COORDINATED MULTI-POINT SYSTEMS FOR FUTURE WIRELESS COMMUNICATION NETWORKS

A DISSERTATION SUBMITTED TO
THE GRADUATE SCHOOL OF
ENGINEERING AND NATURAL SCIENCES
OF ISTANBUL MEDIPOL UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF
DOCTOR OF PHILOSOPHY
IN
ELECTRICAL, ELECTRONICS ENGINEERING AND CYBER SYSTEMS

By

Muhammad Sohaib Jamal Solaija

July, 2023

COORDINATED MULTI-POINT SYSTEMS FOR FUTURE WIRELESS COMMUNICATION NETWORKS

By Muhammad Sohaib Jamal Solaija

28 July 2023

We certify that we have read this dissertation and that in our opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

_____

Prof. Dr. Hüseyin Arslan (Advisor)

_____

Prof. Dr. Ali Emre Pusane

_____

Prof. Dr. Selim Akyokuş

_____

Prof. Dr. Mehmet K. Özdemir

_____

Assoc. Prof. Dr. Ertuğrul Başar

Approved by the Graduate School of Engineering and Natural Sciences:

_____

Prof. Dr. Yasemin Yüksel Durmaz

Director of the Graduate School of Engineering and Natural Sciences

I hereby declare that all information in this document has been obtained and presented in accordance with the academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Signature :

Name, Surname: MUHAMMAD SOHAIB JAMAL SOLAIJA

ACKNOWLEDGEMENT

First and foremost, all praise and gratitude be to Allah SWT for first granting me this opportunity and then the steadfastness to culminate this doctoral journey. I cannot thank and appreciate my parents enough for their unwavering support, prayers and love. Similarly, the pampering that I have received from my siblings has been monumental fun and their children are a joy for the heart.

I want to acknowledge the efforts of my advisor Prof. Arslan for continuously pushing me to do better. I would also like to give a shoutout to the support staff at Medipol/CoSiNC, especially Hasan and Burak Abi, Yusuf, Furkan, Barış, Tuba and Ahmet Yazar for making all the formal (and sometimes unnecessary) procedures easy and manageable. I am also thankful to my thesis committee and jury members for their valuable time and efforts.

This whole adventure would not have been the same if it wasn't for the seniors sharing their experiences, my peers letting me be a part of theirs, and the juniors expressing their enthusiasm and positive vibes.

To the friends outside Medipol, new and old, thank you for reiterating that while this PhD is a critical part of my life it is not the entirety of it; the Earth isn't closed, and there are lots of important things in life beyond this. Finally, to my significant other and her family, thank you for trusting me and welcoming me to your family.

I would like to end by praying to Allah SWT that all that I learned during this journey turns out to be *ilm-e-nafe'* and benefits me and the people around me. Ameen!

Muhammad Sohaib Jamal Solaija

July, 2023

CONTENTS

Page

ACKNOWLEDGEMENT ..... **iv**
CONTENTS ..... **v**
LIST OF FIGURES ..... **vii**
LIST OF TABLES ..... **ix**
LIST OF SYMBOLS ..... **x**
ABBREVIATIONS ..... **xi**
ÖZET ..... **xv**
ABSTRACT ..... **xvii**
1. INTRODUCTION **1**
1.1. Coordinated Multipoint (CoMP) 2
1.1.1. Thesis contributions under CoMP 2
1.2. Physical Layer Security (PLS) 4
1.2.1. Thesis contributions under PLS 6
2. THEORETICAL PART **7**
2.1. Generalized CoMP (GCoMP) Framework 7
2.1.1. Evolution of CoMP 7
2.1.2. CoMP for 5G and Beyond Requirements 11
2.1.3. GCoMP Framework 15
2.2. CoMP for Reliability 21
2.3. CoMP for Physical Layer Security (PLS) 23
2.3.1. Overview of Channel Shortening 24
2.4. Secure Communication in the Presence of Eavesdropping Relays 25
2.5. Delay-Doppler Based Key Generation in V2X Communication 27
2.6. Unified PLS Framework 29
2.6.1. Overview of Wireless Security Threats 29
2.6.3. Physical Layer Security Framework: Definition and Domains 33
2.6.4. Latest Trends and Future Directions for Physical Layer Security 52
3. EXPERIMENTAL PART **62**
3.1. Generalized CoMP (GCoMP) Framework 62
3.1.1. System Model/Assumptions 63
3.1.2. Problem Formulation 65
3.2. CoMP for Reliability 67
3.2.1. System Model and Assumptions 67
3.2.2. Proposed Macro-Diversity Scheme 71
3.3. CoMP for Physical Layer Security (PLS) 72
3.3.1. System Model and Proposed Approach 72
3.3.2. Performance Analysis 73
3.4. Secure Communication in the Presence of Eavesdropping Relays 75
3.4.1. System Model 75
3.4.2. Proposed Approach 76
3.5. Delay-Doppler Based Key Generation in V2X Communication 80
3.5.1. System Model 80
3.5.2. Proposed Key Generation Using Delay-Doppler Indices 81
3.5.3. Security Analysis 82
4. RESULTS AND DISCUSSION **88**
4.1. Generalized CoMP (GCoMP) Framework 88
4.2. CoMP for Reliability 93

