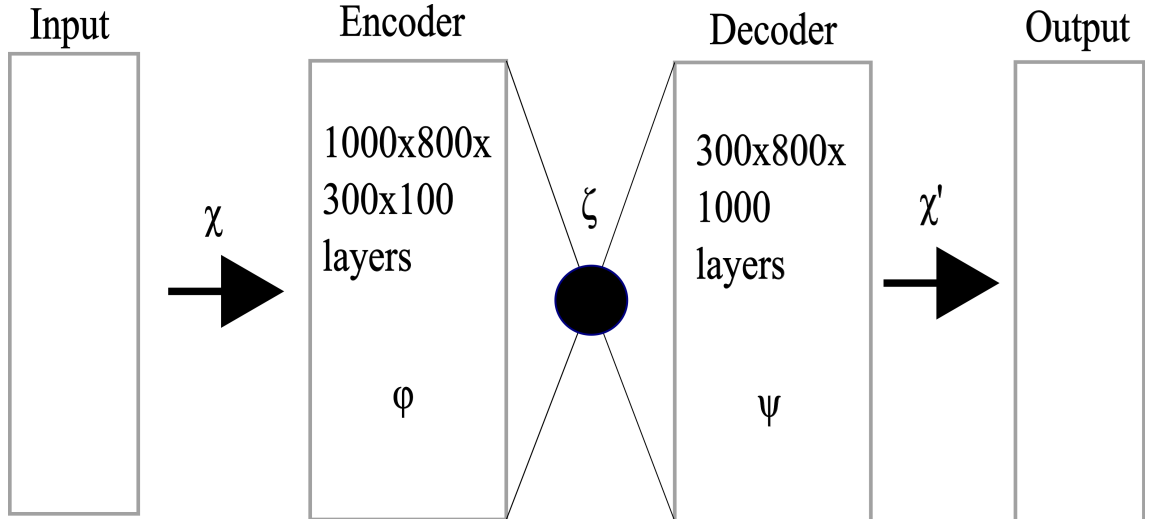


FIGURE 5.4: Layer interaction of the autoencoder

The deployment of the autoencoder follows two distinct phases - training and testing as depicted in fig. 5.5. The training phase allows the network to configure and validate its parameters (weights and biases) using known data. While the testing phases accepts unknown data and makes predictions based on the configurations obtained during training.

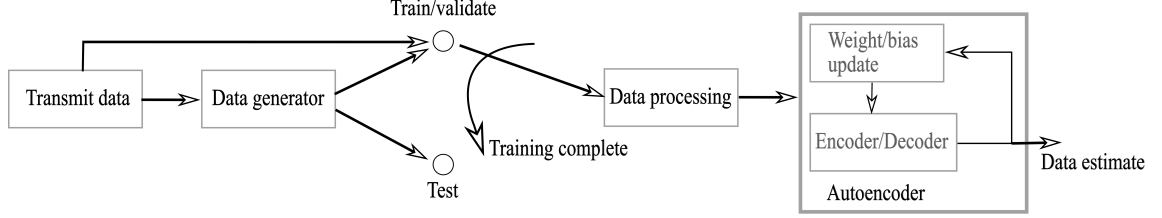


FIGURE 5.5: Data flow to the autoencoder

5.4.3.2 Autoencoder Input Preparation

In processing the input data to the autoencoder, we recall the received signals presented as (5.3) and (5.4) in section 5.3.2. Since the wireless communication and RADAR transmission systems are uncooperative, the receiver systems receive $\mathbf{y}_B(t)$ and $\mathbf{y}_D(t)$ which are corrupt versions of the desired transmitted signals, $\mathbf{s}_{AB}(t)$ and $\mathbf{s}_k(t)$ respectively. We note that in the uncooperative scenario, the design of the beamforming weights focus solely on maximum power transfer to the desired destination.

Although the data to the autoencoder during the training phase comprise of the transmitted signals, received signals by the wireless communication and RADAR receivers, without loss of generality, the data processing was focused on the received signals. The received signal comprise of real and imaginary parts such that $\mathbf{y}_i(t) = \text{real}(\mathbf{y}_i(t)) + \text{imag}(\mathbf{y}_i(t)) \forall i \in \{B, D\}$ and $t \in \{1, \dots, T\}$. Consider that for each snapshot (T), the signal data representation of the communication and RADAR receiver, we obtain $\mathbf{Y}_i = [\mathbf{y}_i(1), \dots, \mathbf{y}_i(T)]^T \sim \mathcal{C}^{N_i \times T}$. The data processing unit designs an extractor function, f_{ex} , that converts \mathbf{Y}_i into a vector, extract and stack the real and imaginary values of the data. The processed data, $\chi = f_{\text{ex}}(\mathbf{Y}_i)$ given

in (5.19) is suited as an input to the autoencoder.

$$\chi = [\text{real}(\text{vec}(\mathbf{Y}_i)), \text{imag}(\text{vec}(\mathbf{Y}_i))]^T. \quad (5.19)$$

5.4.3.3 Autoencoder Training and Validation Phase

Consider that known pilot signals were transmitted within the wireless communication and RADAR cohabitation systems. The known pilot transmission and the received signals of the communication and RADAR receivers were collected as training and validation data set of the autoencoder. These data set were processed following the description presented in section 5.4.3.2. The training and validation process allows the autoencoder to extract the features of the channel response and noise impact on the known pilot transmission. The extracted features were reflected on the network parameters of weights and biases and were used to predict unknown transmissions. During the training, the primary objective of the network is to minimise the reconstruction loss given in [115] as

$$\mathcal{L}(\chi, \chi') = \|\chi - \chi'\|^2,$$

In the training phase of the autoencoder, each snapshot of data comprise of 20,000 variations of a wireless communication pilot signal and the RADAR target reflections. The layers of the autoencoders are activated using ReLU functions.

To ensure that the feature adjustment during the training phase corresponds to the requirement of the data, a validation is periodically performed. While the training is ongoing, the autoencoder pauses to test the network using reserved training data. In the model described herein, 10% of the training data was reserved for validation.

5.4.3.4 Autoencoder Testing Phase

The data used in the testing phase of the autoencoder was the received signal from the communication and RADAR receivers. At the end of the training phase, the

JCR signals were processed with the trained autoencoder networks at the communication and RADAR receivers. The output from the autoencoder estimated the wireless communication and RADAR reflections devoid of interference due to their cohabitation. Since the autoencoder network is domicile at the receivers, increasing number of wireless communication users or RADAR target does not affect its functionality.

5.5 Results and Discussions

The performance evaluation of the scenarios and techniques discussed herein were obtained via numerical simulations. The generic values of the simulation parameters were presented in table 5.1. However, where it explicitly stated in the figure and discussions, some values from the table may change.

TABLE 5.1: Parameter description of the JCR model

Simulation parameter	Symbol	Value
Number of wireless communication transmit antennas	N_A	30
Number of wireless communication receive antennas	N_B	4
Number of RADAR transmit antennas	N_C	30
Number of RADAR receive antennas	N_D	4
Carrier frequency (Surveillance)	f_c	2GHz
Distance between antenna elements	d_x	$\frac{\lambda}{2}$
Number of reflecting targets	L	3
Noise power	σ_B^2 and σ_D^2	30dBm
Radius of uncertainty region	ε	300m

The legends in figs. 5.6 and 5.7 describes the scenario under consideration. When the legend reads:

- 1 RADAR is Eve: refers that the RADAR receiver receives the wireless communication signals illegitimately.
- 2 Eve is external: refers that an illegitimate user listens to the wireless communication transmission. The user acts independent of the wireless communication and RADAR transmission systems. Refer to fig. 5.2 in section 5.4.2.
- 3 Upper Bound: refers to the maximum wireless communication transmission rate as measured at the communication receiver.

We begin the discussions with the design presented in section 5.4.1 where the communication/RADAR cohabiting parameters influenced the beamforming designs. The scenario ignores the presence of an external eavesdropper in its formulations.

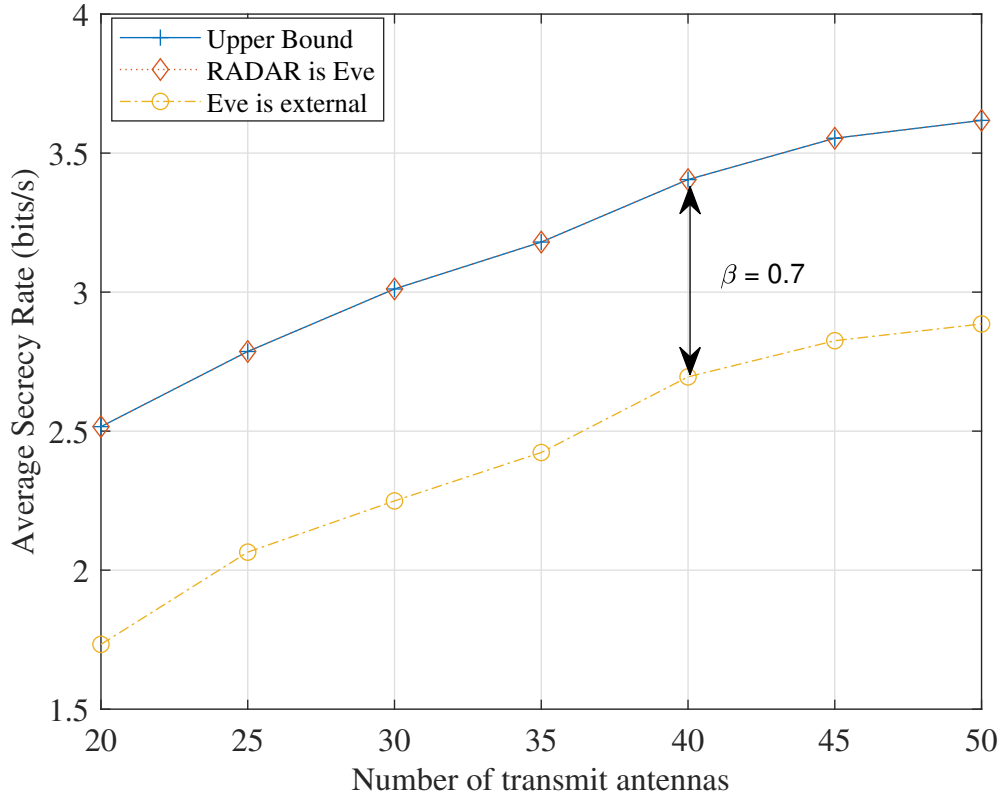


FIGURE 5.6: Average secrecy rate analysis where the only the communication and RADAR cohabiting parameters influence the beamformer.

In fig. 5.6, the cooperative system analysis in terms of average secrecy performance developed in section 5.4.1 was presented. The average secrecy rate of ‘RADAR is

Eve' showed in fig. 5.6 to be approximately the same with the rate of the legitimate communication receiver. From equations (5.6b) and (5.7b), the cross interference from both communication and RADAR systems were effectively suppressed with the choice of the beamforming weights. We recall from section 5.4.1, that for a cooperative system, the channel information of the RADAR and wireless communication systems were shared, and thereby effectively used in designing the beamforming weights. The performance observed for 'RADAR is Eve' allude to the effectiveness of the beamforming designs in nulling the interfering signals. Note that the rate of the legitimate communication receiver defines the upper bound to the average secrecy rate.

In addition, it was also observed in fig. 5.6, that when the eavesdropper is not the RADAR receiver ('Eve is external'), the average secrecy rate becomes smaller. This is because the beamforming designs does not null the external eavesdropper channel in the formulations of section 5.4.1. However, the external eavesdropper was marred by the interfering signal from the cohabiting system causing positive average secrecy rate. The observation is relevant since it provides an additional justification that cohabiting systems supports PLS when the interfering signal is properly managed at the legitimate receiver.

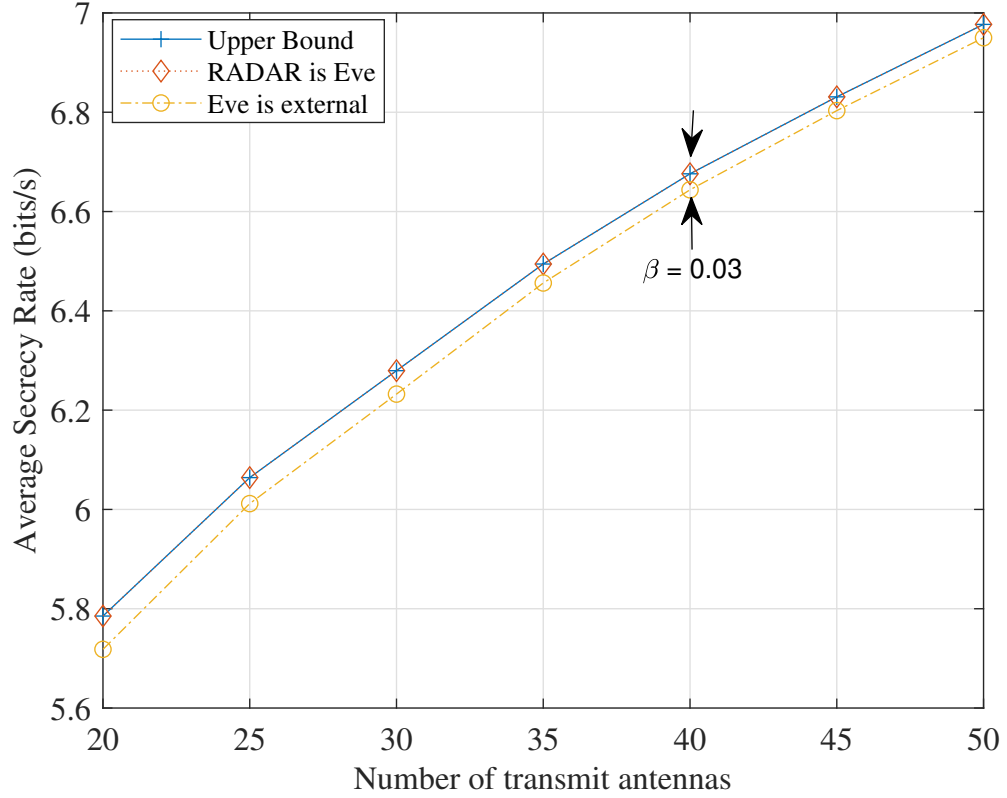


FIGURE 5.7: Average secrecy rate analysis where an external eavesdropper and the communication and RADAR cohabiting parameters influence the beamformer.

Furthermore we consider the PLS analysis of a cooperative wireless communication and RADAR cohabiting system where an external eavesdropper was considered in the design of the beamforming weights. The discussions centre on the problem formulation of the scenario given in section 5.4.2. The performance assessment was shown in fig. 5.7. It is clear from fig. 5.7 that although high average secrecy rates were observed when the eavesdropper is not the RADAR receiver, the rates are below the upper bound¹. The reduction in the average secrecy rate performance for this scenario is attributed to the estimation made of the eavesdropper's location. However, the average secrecy rate observed for 'Eve is external' in fig. 5.7 performed better when compared to the observations shown on fig. 5.6. This observation was made because contrary to the beamforming designs used to generate fig. 5.6, the external eavesdropper was considered in the beamforming design. This comparison

¹We note that the upper bound was defined herein, as the maximum rate observed at the communication receiver.

was made by checking the level of separation (β) between the external eavesdropper performance in both figures.

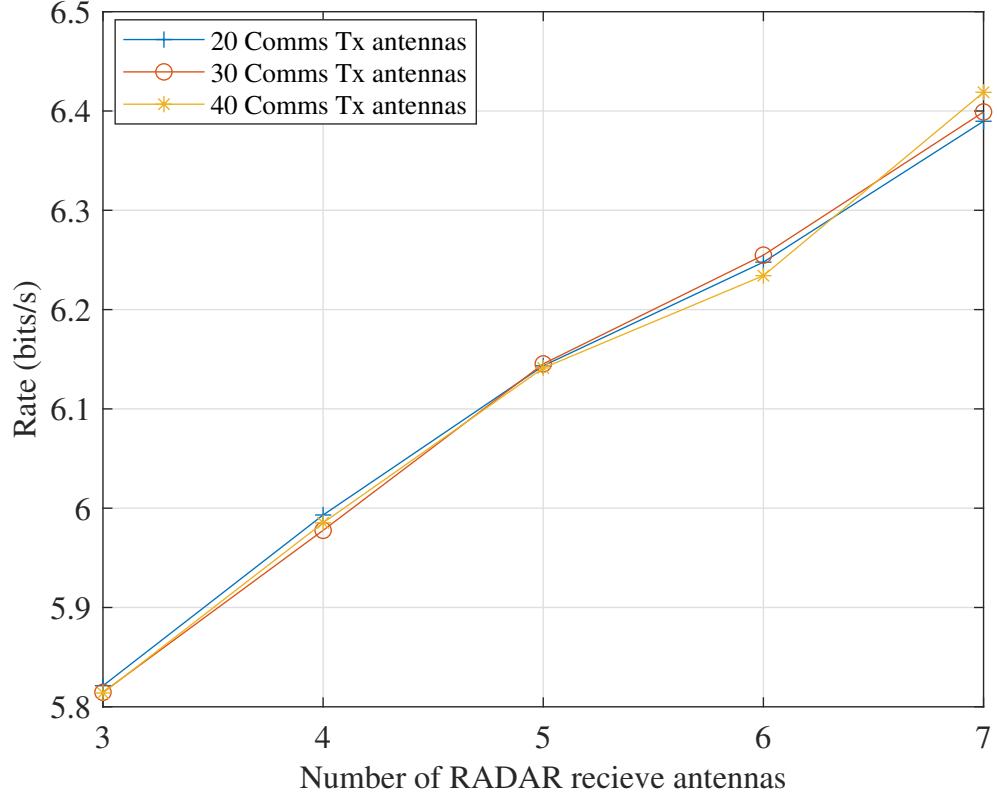


FIGURE 5.8: Impact of the beamforming design on the RADAR receiver for $N_C = 30$.

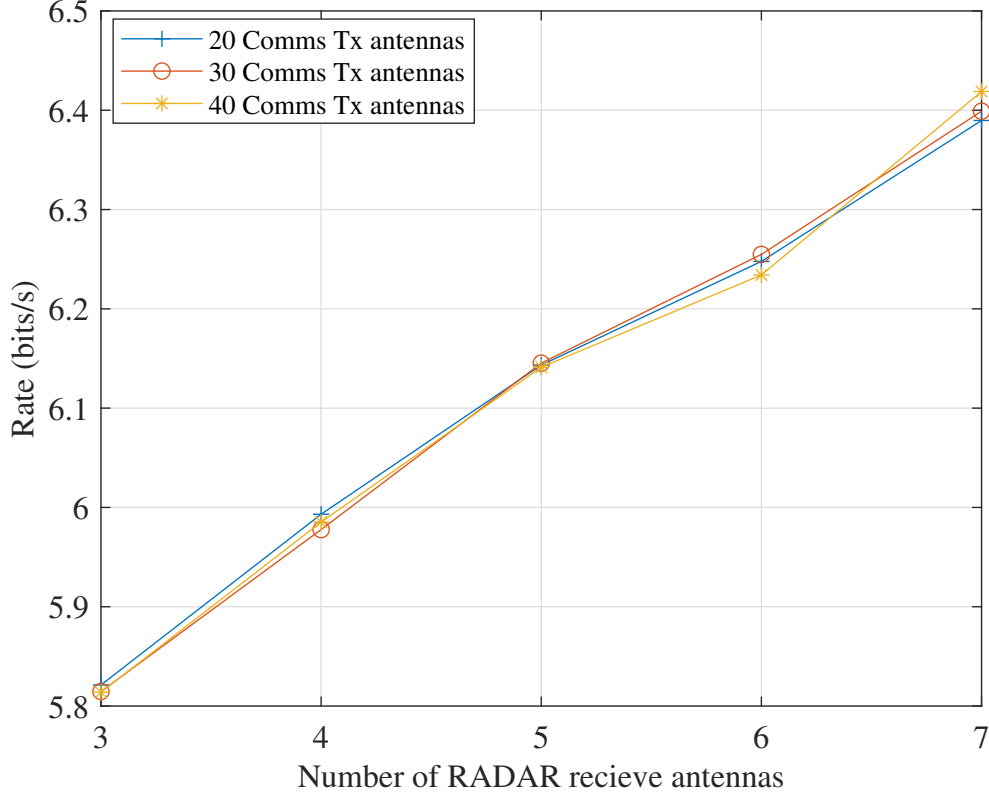


FIGURE 5.9: Impact of the beamforming design on the RADAR transmitter for $N_D = 4$.