4.3. CoMP for Physical Layer Security (PLS) 95
4.4. Secure Communication in the Presence of Eavesdropping Relays 98
4.5. Delay-Doppler Based Key Generation in V2X Communication 101
5. CHALLENGES AND RESEARCH DIRECTIONS 105
5.1. Challenges for (Generalized) Coordinated Multipoint 105
5.2. Challenges for Physical Layer Security 108
6. CONCLUSIONS AND FUTURE WORK 111
BIBLIOGRAPHY 114
CURRICULUM VITAE 141

LIST OF FIGURES

Figure 1.1: Illustration of some wireless scenarios where conventional cryptography-based security struggles 5
Figure 2.1: Illustration of different frequency reuse techniques for ICI avoidance. Reuse-1 scheme uses the whole spectrum in each cell, while reuse-3 splits the spectrum into three bands and different bands are used in neighboring cells. FFR and SFR split the cell into inner and outer regions, where the neighboring cells use different bands for the latter. 9
Figure 2.2: Illustration of CoMP schemes. CS/CB require exchange of channel and scheduling information amongst cooperating TPs. JT/DPS, on the other hand, also require sharing of user data to be transmitted. 10
Figure 2.3: Coverage map of Istanbul Çatalca region - Turkey for different throughput requirements obtained using Atoll radio planning tool. 11
Figure 2.4: Selected 5G/6G use cases, services and requirements. 12
Figure 2.5: GCoMP conceptual framework. User requirements, CoMP architecture, and scenario serve as inputs to the decision mechanism. The outputs of this mechanism include (but are not limited to) selection of CoMP scheme and coordinating cluster. ... 16
Figure 2.6: Example of a decision-making flowchart for generalized CoMP (GCoMP) 18
Figure 2.7: A sketch illustrating the tradeoff between latency, reliability, and throughput (inspired from [1]) 19
Figure 2.8: Effective CIR after (MSSNR) channel shortening is applied. The original CIR has a length of 8 taps, while the desired CIR length is 4 taps. 26
Figure 2.9: Types of physical layer security (PLS) threats in wireless network 31
Figure 2.10: Illustration of PLS conceptual framework 34
Figure 2.11: Difference in observed channel parameters such as CIR's amplitude (shown) and phase (not shown) can be used for link/device authentication. 37
Figure 2.12: Basic steps for wireless channel-based key generation 39
Figure 2.13: The radio frequency (RF) impairments serve as potential "fingerprints" for wireless nodes. 41
Figure 2.14: The physical parameters observed from the environment (such as distance or angle between the nodes) serve as the source of keys to be used for PLS. .. 42
Figure 2.15: The modulation order/scheme is modified according to channel information making it difficult for the eavesdropper to intercept and demodulate the signal. 46
Figure 2.16: Intentional misalignment of the received packets (sent from different antenna elements) at eavesdropper to degrade its interception capability. 49
Figure 2.17: An illustration of the emerging technological trends for beyond 5G network paradigms where PLS might prove critical. 52
Figure 3.1: An example of the generated network layout, cell boundaries following Voronoi tessellation. 68
Figure 3.2: An illustration of the considered hybrid network layout 68
Figure 3.3: Average pathloss and P(LoS) for the defined user locations is plotted as a function of the FBS altitude. Inset figure shows P(LoS) as function of θ for urban environment. 70
Figure 3.4: Illustration of the utilized system model 73
Figure 3.5: Illustration of the Tx/Rx block diagrams for the proposed method for two coordinating transmission points (TPs) (K = 2). Gray shaded blocks represent the additional stages compared to conventional orthogonal frequency division multiplexing (OFDM) 74