In addition, we consider the effect of designs of the transmit wireless communication and RADAR beamforming designs in figs. 5.8 and 5.9. It is clear from both figures that only the RADAR antenna parameters affects the reception rates. By increasing the number of antennas at the RADAR transmitter and receiver, the rates of the reflected signals increases. However, changing the number of wireless communication transmitter, do not cause significant change in the reflected RADAR rates as observed from both figs. 5.8 and 5.9. Although the wireless communication transmission continues to interfere with the RADAR reflected signals, the designs of the beamforming weights of the wireless communication ensures that the impact of the interference is minimal.

Furthermore, we recall that the objective of the discussions on figs. 5.7 and 5.6 was to infer that minimising the cross interference of a cohabiting systems leads to increase PLS. The interference had been minimised under cooperative assumption of

the wireless communication and RADAR systems. In practice the wireless communication and RADAR systems are not cooperative, hence the need for a method to minimise the impact of the interfering signal at the legitimate receiver. The method proposed and discussed in section 5.4.3 of the chapter was the use of autoencoders for filtering the interfering signals at the desired receivers. The analysis of the autoencoder performance in estimating the transmitted signal were presented in figs. 5.10 and 5.11. The legend ‘ x snapshots’ (where $x \in \{10, 20, 30\}$) used in both figures describes the number of snapshots used in training the autoencoder network. We note that each snapshot comprises of 20000 training samples. The legends ‘CRB Null Space Projection’ and ‘CRB (Original)’ present comparison with null space projection algorithm given in [108] and the Cramer Rao lower bound (CRB) derived in [114, eq. 44] respectively.

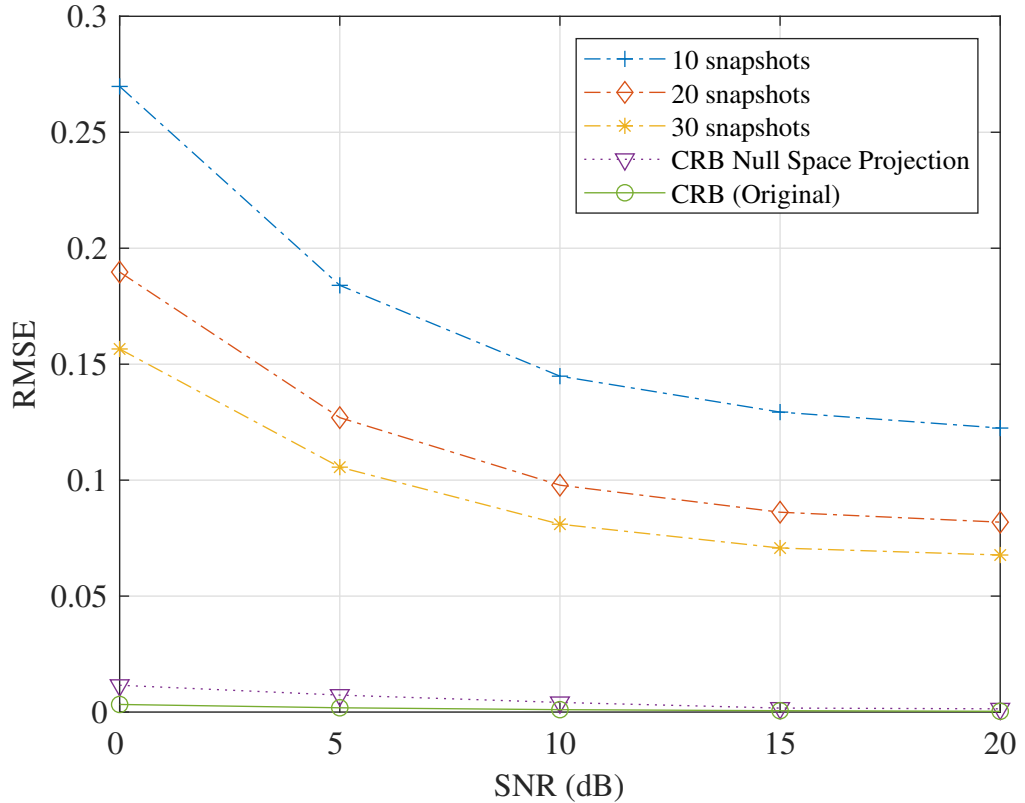


FIGURE 5.10: RMSE performance graph of test Communication signals.

Figure 5.10 illustrates the performance of the estimated received wireless communication signal compared to the original transmitted signal in terms of root mean

square error (RMSE). It was observed that higher SNR presents lower decoding error corresponding to low RMSE value. By increasing the number of snapshots taken to train the neural network, better performance was also observed in the figure. Although better performance of the autoencoder was observed with increased snapshots as shown in fig. 5.10, large training snapshots are required to minimise the RMSE. In practice, it places a constraint on the physical device used for training purposes.

Furthermore, comparing the autoencoder estimation with the algorithms from the null space projection [108] and the CRB [114, eq. 44], fig. 5.10 showed that the autoencoder's performance is low. This poor performance is further worsened when the training samples are few. However, we note that the exact channel response from and CRB were assumed to be known in [108] and [114, eq. 44] respectively; hence the lower RMSE. This assumption is contrary to the autoencoder design where the only available data during the testing phase is the corrupt received signals. Therefore, the trade-off of the availability of training data and the uncooperative constraint on that the autoencoder solution presents a window to manage the cohabiting interference.

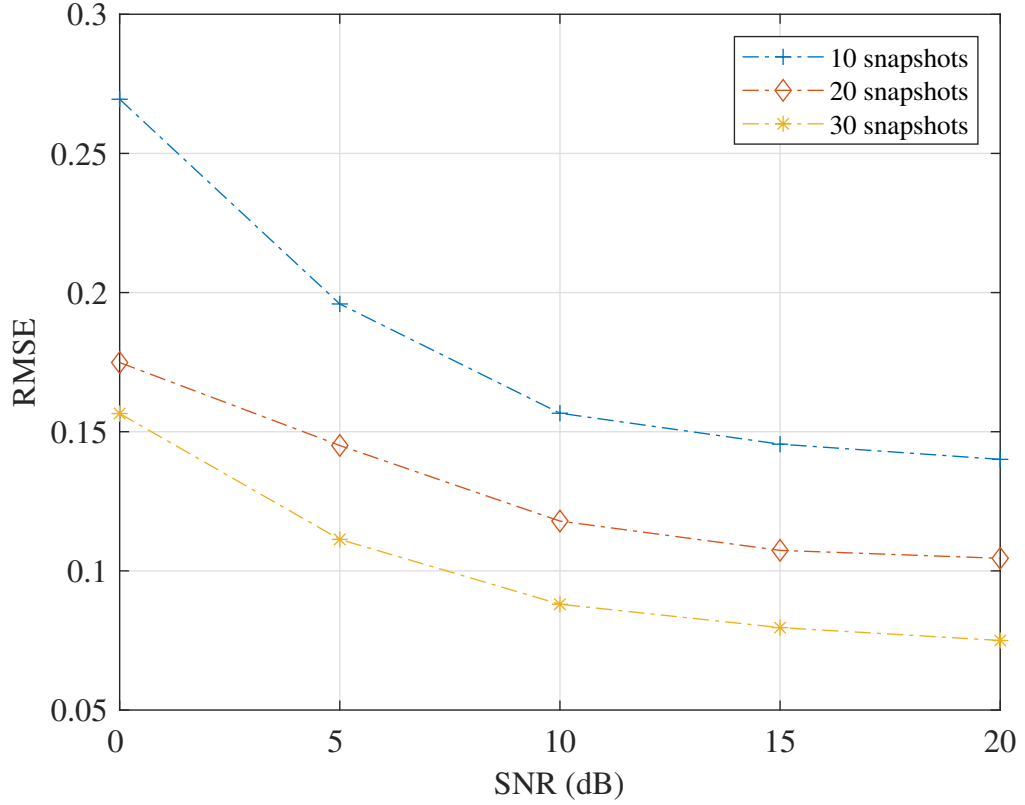


FIGURE 5.11: RMSE performance graph of test RADAR reflected signals.

Furthermore, the ability of the autoencoder to estimate desired target reflections at the RADAR receiver was presented in fig. 5.11. Similar to the observations shown in fig. 5.10, higher SNR leads to lower RMSE values. Additionally, better performance, in terms of low RMSE values were observed when the number of training snapshots were increased.

5.6 Chapter Summary

In this chapter, we examined wireless communication sensing as a panacea to transmit-based spectrum sharing and cohabiting while guaranteeing PLS. JCR system acted as a typical representation of application collaboration due to cohabitation for the assessment conducted in the chapter. Specifically, the impact of minimising the cross interference at the legitimate receiver was emphasised. The chapter explored

the design of beamforming weights to null the interfering signals at desired receivers for cooperative cohabiting systems. To further improve on the PLS of such systems, the weights were designed with the knowledge of a passive eavesdropper. We showed that canceling the interfering signals by method of beamforming design, improves on the PLS. The interference cancellation deduction made from the cooperative scenarios, enabled a postulation to filter interfering signals when the cohabiting systems were uncooperative. Hence, we further investigated an autoencoder network based approach of filtering interfering and noise signals at the legitimate receiver. The proposal made in this chapter promoted better PLS at the legitimate receiver in the presence of a passive eavesdropper. It was observed that with enhanced design configuration at the receiver and transmitter of cohabiting systems, PLS guarantees can be ensured.

Chapter 6

Conclusion and Recommendation

As more devices use wireless communication to move towards a technological singularity, securing the physical layer is necessary. In future network applications, attempts to explore the physical layer vulnerabilities will increase due to its broadcast nature. In this thesis, we have developed algorithms to secure the physical layer using UAV, IRS and sensing technologies. Section 6.1 presents a summary of the entire thesis while section 6.2 gives a path for future research exploration.

6.1 Summary

The emphasis of thesis work is securing the physical layer communication from passive eavesdroppers. In chapter 2, we investigated the use of jamming signals delivered from a UAV to improve keyless PLS where a passive eavesdropper listens to communication between two points. We encase the location of the passive eavesdropper within an ellipse measuring over the coverage of the transmitter. An average secrecy rate formulation of passive eavesdropping was developed in chapter 2. The parameters highlighted from the formulation that were investigated to increasing the PLS of the communication include the trajectory of the UAV, the jamming power delivered from the UAV and the transmission power of the communication. An algorithm to compute these parameters was presented. The simulation results

obtained by testing the algorithm compared the performance of the optimal UAV trajectory design with the fixed trajectory and fixed jamming node. The numerical analysis shows that even with the passive eavesdropping, positive average secrecy rate comparable to a scenario when the active eavesdropping can be obtained using the jamming algorithm developed in chapter 2. Although the average secrecy rate of the passive eavesdropper depends on its proximity to the transmitter. By examining the received envelop power of the passive eavesdropper, we also showed that positive secrecy rate is maintained, albeit with low values as the envelop power increase.

Furthermore, having observed the PLS benefits of using a single UAV to deliver jamming signals in chapter 2, we considered using multiple UAVs for the same purpose. Therefore, in chapter 3, we considered the grid formation of several UAVs forming a swarm to maximise the secrecy rate while considering passive eavesdropping scenario. Null projection of the swarm beamforming weights on the estimated passive eavesdropper channel were conducted to degrade the quality of signals it received. The beamforming weights, forming a single ray beam, were computed using SCA optimisation method. Based on the design of the null beamforming, an iterative algorithm was obtained to also evaluate the trajectory of the UAV swarm. Chapter 3 also discussed the results obtained by testing the algorithm via simulations. Some key observations from the numerical analysis showed the effect of increase the geometric uncertain location of the passive eavesdropper, and comparison to the active eavesdropper and single UAV jamming model presented in chapter 2. It is also notable that the physical limitation of the distance between the UAVs within half wavelength ($\frac{\lambda}{2}$) reduced the number of UAVs necessary to improve the PLS.

To reduce the physical challenges of deploying multiple UAVs to form the swarm, we used the IRS to relay the communication between the transmitter and receiver. Due to the inherent properties of the IRS, the passive eavesdropper ability to listen to the communication was limited. Rather than jam the signal received by the passive eavesdropper, we focus on using the IRS mounted on a UAV to optimally reflect the communication signal to the desired receiver. Therefore, in addition to the design of the trajectory of the UAV carrying the IRS and the transmission power,

we also examined the a low complex design of the reflection coefficients of the IRS. Algorithms to jointly obtain the aforementioned parameters necessary for improving the PLS of the communication were generated and tested. The numerical results showed the performance in terms of correlation between the passive eavesdropper and the legitimate receiver. We also investigated the impact of increasing the uncertain region of the eavesdropper and the relationship between the PLS and transmission power.

In chapter 5, we performed wireless communication sensing at the legitimate receiver. We separated the wireless communication from its cohabiting RADAR signals using machine learning approach - autoencoder. This method guaranteed their cohabitation and acts as a panacea to transmit-based spectrum sensing. Considering that the channel impulse response were known by the receivers (communication and RADAR), we showed that optimising beamforming weights mitigates the interference caused by signals and improve the PLS of the system. Furthermore, when the channel response were unknown, we designed an interference filter as a low complex noise and interference cancellation autoencoder. Results showed that even for low SNR, the autoencoder produces low RMSE values.

In conclusion, this thesis journeyed through current and future technologies to enhance PLS. These technologies refer to the use of jamming while the other robust applications explored IRS and communication sensing. We note that technologies like the IRS and wireless communication sensing inherently imbibe PLS by their functionalities.

6.2 Recommendation

In this thesis, we have shown several methods to enhance PLS where an eavesdropper is passive. However, we highlight in this section some areas for further works in the future.

The solution to the methods derived in this thesis are mainly iterative due to the non-convex nature of the problems. However the solutions to the iterative process are sub-optimal and complex. A future approach is to explore closed-form expressions and adapting the solutions with machine learning to non-convex problems.

Furthermore, research into quantum communication is on-going and will likely become the stable future of wireless communication. Considering the prospects and specifications of quantum communication, its robustness to PLS for passive eavesdropping is an interesting area to investigate. This investigation integrated with the use of artificial intelligence (AI) to perform wireless communication will likely produce a near perfect secured physical layer communication.

Finally, the algorithms generated in this thesis were tested with simulations. In future, they can be validated with experimental results. This experimental testing can lead to certain adjustments that will support the deployment of the algorithms.

Appendix A

Proof of the Sum Composition from Section 2.3.1

In this section, we show that the non-convexity of (2.10) from section 2.3.1 is the sum of a concave and a convex functions in terms of P_a . From (2.10), we obtain

$$R_s = \sum_{n=1}^N \underbrace{\log(1 + h_b[n]P_a[n])}_{f_1(P_a)} - \underbrace{\int_0^{h_b[n]} \frac{P_a[n]e^{-\frac{h_e[n]}{y_e}}}{1 + h_e[n]P_a[n]} dh_e}_{f_2(P_a)}. \quad (\text{A.1})$$

We consider (A.1) in two parts, showing their convexity with the second derivative method. In general, the convexity of a function is defined as [67]

$$f''(x) = \begin{cases} \textit{Convex} & :> 0 \\ \textit{Concave} & :< 0 \\ \textit{Affine} & := 0. \end{cases}$$

Thus we have from (A.1) that

$$f_1''(P_a) = - \left(\frac{h_b}{1 + h_b P_a} \right)^2.$$

We then show the convexity of the $f_2(P_a)$ using the principle that the nonnegative weighted-sum of a convex (concave) function is a convex (concave) [67, Section 3.2.1]. The second part can be rewritten as

$$\int_0^{h_b[n]} e^{-\frac{h_e[n]}{y_e}} \frac{P_a[n]}{1 + h_e[n]P_a[n]} dh_e \equiv \int_0^{h_b[n]} w(h_e) f(P_a, h_e) dh_e.$$

It has been shown in [67] that if $f(P_a, h_e)$ is convex (concave), then $f_2(P_a)$ is convex (concave). Thus, we have that the second derivative of $f_2(P_a)$ as

$$f_2''(P_a) = -\frac{2h_e}{(1 + h_e P_a)}.$$

Thus both parts of (A.1) are concave functions independently under the constraint of $h_b \geq 0$ and $P_a \geq 0$. These are the positive semi-definite constraints that guarantees communication between the source and the destination. If $h_b < 0$ and $P_a < 0$ then no information could be transmitted successfully. Therefore, we have that (A.1) is the sum of a concave and a convex function ($-f(x)$ = convex if $f(x)$ = concave) in terms of P_a .

Appendix B

UAV-IRS Signal to Interference Noise (SINR) Distribution

Consider that the received SINR at an arbitrary i th location ($\forall i \in \{B, E\}$) is given as

$$\gamma_i = \frac{|\mathbf{h}_i^T \mathbf{\Theta} \mathbf{G} \mathbf{w}|^2}{S_{n+int}}, \quad (\text{B.1})$$

where \mathbf{h}_i is the impulse response between the IRS and the i th location, $\mathbf{\Theta}$ and \mathbf{G} are the reflection coefficient matrix and the channel matrix between the transmitter and the IRS respectively. S_{n+int} represents the noise and interference power.

Proposition: Given that S_{n+int} is Rician distributed, the PDF of γ_i is given as (B.2).

$$p_\gamma(\gamma_i) = \sum_{k=0}^{\infty} A_k \frac{\gamma_i^{k-\frac{1}{2}}}{(\gamma_i + 1)^{2k+2}} {}_2F_1\left(-k, \frac{1}{2} - k; 1; \frac{v^2 \sigma^2}{\mu^2 \sigma_1^2 \gamma_i}\right), \quad \forall \gamma_i > 0, \quad (\text{B.2})$$

where $A_k = \frac{\sqrt{8e}^{-\left(\frac{\mu^2}{2\sigma^2} + \frac{v^2}{2\sigma_1^2}\right)} \Gamma(k+2)}{k! \sigma_1 \sigma^2 \Gamma(k+\frac{1}{2})} \left(\frac{\mu^2}{\sigma^2}\right)^k$. $\Gamma(\cdot)$ and ${}_2F_1(\cdot)$ represents the gamma and Gauss hypergeometric functions respectively. For $\gamma_i \leq 0$, $f(\gamma_i) = 0$ since the $p_A(a)$ and $p_B(b)$ are equal to 0 for negative values. Since γ_i represents the SINR at specific

i – th node, it is lower bound by zero and physical environmental factors restricts its upper bound.

Proof: Due to the random channel variations, let $b = |\mathbf{h}_i^T \mathbf{\Theta} \mathbf{G} \mathbf{w}|^2$ and $a = S_{n+int}$ representing randomly generated variable such that $\gamma_i = \frac{b}{a}$. We consider $S_{n+int} \in \mathcal{R}_+$ is a Rician distributed random variable with PDF given as (B.3)

$$p_A(a) = \frac{a}{\sigma_1^2} e^{-\left(\frac{a^2+v^2}{2\sigma_1^2}\right)} I_0\left(\frac{av}{\sigma_1^2}\right), \forall a > 0. \quad (\text{B.3})$$

We note that the PDF of a rician distribution can be written as a scaled non-central chi-squared distribution such that $p_A(a) = \frac{2a}{\sigma_1^2} f\left(x_a = \frac{a^2}{\sigma_1^2} \mid k=2, \lambda = \frac{v^2}{\sigma_1^2}\right)$. The PDF of the non-central chi-squared distribution is presented in (B.4)

$$f(x \mid k, \lambda) = \frac{1}{2} e^{-\left(\frac{x+\lambda}{2}\right)} \left(\frac{x}{\lambda}\right)^{\frac{k}{4}-\frac{1}{2}} I_{\frac{k}{2}-1}(\sqrt{\lambda x}) \quad (\text{B.4})$$

Furthermore, following algebraic matrix manipulations and similar expression with [120, eq.1], we can write (B.5).

$$\mathbf{h}_i^T \mathbf{\Theta} \mathbf{G} \mathbf{w} = \sum_{k=1}^K h_k \theta_k \sum_{m=1}^M G_{km} w_m. \quad (\text{B.5})$$

Let $X_k = h_k \theta_k$ and $Y_k = \sum_{m=1}^M G_{km} w_m$ be independent and uncorrelated random variables. By central limit theory (CTL), the PDF of $\sum_{k=1}^K X_k Y_k$ is Gaussian distributed with expected value and variance of $\mu = K \mathbb{E}[X_k] \mathbb{E}[Y_k]$ and $\sigma^2 = K \mathbb{E}[X_k^2 Y_k^2] - \mathbb{E}[X_k Y_k]^2$ respectively [121]. By definition, taking the magnitude of a Gaussian random variable gives a folded normal distribution with parameters μ and σ . Invariably the squared of the folded normal distribution can be obtained using the transformation of random variables to arrive at (B.6) which is further simplified to (B.9).