Figure 3.6: Illustration of the proposed approach in a relaying scenario. (a) A typical dual-hop relay aided system comprising a single source, relay and destination each. (b) The user signal is transmitted from source (S) at time $t0$, reaching the relay (R) and destination *(D)* at times *t1* and *t2,* respectively, while the jamming signal is transmitted by *D* at *t2* and reaches *R* at *t3.* 79
Figure 3.7: A simplified block diagram of the proposed approach 82
Figure 3.8: Illustration of the Doppler (angular) relations between transmitter and receiver in the presence of a reflector 83
Figure 3.9: The variance of error observed at the receiver for different SNRp values. (a) SNRp = 20dB, (b) SNRp = 30dB, (c) SNRp = 40dB, (d) SNRp = 50dB. 84
Figure 4.1: Performance comparison of different coordination schemes and clustering approaches when all applications (given in Table 3.2) are equiprobable. (a) Number of unconnected users, (b) Energy efficiency, (c) Average backhaul bandwidth required per TP. 90
Figure 4.2: Performance comparison of different coordination schemes and clustering approaches when 100% of the user equipments (UEs) use conversational video. (a) Number of unconnected users, (b) Energy efficiency, (c) Average backhaul bandwidth required per TP. 91
Figure 4.3: Performance comparison of different coordination schemes and clustering approaches when 100% of the UEs use vehicle-to-everything (V2X) messaging. (a) Number of unconnected users, (b) Energy efficiency, (c) Average backhaul bandwidth required per TP. 92
Figure 4.4: Large scale fading comparison between the primary terrestrial base station (TBS1) and flying base station (FBS). 94
Figure 4.5: SNR comparison between different user-base station links. User link with flying base station (UE-FBS) is shown in blue, link between user and first terrestrial base station (UE-TBS1) is shown in red while user and second terrestrial base station link is shown in cyan (UE-TBS2). 95
Figure 4.6: SNR comparison with and without MRC combining. Blue, red and cyan colors represent UE1, UE2 and UE3, respectively. The solid lines are the results for MRC combining of TBS1 and FBS, dotted lines are obtained after combining both TBS links while the dashed line represents SNR without any combining. 96
Figure 4.7: Performance comparison of the proposed approach with channel shortening [2], and baseline OFDM in terms of achievable capacity at Bob and Eve in normal, single TP-based channel shortening and proposed approaches. 97
Figure 4.8: Comparison of secrecy capacity between the proposed approach and [2].. 98
Figure 4.9: BER performance comparison of relay and destination. Relay's performance is seen to be degraded severely with the proposed CP jamming scheme.. 99
Figure 4.10: Effect of jamming power and cyclic prefix (CP) duration 100
Figure 4.11: Performance analysis of the proposed scheme. (a) key mismatch rate (KMR) between Alice and Bob as a function of signal-to-noise ratio (SNR) for different values of Δ. (b) KMR comparison between Bob and Eve as a function of ρ and Δ. (c) Secret key capacity for different values of L and Δ. 102
Figure 5.1: Challenges and future directions 106

LIST OF TABLES

Table 1.1: Summary of CoMP state-of-the-art categorized according to different 5G and beyond network requirements (CB = Coordinated Beamforming, CS = Coordinated Scheduling, DPS = Dynamic Point Selection, JD = Joint Detection, JP = Joint Processing, JT = Joint Transmission). 3
Table 2.1: Examples of existing PLS schemes categorized according to PLS's threats, countermeasures and definition 35
Table 3.1: Simulation parameters 67
Table 3.2: User/application priorities and requirements 67
Table 4.1: Simulation parameters for hybrid aerial-terrestrial network in support of uRLLC 103
Table 4.2: Simulation parameters and assumptions for spatially distributed channel shortening 103
Table 4.3: Simulation parameters and assumptions for CP jamming against eavesdropping relays in OFDM systems 104
Table 4.4: Proportion of sequences successful in NIST randomness tests 104