$$p_B(b) = \frac{1}{2\sqrt{b}\sqrt{2\pi}\sigma^2} \left(e^{-\left(\frac{(\sqrt{b}-\mu)^2}{2\sigma^2}\right)} + e^{-\left(\frac{(\sqrt{b}+\mu)^2}{2\sigma^2}\right)} \right) \quad (\text{B.6})$$

$$p_B(b) = \frac{1}{2\sqrt{b\sigma^2}} e^{-\left(\frac{b+\mu^2}{2\sigma^2}\right)} \sqrt{\frac{2}{\pi}} \cosh\left(\frac{\mu\sqrt{b}}{\sigma^2}\right) \quad (\text{B.7})$$

But $I_{-\frac{1}{2}}(x) = \frac{\sqrt{\frac{2}{\pi}} \cosh(x)}{\sqrt{x}}$ [122]

$$p_B(b) = \frac{1}{2\sqrt{b\sigma^2}} e^{-\left(\frac{b+\mu^2}{2\sigma^2}\right)} \sqrt{\frac{2}{\pi}} \sqrt{\left(\frac{\mu\sqrt{b}}{\sigma^2}\right)} I_{-\frac{1}{2}}\left(\frac{\mu\sqrt{b}}{\sigma^2}\right) \quad (\text{B.8})$$

$$p_B(b) = \frac{1}{2\sigma^2} \sqrt{\frac{\mu}{\sqrt{b}}} e^{-\left(\frac{b+\mu^2}{2\sigma^2}\right)} I_{-\frac{1}{2}}\left(\frac{\mu\sqrt{b}}{\sigma^2}\right) \quad (\text{B.9})$$

where $\sigma > 0$ and $b > 0$. (B.9) is a scaled non-central chi-squared distribution ($f(x | k, \lambda)$) with a scaling parameter of $\frac{1}{\sigma^2}$. It has one degree of freedom and a non centrality parameter $\lambda = \frac{\mu^2}{\sigma^2}$. Therefore, $p_B(b) = \frac{1}{\sigma^2} f\left(x_b = \frac{b}{\sigma^2} | k = 1, \lambda = \frac{\mu^2}{\sigma^2}\right)$.

We can therefore present (B.3) and (B.9) as a scaled non-central chi-squared distribution as given in (B.10) and (B.11) respectively.

$$p_A(x_a) = \frac{\sqrt{x_a}}{\sigma_1} e^{-\left(\frac{x_a}{2} + \frac{v^2}{2\sigma_1^2}\right)} I_0\left(\frac{v}{\sigma_1} \sqrt{x_a}\right) \quad (\text{B.10})$$

$$p_B(x_b) = \frac{1}{2\sigma^2} e^{-\left(\frac{x_b}{2} + \frac{\mu^2}{2\sigma^2}\right)} \left(\frac{\sigma^2 x_b}{\mu^2}\right)^{-\frac{1}{4}} I_{-\frac{1}{2}}\left(\frac{\mu}{\sigma} \sqrt{x_b}\right) \quad (\text{B.11})$$

Recall $\gamma_i = \frac{x_b}{x_a} = \frac{|\mathbf{h}_i^T \mathbf{\Theta} \mathbf{G} \mathbf{w}|^2}{S_{n+int}}$. Let z be a random variable with a one to one mapping to the variable x_a . The PDF of γ_i is obtained by solving (B.12).

$$p_\gamma(\gamma_i) = \int_{-\infty}^{\infty} p_B(\gamma_i z) p_A(z) |z| dz. \quad (\text{B.12})$$

$$p_\gamma(\gamma_i) = \int_{-\infty}^{\infty} \frac{1}{2\sigma^2} e^{-\left(\frac{\gamma_i z}{2} + \frac{\mu^2}{2\sigma^2}\right)} \left(\frac{\sigma^2 \gamma_i z}{\mu^2}\right)^{-\frac{1}{4}} I_{-\frac{1}{2}}\left(\frac{\mu}{\sigma} \sqrt{\gamma_i z}\right) \frac{\sqrt{z}}{\sigma_1} e^{-\left(\frac{z}{2} + \frac{v^2}{2\sigma_1^2}\right)} I_0\left(\frac{v}{\sigma_1} \sqrt{z}\right) |z| dz. \quad (\text{B.13})$$

We note that $\int_{-\infty}^{\infty} p_B(\gamma_i z) p_A(z) |z| dz = \int_{-\infty}^0 0 dz + \int_0^{\infty} p_B(\gamma_i z) p_A(z) |z| dz$ since $p_A(a) = p_B(b) = 0$ for $a \leq 0$ and $b \leq 0$. This implies that $z \geq 0$, therefore $|z| = z$.

$$p_\gamma(\gamma_i) = A(\gamma_i) \int_0^{\infty} z^{\frac{5}{4}} e^{-\left(\frac{z(\gamma_i+1)}{2}\right)} I_{-\frac{1}{2}}\left(\sqrt{\frac{\mu^2 \gamma_i}{\sigma^2}} \sqrt{z}\right) I_0\left(\sqrt{\frac{v^2}{\sigma_1^2}} \sqrt{z}\right) dz. \quad (\text{B.14})$$

where $A(\gamma_i) = \frac{1}{2\sigma^2\sigma_1} \left(\frac{\gamma_i\sigma^2}{\mu^2}\right)^{-\frac{1}{4}} e^{-\left(\frac{\mu^2}{2\sigma^2} + \frac{v^2}{2\sigma_1^2}\right)}$. Let $w = \sqrt{z}$, we therefore have that $dz = 2w dw$ and $z = w^2$.

$$p_\gamma(\gamma_i) = 2A(\gamma_i) \int_0^{\infty} w^{\frac{7}{2}} e^{-\left(\frac{w^2(\gamma_i+1)}{2}\right)} I_{-\frac{1}{2}}\left(\sqrt{\frac{\mu^2 \gamma_i}{\sigma^2}} w\right) I_0\left(\sqrt{\frac{v^2}{\sigma_1^2}} w\right) dw. \quad (\text{B.15})$$

Equation (B.15) satisfies the conditions given in [123, eq. 2.15.20.7] to obtain a closed form expression for the integral as given in (B.16).

$$p_\gamma(\gamma_i) = \frac{\sqrt{8} e^{-\left(\frac{\mu^2}{2\sigma^2} + \frac{v^2}{2\sigma_1^2}\right)}}{\gamma_i^{\frac{1}{2}} (\gamma_i + 1)^2 \sigma_1 \sigma^2} \sum_{k=0}^{\infty} \frac{\Gamma(k+2)}{k! \Gamma(k + \frac{1}{2})} \left(\frac{\mu^2 \gamma_i}{\sigma^2 (\gamma_i + 1)^2}\right)^k {}_2F_1\left(-k, \frac{1}{2} - k; 1; \frac{v^2 \sigma^2}{\mu^2 \sigma_1^2 \gamma_i}\right),$$

$\forall \gamma_i > 0. \quad (\text{B.16})$

By rearranging (B.16) to collect the terms of γ_i , we obtain (B.2) given in the Proposition. This completes the proof of the proposition.

Remark 1: Since the first element of the hypergeometric function is negative integer, the hypergeometric series is guaranteed to terminate thereby reducing to a polynomial [124], [66, eq. 9.101] [125, eq. 2.1.1.4], such that:

$${}_2F_1\left(-k, \frac{1}{2} - k; 1; \frac{v^2 \sigma^2}{\mu^2 \sigma_1^2 \gamma_i}\right) = \sum_{m=0}^k (-1)^m \binom{k}{m} \frac{(\frac{1}{2} - k)_m}{(1)_m} \left(\frac{v^2 \sigma^2}{\mu^2 \sigma_1^2 \gamma_i}\right)^m,$$

$\forall \left|\frac{v^2}{\sigma_1^2}\right| < \left|\frac{\mu^2}{\sigma^2} \gamma_i\right|, \quad (\text{B.17})$

where $\binom{k}{m} = \frac{k!}{m!(k-m)!}$.

Remark 2: By varying v and μ , the PDF in (B.2) moves from Rayleigh to exponential distribution. We note that the Rician distribution captures an LoS property

of the signal as well as its NLoS property. However, it can easily be reduced to a Rayleigh distribution representing a typical wireless scenario by setting $v = 0$.

Corollary 1: Based on (B.2), the cumulative density function (CDF) of γ_i is given as (B.18).

$$F_{\gamma_i}(t) = \sum_{k=0}^{\infty} \sum_{m=0}^k A_k (-1)^k \frac{(\frac{1}{2} - k)_k}{(1)_k} \left(\frac{v^2 \sigma^2}{\mu^2 \sigma_1^2} \right)^{k-m} \frac{(-k)_m (-k)_m t^{\frac{1}{2}+m}}{(\frac{1}{2})_m m! (\frac{1}{2} + m)} {}_2F_1 \left(2k + 2, \frac{1}{2} + m; \frac{3}{2} + m; -t \right),$$

$$\forall |\arg(1+t)| < \pi. \quad (\text{B.18})$$

where $(a)_m$ is the Pochhammer symbol (rising factorial) is presented as

$$(a)_m = \begin{cases} 1, & m = 0 \\ a(a+1)\dots(a+m-1) = \frac{\Gamma(a+m)}{\Gamma(a)}, & m > 0 \end{cases}$$

Proof: By definition of CDF, we have that $F_{\gamma_i}(t) = \int_{-\infty}^t p_{\gamma}(\gamma_i) d\gamma_i$. However, since $p_{\gamma}(\gamma_i) = 0 \ \forall \gamma_i \leq 0$, we have that $F_{\gamma_i}(t) = \int_0^t p_{\gamma}(\gamma_i) d\gamma_i$. By simplifying (B.2) with the definition of CDF, we have that

$$F_{\gamma_i}(t) = \sum_{k=0}^{\infty} A_k \int_0^t \frac{\gamma_i^{k-\frac{1}{2}}}{(\gamma_i + 1)^{2k+2}} {}_2F_1 \left(-k, \frac{1}{2} - k; 1; \left(\frac{v^2 \sigma^2}{\mu^2 \sigma_1^2 \gamma_i} \right) \right) d\gamma_i. \quad (\text{B.19})$$

For simplification, by applying the transformation of [126, eq. 15.8.6] to the hypergeometric function and expanding with the terminating hypergeometric series definition presented in Remark 1, (B.19) can be re-written as (B.20).

$$F_{\gamma_i}(t) = \sum_{k=0}^{\infty} \sum_{m=0}^k A_k (-1)^k \frac{(\frac{1}{2} - k)_k}{(1)_k} \left(\frac{v^2 \sigma^2}{\mu^2 \sigma_1^2} \right)^{k-m} \frac{(-k)_m (-k)_m}{(\frac{1}{2})_m m!} \int_0^t \frac{\gamma_i^{m-\frac{1}{2}}}{(\gamma_i + 1)^{2k+2}} d\gamma_i. \quad (\text{B.20})$$

The integral in (B.20) can be obtained from [66, eq. 3.194.1] to (B.21).

$$\begin{aligned}
 F_{\gamma_i}(t) = & \sum_{k=0}^{\infty} \sum_{m=0}^k A_k (-1)^k \frac{\left(\frac{1}{2} - k\right)_k}{(1)_k} \left(\frac{v^2 \sigma^2}{\mu^2 \sigma_1^2} \right)^{k-m} \\
 & \frac{(-k)_m (-k)_m t^{\frac{1}{2}+m}}{\left(\frac{1}{2}\right)_m m! \left(\frac{1}{2} + m\right)} {}_2F_1 \left(2k + 2, \frac{1}{2} + m; \frac{3}{2} + m; -t \right), \\
 & \forall |\arg(1+t)| < \pi, \quad (\text{B.21})
 \end{aligned}$$

$$\text{where } A_k = \frac{\sqrt{8} e^{-\left(\frac{\mu^2}{2\sigma^2} + \frac{v^2}{2\sigma_1^2}\right)} \Gamma(k+2)}{k! \sigma_1 \sigma^2 \Gamma\left(k + \frac{1}{2}\right)} \left(\frac{\mu^2}{\sigma^2} \right)^k.$$

The conditions for the validity for (B.21) holds true for real values of $t \geq 0$. That completes the proof of the corollary.

Appendix C

KKT Solution to P4.5 in Section

4.3.3.1

To provide a solution to (4.26) from section 4.3.3.1, we express the lower bound for the distances using the reverse triangular inequality and variable change as

$$\begin{aligned} d_{\text{RE}}^2 d_{\text{AR}}^2 &= \|\boldsymbol{\Omega}_{\text{E}} - \mathbf{q}_{\text{R}}\|^2 \|\mathbf{q}_{\text{R}} - \boldsymbol{\Omega}_{\text{A}}\|^2 \geq (\|\boldsymbol{\Omega}_{\text{E}}\| - \|\mathbf{q}_{\text{R}}\|)^2 (\|\mathbf{q}_{\text{R}}\| - \|\boldsymbol{\Omega}_{\text{A}}\|)^2 \\ &= \left(\underbrace{\frac{\|\boldsymbol{\Omega}_{\text{E}}\|}{\|\boldsymbol{\Omega}_{\text{A}}\|}}_{\bar{\Omega}_{\text{E}}} - \underbrace{\frac{\|\mathbf{q}_{\text{R}}\|}{\|\boldsymbol{\Omega}_{\text{A}}\|}}_{\varepsilon} \right)^2 \left(\underbrace{\frac{\|\mathbf{q}_{\text{R}}\|}{\|\boldsymbol{\Omega}_{\text{A}}\|}}_{\varepsilon} - 1 \right)^2 \|\boldsymbol{\Omega}_{\text{A}}\|^4 = (\bar{\Omega}_{\text{E}} - \varepsilon)^2 (\varepsilon - 1)^2 \|\boldsymbol{\Omega}_{\text{A}}\|^4 \end{aligned}$$

Similarly,

$$\begin{aligned} d_{\text{RB}}^2 d_{\text{AR}}^2 &\geq (\bar{\Omega}_{\text{B}} - \varepsilon)^2 (\varepsilon - 1)^2 \|\boldsymbol{\Omega}_{\text{A}}\|^4, \\ \|\mathbf{q}_{\text{R}}[n] - \mathbf{q}_{\text{R}}[n-1]\|^2 &\geq (\varepsilon - \bar{\Omega}_q)^2 \|\boldsymbol{\Omega}_{\text{A}}\|^2; \\ \text{where } \bar{\Omega}_q &= \frac{\|\mathbf{q}_{\text{R}}[n-1]\|}{\|\boldsymbol{\Omega}_{\text{A}}\|}. \end{aligned}$$

Considering that the trajectory of the UAV is a sequential combination of its location at instantaneous n samples, the objective of (4.26) can be scaled to obtaining the maximum value for each n sample. The summation of these isolated optimal points

provides optimal the objective value as defined in (4.26). Hence, by using variable change as defined above, (4.26) can be rewritten as (C.2) $\forall n \in [1, \dots, N]$.

$$\max_{\varepsilon} \log_2 \left(\frac{1}{\beta} + \frac{\bar{P}M\rho_0^2\varsigma_B^2K^2}{\beta(\bar{\Omega}_B - \varepsilon)^2(\varepsilon - 1)^2\|\mathbf{\Omega}_A\|^4} \right), \quad (\text{C.2a})$$

$$\text{s.t. } \frac{1 - \beta}{|\varsigma|^2} + \frac{\bar{P}M\rho_0^2\varsigma_E^2}{\beta(\bar{\Omega}_E - \varepsilon)^2(\varepsilon - 1)^2\|\mathbf{\Omega}_A\|^4} \leq 0, \quad (\text{C.2b})$$

$$(\varepsilon - \bar{\Omega}_q)^2\|\mathbf{\Omega}_A\|^2 \leq (Z\alpha)^2. \quad (\text{C.2c})$$

Problem (C.2) is differentiable and possibly non-convex due to (C.2a) and (C.2b). However, let ε^* and $(\lambda_1^*, \lambda_2^*)$ represent the primal and dual optimal variables with zero duality gap, the KKT conditions given in (C.3) must be satisfied.

$$\nabla f_0(\varepsilon^*) + \lambda_1^* \nabla f_1(\varepsilon^*) + \lambda_2^* \nabla f_2(\varepsilon^*) = 0, \quad (\text{C.3a})$$

$$\lambda_1^* f_1(\varepsilon^*) = 0, \quad (\text{C.3b})$$

$$\lambda_2^* f_2(\varepsilon^*) = 0. \quad (\text{C.3c})$$

By using the functions from (C.2) where f_0 is the objective function and f_1 and f_2 are the constraint functions corresponding to (C.3b) and (C.3c) respectively, we note that $\lambda_1^* = f(\varepsilon^*, \lambda_2^*)$ by solving (C.3a), $\lambda_2^* = f(\varepsilon^*)$ by solving (C.3b) and substituting λ_1^* . Therefore, by solving (C.3c), we obtain the cubic function $\varepsilon^3 - b\varepsilon^2 + c\varepsilon + d = 0$ with discriminant $\Delta = (bc)^2 + 18(bcd) - 4c^3 - 4b^3d - 27d^2$; (ε, b, c, d has been presented in (4.28)). It is easy to see that the discriminant is less than 0 which implies that the solution to the cubic function comprise of 2 complex conjugate pairs roots and one real root. Since we are interested in the coordinates located in the real plane, the only relevant solution is the real root as shown in (4.28). Having obtained ε , the location of the UAV at the n th sample can be deduced by modifying $\varepsilon = \frac{\|\mathbf{q}_R\|}{\|\mathbf{\Omega}_A\|}$ leading to Proposition 1.

References

- [1] D. G. Costa, L. A. Guedes, F. Vasques, and P. Portugal, “Partial energy-efficient hop-by-hop retransmission in wireless sensor networks,” in *11th IEEE Int. Conf. on Ind. Informatics (INDIN)*, 2013, pp. 146–151.
- [2] T. M. Hoang, T. Q. Duong, H. D. Tuan, S. Lambotharan, and L. Hanzo, “Physical layer security: Detection of active eavesdropping attacks by support vector machines,” *IEEE Access*, vol. 9, pp. 31 595–31 607, 2021.
- [3] A. Mukherjee and A. L. Swindlehurst, “Detecting passive eavesdroppers in the mimo wiretap channel,” in *IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, 2012, pp. 2809–2812.
- [4] A. Mukherjee, “Physical-layer security in the Internet of things: Sensing and communication confidentiality under resource constraints,” *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.
- [5] P. K. Gopala, L. Lai, and H. E. Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Info. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
- [6] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
- [7] H. Zimmermann, “OSI reference model - the ISO model of architecture for open systems interconnection,” *IEEE Trans. Commun.*, vol. 28, no. 4, pp. 425–432, 1980.

- [8] J. Day and H. Zimmermann, “The OSI reference model,” *Proc. IEEE*, vol. 71, no. 12, pp. 1334–1340, 1983.
- [9] V. Cerf and R. Kahn, “A protocol for packet network intercommunication,” *IEEE Trans. Commun.*, vol. 22, no. 5, pp. 637–648, 1974.
- [10] L. Sun and Q. Du, “Physical layer security with its applications in 5G networks: A review,” *China Commun.*, vol. 14, no. 12, pp. 1–14, Dec. 2017.
- [11] Y. Liu, H.-H. Chen, and L. Wang, “Physical layer security for next generation wireless networks: Theories, technologies, and challenges,” *IEEE Commun. Surveys and Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.
- [12] A. Yener and S. Ulukus, “Wireless physical-layer security: Lessons learned from information theory,” *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, 2015.
- [13] L. Sun and Q. Du, “A review of physical layer security techniques for internet of things: Challenges and solutions,” *Entropy*, vol. 20, no. 10, p. 730, Sep. 2018.
- [14] N. Ebrahimi, H.-S. Kim, and D. Blaauw, “Physical layer secret key generation using joint interference and phase shift keying modulation,” *IEEE Trans. Microwave Theory and Techniques*, vol. 69, no. 5, pp. 2673–2685, 2021.
- [15] M. Bottarelli, P. Karadimas, G. Epiphaniou, D. K. B. Ismail, and C. Maple, “Adaptive and optimum secret key establishment for secure vehicular communications,” *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2310–2321, 2021.
- [16] R. Melki, H. N. Noura, and A. Chehab, “Lightweight and secure d2d authentication & key management based on pls,” in *IEEE 90th Veh. Technol. Conf. (VTC2019-Fall)*, 2019, pp. 1–7.
- [17] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, “A tutorial on UAVs for wireless networks: Applications, challenges, and open problems,” *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 3, pp. 2334–2360, 2019.