LIST OF SYMBOLS

$|.|$: Cardinality of a set
$(.)^T$: Transpose
Δf : Subcarrier spacing
$\boldsymbol{\lambda}$: Poisson point process (PPP) density
ρ : Correlation coefficient
$\boldsymbol{\sigma}$: Standard deviation
$\boldsymbol{\tau}$: Delay shift
Ω_i : *i*-th hypothesis (GCoMP)
Ω^* : Optimum hypothesis (GCoMP)
$\mathcal{A}$: Set of all UEs associated with a TP
B : Bandwidth
$\mathcal{B}$: Set of all TPs in the coverage area
d : Distance
f_c : Carrier frequency
h : Channel coefficient (time domain)
H : Channel coefficient (frequency domain)
$I(;)$: Mutual information between two random variables
$\mathcal{I}$: Imaginary part of a complex number
k : Integer Doppler shift index
κ : Fractional Doppler shift index
L : Number of channel taps
M : Number of subcarriers
$\mathcal{M}$: Set of muted TPs in the coverage area
N : Number of symbols
$\mathcal{N}()$: Gaussian distribution
N_0 : Noise PSD
P : Signal power
PL : Pathloss
R : Capacity of a link
$\mathcal{R}$: Real part of a complex number
T : Symbol duration
T_{cp} : CP duration
T_s : Sampling interval
$\mathcal{T}$: Set of transmitting TPs in the coverage area
$\mathcal{U}$: Set of all users in the coverage area
v : Velocity
υ : Doppler shift
x : Transmitted signal (time)
X : Transmitted signal (frequency)
y : Received signal (time)
Y : Received signal (frequency)

ABBREVIATIONS

3GPP : 3rd Generation Partnership Project
4G : fourth generation
5G : fifth generation
5QI : 5G QoS identifier
6G : sixth generation
AAF : amplify-and-forward
ABS : absolute blank subframe
AC : access category
AI : artificial intelligence
AoA : angle of arrival
AP : access point
APP : application
ARQ : automatic repeat request
ATSSS : access traffic steering, switching and splitting
AWGN : additive white Gaussian noise
BER : bit error rate
BS : base station
CA : coordination area
CB : coordinated beamforming
CBRS : Citizens Broadband Radio Service
CCI : co-channel interference
CFO : carrier frequency offset
CFR : channel frequency response
CIR : channel impulse response
C-JT : coherent JT
CLT : central limit theorem
CoMP : coordinated multipoint
CP : cyclic prefix
C-RAN : cloud RAN
CS : coordinated scheduling
CSF : channel shortening filter
CSI : channel state information
D2D : device-to-device
DC : dual-connectivity
DD : delay-Doppler
DL : downlink
DMT : discrete multi-tone
DNN : deep neural network
DoS : denial of service
DPS : dynamic point selection
eICIC : enhanced ICIC
ELPC : extremely low-power communication
eMBB : enhanced mobile broadband
eNB : eNodeB
ERLLC : extremely reliable and low-latency communication
eRNTP : enhanced RNTP
FBS : flying base station
FDD : frequency-division duplexing
FeMBB : further-enhanced mobile broadband

FFR : fractional frequency reuse
FFT : fast Fourier transform
FIR : finite impulse response
FTR : fluctuating two-ray
GBR : guaranteed bit-rate
GCoMP : generalized CoMP
HAPS : high altitude platform systems
HARQ : hybrid ARQ
HetNet : heterogeneous network
HII : high interference indicator
ICI : inter-carrier interference
ICIC : inter-cell interference coordination
i.i.d. : independent and identically distributed
IFFT : inverse fast Fourier transform
IoT : Internet of Things
IP : Internet protocol
IQI : in-phase/quadrature imbalance
ISFT : inverse symplectic Fourier transform
ISI : inter-symbol interference
IT : information technology
ITS : intelligent transportation system
JSC : joint sensing and communication
JT : joint transmission
KGR : key generation rate
KMR : key mismatch rate
LDHMC : long-distance and high-mobility communication
LDPC : low-density parity check
LED : light-emitting diode
LoS : line-of-sight
LPI : low probability of intercept
LTE : Long-Term Evolution
MAC : medium access control
MBB : make-before-break
MCC : mission-critical communication
MEC : mobile-edge computing
MIMO : multiple-input multiple-output
ML : machine learning
mMTC : massive machine-type communications
mmWave : millimeter wave
MPC : multipath component
MP-TCP : Multipath Transmission Control Protocol
MRC : maximum ratio combining
MSSNR : maximum shortening signal-to-noise ratio
NB-IoT : narrowband IoT
NC-JT : non-coherent JT
NIST : National Institute of Standards and Technology
NLoS : non-line-of-sight
NTN : non-terrestrial network
NWDP : N-wave with diffuse power
OFDM : orthogonal frequency division multiplexing