- [18] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
- [19] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Info. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.
- [20] A. B. Carleial and M. E. Hellman, "A note on wyner's wiretap channel," *IEEE Trans. Info. Theory*, vol. 23, no. 3, pp. 387–390, May 1977.
- [21] A. D. Wyner, "The wire-tap channel," *The Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [22] R. Roy, "An overview of smart antenna technology and its application to wireless communication systems," in *IEEE Int. Symp. Pers., Indoor, Mobile Radio Commun.* IEEE, 1997.
- [23] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Info. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [24] L. Tao, W. Yang, Y. Cai, and D. Chen, "On secrecy outage probability and average secrecy rate of large-scale cellular networks," *Hindawi Wireless Commun. and Mobile Computing*, 2018, ISSN: 1530-8669.
- [25] J. A. Anastasov, A. S. Panajotovic, N. M. Sekulovic, D. N. Milic, and D. M. Milovic, "Secrecy outage probability and intercept probability analysis over α -f fading channels," in *57th Intl. Sci. Conf. on Inf., Commun. and Energy Sys. and Technol. (ICEST)*, 2022, pp. 1–4.
- [26] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [27] Y. Yang, C. Sun, H. Zhao, H. Long, and W. Wang, "Algorithms for secrecy guarantee with null space beamforming in two-way relay networks," *IEEE Trans. Signal Process.*, vol. 62, no. 8, pp. 2111–2126, Apr. 2014.

- [28] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, “Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, Dec. 2013.
- [29] A. Li, Q. Wu, and R. Zhang, “UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel,” *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 181–184, Feb. 2019.
- [30] J. Zhu, R. Schober, and V. K. Bhargava, “Linear precoding of data and artificial noise in secure massive mimo systems,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, 2016.
- [31] Z. Li, M. Chen, C. Pan, N. Huang, Z. Yang, and A. Nallanathan, “Joint trajectory and communication design for secure UAV networks,” *IEEE Commun. Lett.*, vol. 23, no. 4, pp. 636–639, Apr. 2019.
- [32] G. Zhang, Q. Wu, M. Cui, and R. Zhang, “Securing UAV communications via joint trajectory and power control,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1376–1389, Feb. 2019.
- [33] Y. Zeng and R. Zhang, “Energy-efficient UAV communication with trajectory optimization,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3747–3759, Jun. 2017.
- [34] İbrahim Kocaman, “Distributed beamforming in a swarm UAV network,” Master’s thesis, Naval Postgraduate School, 2008.
- [35] D. Fan, F. Gao, B. Ai, G. Wang, Z. Zhong, Y. Deng, and A. Nallanathan, “Channel estimation and self-positioning for UAV swarm,” *IEEE Trans. Commun.*, pp. 1–10, 2019.
- [36] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, “Physical layer security in UAV systems: Challenges and opportunities,” *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 40–47, Oct. 2019.

- [37] X. Zhu, Z. Liu, and J. Yang, “Model of collaborative UAV swarm toward coordination and control mechanisms study,” *Procedia Computer Science*, vol. 51, pp. 493–502, 2015, Int. conf. on computational science, (ICCS).
- [38] H. Ling, H. Luo, H. Chen, L. Bai, T. Zhu, and Y. Wang, “Modelling and simulation of distributed UAV swarm cooperative planning and perception,” *Int. J. of Aerospace Engineering*, vol. 2021, 2021.
- [39] A. Ahmed, S. Zhang, and Y. D. Zhang, “Multi-target motion parameter estimation exploiting collaborative UAV network,” in *IEEE Int. Conf. Acoustics, Speech and Signal Process. (ICASSP)*. Brighton, United Kingdom: IEEE, May 2019, pp. 4459–4463.
- [40] X. Wang, W. Feng, Y. Chen, and N. Ge, “UAV swarm-enabled aerial CoMP: A physical layer security perspective,” *IEEE Access*, vol. 7, pp. 120 901–120 916, 2019.
- [41] P. Gaudiano, B. Shargel, E. Bonabeau, and B. T. Clough, “Swarm intelligence and a new and c2 paradigm and with an and application to control and of swarms and of UAVs,” *8th ICCRTS Command and Control Research and Technology Symposium*, 1999.
- [42] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M. Alouini, and R. Zhang, “Wireless communications through reconfigurable intelligent surfaces,” *IEEE Access*, vol. 7, pp. 116 753–116 773, 2019.
- [43] J. Zhao and Y. Liu, “A survey of intelligent reflecting surfaces (IRSs): Towards 6G wireless communication networks with massive MIMO 2.0,” 2019, Accessed 12-December-2020 <https://arxiv.org/abs/1907.04789>.
- [44] Y. Song, M. R. A. Khandaker, F. Tariq, and K.-K. Wong, “Truly intelligent reflecting surface-aided secure communication using deep learning,” in *IEEE 91st Veh. Technol. Conf.: VTC2020-Fall*, 2020.

- [45] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, “Intelligent reflecting surface-aided wireless communications: A tutorial,” *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3313–3351, 2021.
- [46] S. Mazahir, S. Ahmed, and M.-S. Alouini, “A survey on joint communication-radar systems,” *Frontiers in Commun. and Net.*, vol. 1, p. 9, 2021, <https://www.frontiersin.org/article/10.3389/frcmn.2020.619483>.
- [47] A. Martone and M. Amin, “A view on radar and communication systems coexistence and dual functionality in the era of spectrum sensing,” *Digital Signal Process.*, vol. 119, p. 103135, 2021, <https://www.sciencedirect.com/science/article/pii/S1051200421001743>.
- [48] J.-w. Pak and M.-k. Kim, “Convolutional neural network approach for aircraft noise detection,” in *2019 Intl. Conf. on Artificial Intelligence in Info. and Commun. (ICAIIC)*, 2019, pp. 430–434.
- [49] Y. Gu, Z. Wu, Z. Yin, and X. Zhang, “The secrecy capacity optimization artificial noise: A new type of artificial noise for secure communication in mimo system,” *IEEE Access*, vol. 7, pp. 58 353–58 360, 2019.
- [50] H. Deng, H.-M. Wang, W. Guo, and W. Wang, “Secrecy transmission with a helper: To relay or to jam,” *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 293–307, 2015.
- [51] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, “Physical layer security jamming: Theoretical limits and practical designs in wireless networks,” *IEEE Access*, vol. 5, pp. 3603–3611, 2017.
- [52] G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng, and Y. Chen, “Physical-layer security over non-small-scale fading channels,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1326–1339, Mar. 2016.

- [53] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, 2010.
- [54] O. Punal, C. Pereira, A. Aguiar, and J. Gross, “Experimental characterization and modeling of rf jamming attacks on vanets,” *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 524–540, 2015.
- [55] S. Zhang, Y. Zeng, and R. Zhang, “Cellular-enabled UAV communication: A connectivity-constrained trajectory optimization Perspective,” *IEEE Trans. Commun.*, vol. 67, no. 4, pp. 2580–2604, Mar. 2019.
- [56] X. Zhou, Q. Wu, S. Yan, F. Shu, and J. Li, “UAV-enabled secure communications: Joint trajectory and transmit power optimization,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 4069–4073, Apr. 2019.
- [57] Q. Wu and R. Zhang, “Common throughput maximization in UAV-enabled OFDMA systems with delay consideration,” *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6614–6627, Dec. 2018.
- [58] Y. Zeng, R. Zhang, and T. J. Lim, “Throughput maximization for UAV-enabled mobile relaying systems,” *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 4983–4996, Dec. 2016.
- [59] F. Cheng and S. Zhang and Z. Li and Y. Chen and N. Zhao and F. R. Yu and V. C. M. Leung, “UAV trajectory optimization for data offloading at the edge of multiple cells,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6732–6736, Jul. 2018.
- [60] H. Wang, J. Wang, J. Chen, Y. Gong, and G. Ding, “Network-connected UAV communications: Potentials and Challenges,” *China Commun.*, vol. 15, no. 12, pp. 111–121, Dec. 2018.
- [61] L. Shen, N. Wang, and X. Mu, “Iterative UAV trajectory optimization for physical layer secure mobile relaying,” in *Int. Conf. Cyber-Enabled Distributed*

- Computing and Knowledge Discovery (CyberC '18)*. Zhengzhou, China: IEEE, Oct. 2018, pp. 19–23.
- [62] A. Li and W. Zhang, “Mobile jammer-aided secure UAV communications via trajectory design and power control,” *China Commun.*, vol. 15, no. 8, pp. 141–151, Aug. 2018.
- [63] Y. Gao, H. Tang, B. Li, and X. Yuan, “Joint trajectory and power design for UAV-enabled secure communications with no-fly zone Constraints,” *IEEE Access*, vol. 7, pp. 44 459–44 470, Apr. 2019.
- [64] M. Cui, G. Zhang, Q. Wu, and D. W. K. Ng, “Robust trajectory and transmit power design for secure UAV communications,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 9042–9046, Sep. 2018.
- [65] J. Ye, C. Zhang, H. Lei, G. Pan, and Z. Ding, “Secure UAV-to-UAV systems with spatially random UAVs,” *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 564–567, Apr. 2019.
- [66] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series and products*, 7th ed., A. Jeffrey and D. Zwillinger, Eds. USA: Academic Press, 2007.
- [67] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U. K.: Cambridge University Press, 2004.
- [68] Wei Yu and R. Lui, “Dual methods for nonconvex spectrum optimization of multicarrier systems,” *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1310–1322, Jul. 2006.
- [69] F. W. J. Olver, W. Lozier, Daniel, F. Boisvert, Ronald, and W. Clark, Charles, Eds., *NIST handbook of mathematical functions*. Cambridge University Press, Jul. 2010.
- [70] Yang Yang, Marius Pesavento, Symeon Chatzinotas, and Bjorn Ottersten, “Successive convex approximation algorithms for sparse signal estimation with

- nonconvex regularizations,” *IEEE J. Selected Topics in Signal Process.*, vol. 12, no. 6, pp. 1286–1302, 2018.
- [71] M. Razaviyayn, *Successive convex approximation: Analysis and applications*. University of Minnesota, PhD Thesis, 2014.
- [72] M. Grant and S. Boyd, *Recent advances in learning and control*, ser. Lecture Notes in Control and Information Sciences. Springer-Verlag Limited, Mar 2008, ch. Graph implementations for nonsmooth convex programs, pp. 95–110.
- [73] —, “CVX: Matlab software for disciplined convex programming, version 2.1,” <http://cvxr.com/cvx>, Mar. 2014.
- [74] F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, “A speculative study on 6G,” *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 118–125, 2020.
- [75] I. F. Akyildiz, A. Kak, and S. Nie, “6G and beyond: The future of wireless communication system,” *IEEE Access*, vol. 8, pp. 133 995–134 030, 2020.
- [76] C. O. Nnamani, M. R. A. Khandaker, and M. Sellathurai, “UAV-aided jamming for secure ground communication with unknown eavesdropper location,” *IEEE Access*, vol. 8, pp. 72 881–72 892, Apr. 2020.
- [77] S. Yeh, J.-F. Chamberland, and G. H. Huff, “An investigation of geolocation-aware beamforming algorithms for swarming UAVs,” in *IEEE Int. Symp. Antennas Propag.* IEEE, Jul. 2017.
- [78] Y. Lu and J. Fang and Z. Guo and J. A. Zhang, “Distributed transmit beamforming for UAV to base station,” *China Communications*, vol. 16, no. 1, pp. 15–25, Jan. 2019.
- [79] R. Mudumbai, D. R. Brown Iii, U. Madhow, and H. V. Poor, “Distributed transmit beamforming: challenges and recent progress,” *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 102–110, 2009.

- [80] M. R. A. Khandaker and K. Wong, “Swipt in MISO multicasting systems,” *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 277–280, Jun. 2014.
- [81] M. R. A. Khandaker and K.-K. Wong, “Masked beamforming in the presence of energy-harvesting eavesdroppers,” *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 40–54, 2015.
- [82] K. B. Petersen and M. S. Pedersen, “The matrix cookbook,” Nov. 2012, version 20121115, <http://localhost/pubdb/p.php?3274>.
- [83] M. R. A. Khandaker and Y. Rong, “Interference MIMO relay channel: Joint power control and transceiver-relay beamforming,” *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6509–6518, 2012.
- [84] P. Comon, G. Golub, L.-H. Lim, and B. Mourrain, “Symmetric tensors and symmetric tensor rank,” *SIAM J. on Matrix Analysis and Applications*, vol. 30, no. 3, 2008.
- [85] J. Hoydis, S. ten Brink, and M. Debbah, “Massive MIMO in the UL/DL of cellular networks: How many antennas do we need?” *IEEE J. on Selected Areas in Commun.*, vol. 31, no. 2, pp. 160–171, 2013.
- [86] Q. Wu and R. Zhang, “Intelligent reflecting surface enhanced wireless network: Joint active and passive beamforming design,” in *IEEE Global Commun. Conf. (GLOBECOM)*, 2018.
- [87] S. Li, B. Duo, X. Yuan, Y.-C. Liang, and M. D. Renzo, “Reconfigurable intelligent surface assisted UAV communication: Joint trajectory design and passive beamforming,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 716–720, 2020.
- [88] D. Ma, M. Ding, and M. Hassan, “Enhancing cellular communications for UAVs via intelligent reflective surface,” in *IEEE Wireless Commun. and Net. Conf. (WCNC)*, 2020.
- [89] J. Chen, Y. Liang, Y. Pei, and H. Guo, “Intelligent reflecting surface: A programmable wireless environment for physical layer security,” *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019.

- [90] M. Cui, G. Zhang, and R. Zhang, “Secure wireless communication via intelligent reflecting surface,” *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, 2019.
- [91] O. Ozdogan, E. Bjornson, and E. G. Larsson, “Intelligent reflecting surfaces: Physics, propagation, and pathloss modeling,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 581–585, 2020.
- [92] H. Lu, Y. Zeng, S. Jin, and R. Zhang, “Aerial intelligent reflecting surface: Joint placement and passive beamforming design with 3D beam flattening,” *IEEE Trans. Wireless Commun.*, 2020.
- [93] H. Long, M. Chen, Z. Yang, B. Wang, Z. Li, X. Yun, and M. Shikh-Bahaei, “Reflections in the sky: Joint trajectory and passive beamforming design for secure UAV networks with reconfigurable intelligent surface,” 2020, Accessed 15-January-2021 <https://arxiv.org/abs/2005.10559>.
- [94] K. Zarifi, S. Affes, and A. Ghayeb, “Collaborative null-steering beamforming for uniformly distributed wireless sensor networks,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1889–1903, 2010.
- [95] E. Basar, “Reconfigurable intelligent surfaces for doppler effect and multipath fading mitigation,” 2020, Accessed 15-January-2021 <https://arxiv.org/abs/1912.04080>.
- [96] B. Matthiesen, E. Björnson, E. De Carvalho, and P. Popovski, “Intelligent reflecting surface operation under predictable receiver mobility: A continuous time propagation model,” *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 216–220, 2021.
- [97] L. Ge, P. Dong, H. Zhang, J. Wang, and X. You, “Joint beamforming and trajectory optimization for intelligent reflecting surfaces-assisted UAV communications,” *IEEE Access*, vol. 8, pp. 78 702–78 712, 2020.

- [98] M. Tummala, C. C. Wai, and P. Vincent, “Distributed beamforming in wireless sensor networks,” in *39 Asilomar Conf. on Signals, Systems and Computers*, 2005, pp. 793–797.
- [99] J. Si, Z. Li, J. Cheng, and C. Zhong, “Secrecy performance of multi-antenna wiretap channels with diversity combining over correlated Rayleigh fading channels,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 1, pp. 444–458, 2019.
- [100] M. Z. I. Sarkar and T. Ratnarajah, “Enhancing security in correlated channel with maximal ratio combining diversity,” *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6745–6751, 2012.
- [101] J. Lundén, “Spectrum sensing for cognitive radio and radar systems,” Ph.D. dissertation, Helsinki University of Technology, 2009.
- [102] A. Nasser, A. H. Hassan, A. C. H., M. A. J., and K. C. Yao, “Spectrum sensing for cognitive radio: Recent advances and future challenge,” *Sensors*, vol. 21, no. 7, 2021.
- [103] Y. Cui, F. Liu, X. Jing, and J. Mu, “Integrating sensing and communications for ubiquitous IoT: Applications, trends and challenges,” 2021, Accessed 16-February-2022, <https://arxiv.org/abs/2104.11457>.
- [104] J. A. Zhang, F. Liu, C. Masouros, R. W. Heath, Z. Feng, L. Zheng, and A. Petropulu, “An overview of signal processing techniques for joint communication and radar sensing,” *IEEE J. Selected Topics in Signal Process.*, vol. 15, no. 6, pp. 1295–1315, Nov. 2021.
- [105] R. Thomä, T. Dallmann, S. Jovanoska, P. Knott, and A. Schmeink, “Joint communication and radar sensing: An overview,” in *15th European Conf. on Antennas and Propagation (EuCAP)*, 2021, pp. 1–5.
- [106] F. Liu, C. Masouros, A. P. Petropulu, H. Griffiths, and L. Hanzo, “Joint radar and communication design: Applications, state-of-the-art, and the road ahead,” *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3834–3862, 2020.

- [107] H. Li, “Inseparable waveform synthesis in joint communications and radar via spatial-frequency spectrum,” in *IEEE Global Commun. Conf. (GLOBECOM)*, 2021.
- [108] S. Sodagari, A. Khawar, T. C. Clancy, and R. McGwier, “A projection based approach for radar and telecommunication systems coexistence,” in *IEEE Global Commun. Conf. (GLOBECOM)*, 2012, pp. 5010–5014.
- [109] A. Hassanien, B. Himed, and M. G. Amin, “Transmit/receive beamforming design for joint radar and communication systems,” in *IEEE Radar Conf. (RadarConf18)*, 2018, pp. 1481–1486.
- [110] F. Liu, C. Masouros, A. Li, H. Sun, and L. Hanzo, “MU-MIMO communications with MIMO radar: From co-existence to joint transmission,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2755–2770, 2018.
- [111] N. Su, F. Liu, and C. Masouros, “Enhancing the physical layer security of dual-functional radar communication systems,” in *IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6.
- [112] A. Hassanien, M. G. Amin, Y. D. Zhang, and F. Ahmad, “Dual-function radar-communications: Information embedding using sidelobe control and waveform diversity,” *IEEE Trans. Signal Process.*, vol. 64, no. 8, pp. 2168–2181, 2016.
- [113] A. N. Pineda, L. U. Aragonés, J. R. F. del Castillo Díez, and M. Ángel Patriocio Guisado, “Radar tracking system using contextual information on a neural network architecture in air combat maneuvering,” *Int. J. of Distributed Sensor Net.*, vol. 9, no. 8, pp. 1–11, 2013.
- [114] I. Bekkerman and J. Tabrikian, “Target detection and localization using mimo radars and sonars,” *IEEE Trans. Signal Process.*, vol. 54, no. 10, pp. 3873–3883, 2006.
- [115] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016, <http://www.deeplearningbook.org>.

- [116] K. Slot, P. Kapusta, and J. Kucharski, “Autoencoder-based image processing framework for object appearance modifications,” *Neural Computing and Applications*, vol. 33, 2021.
- [117] K. Adamiak, P. Kapusta, and K. Ślot, “Facial appearance modifications using skpca-derived features extracted from convolutional autoencoder’s latent space,” in *Int. Joint Conf. on Neural Networks (IJCNN)*, 2020, pp. 1–7.
- [118] G. K. Papageorgiou and M. Sellathurai, “Direction-of-arrival estimation in the low-snr regime via a denoising autoencoder,” in *IEEE 21st Int. Workshop on Signal Process. Advances in Wireless Commun. (SPAWC)*, 2020, pp. 1–5.
- [119] —, “Fast direction-of-arrival estimation of multiple targets using deep learning and sparse arrays,” in *Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, 2020, pp. 4632–4636.
- [120] R. D. Devapriya, P. Sudharsan, and C. Tellambura, “Coverage analysis of intelligent reflecting surface systems in rayleigh fading,” *Electronics Lett.*, vol. 58, 2022.
- [121] I. Hazem, T. Hina, and T. N. Uyen, “Exact coverage analysis of intelligent reflecting surfaces with Nakagami-m channels,” 2021, Accessed 16-November-2021, <https://arxiv.org/abs/2101.00740v1>.
- [122] “The Wolfram Functions site. BesselI function. [Online].” 2001, Accessed 10-September-2021, <http://functions.wolfram.com/03.02.03.0005.01>.
- [123] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and series*. UK: Gordon and Breach Science Publishers, 1986, vol. 2 - Special Functions.
- [124] “Hypergeometric function,” 2021, Accessed 10-September-2021, https://en.wikipedia.org/wiki/Hypergeometric_function.
- [125] A. Erdelyi, ed., *Higher Transcendental Functions*. USA: McGraw Hill Book Company, 1953, vol. 1.

- [126] F. W. J. Olver, A. B. Olde Daalhuis, D. W. Lozier, B. I. Schneider, R. F. Boisvert, C. W. Clark, B. R. Miller, B. V. Saunders, H. S. Cohl, and M. A. McClain, eds., “Nist digital library of mathematical functions,” Release 1.1.2, Accessed 22-September-2021, <http://dlmf.nist.gov/>.