OI : overload indicator
OTFS : orthogonal time-frequency space
PAPR : peak-to-average power ratio
PDCP : packet data convergence protocol
PDF : probability distribution function
PEAC : phase enciphered Alamouti coding
PHY : physical
PLS : physical layer security
PMI : precoding matrix indicator
PPP : Poisson point process
PSD : power spectral density
QoE : quality of experience
QoS : quality of service
QPSK : Quadrature Phase Shift Keying
RB : resource block
REM : radio environment map
RF : radio frequency
RIS : reconfigurable intelligent surface
RNTP : relative narrowband transmission power
RRH : remote radio head
RRM : radio resource management
RSRP : reference signal received power
RSS : received signal strength
RSSI : received signal strength indicator
SFR : soft frequency reuse
SIMO : single-input multiple-output
SINR : signal-to-interference-plus-noise ratio
SISO : single-input single-output
SNR : signal-to-noise ratio
SON : self-organizing network
SPS : semi-persistent scheduling
SWIPT : simultaneous wireless information and power transfer
TBS : terrestrial base station
TDD : time-division duplexing
TDL : tapped delay line
TDoA : time difference of arrival
THz : terahertz
TN : terrestrial network
TP : transmission point
TRP : transmission-reception point
TWDP : two-wave with diffuse power
UAV : unmanned aerial vehicle
UE : user equipment
UL : uplink
umMTC : ultra-massive machine-type communication
UP : user priority
uRLLC : ultra-reliable low latency communication
V2I : vehicle-to-infrastructure
V2N : vehicle-to-network
V2P : vehicle-to-pedestrian

V2V : vehicle-to-vehicle
V2X : vehicle-to-everything
VLC : visible light communication
WSN : wireless sensor network
XAI : explainable AI
XR : extended reality
ZF : zero-forcing

GELECEK NESİL KABLOSUZ HABERLEŞME AĞLARINDA KOORDİNELİ ÇOK NOKTALI SİSTEMLER

ÖZET

Muhammad Sohaib Jamal Solaija

Elektrik-Elektronik Mühendisliği, Doktora

Tez Danışmanı: Prof. Dr. Hüseyin Arslan

Temmuz, 2023

Beşinci nesil (5G), ultra güvenilir, düşük gecikme ve masif makine tipi iletişim gibi hizmetlerin tanıtılmasıyla insanlardan ziyade nesnelerin bağlanabilirliğine vurgu yaparak kablosuz iletişim ağlarında bir paradigma değişiminin sinyalini verdi. Bu, enerji/spektral verimlilik, bağlantı, gecikme, güvenilirlik ve güvenlik vb. gibi yeni veya daha yüksek gereksinimlere ihtiyaç gerektirmektedir. Koordineli çoklu noktayı (Coordinated MultiPoint - CoMP), bunlardan bazılarını, özellikle de bağlantı gereksinimini gerçekleştirmenin potansiyel sağlayıcısı olarak görülmektedir. İlk olarak, geleneksel yerden-yere kanala kıyasla havadan-yere kanalın sinyal yayılım özelliklerindeki farktan yararlanarak güvenilirliği artırmak için hibrit hava-yer ağının kullanılması önerilmektedir. Özellikle, daha yüksek görüş hattı olasılığı, daha az gölgelenmesine ve daha yüksek alınan sinyal gücünün alınmasına yol açar. Hava ve karasal kanallarının uygun şekilde birleştirilmesi, gelişmiş sinyal kalitesi ve güvenilirliğini sağlar. Daha sonra, fiziksel katman güvenliği (Physical Layer Security - PLS) sağlamak için CoMP tarafından sunulan mekansal olarak dağıtılmış iletim noktalarından (Transmission Points - TPs) yararlanılır. Spesifik olarak, farklı TP'lerden bölünmüş ve iletilen kullanıcı verileri üzerinde bağlantıya özgü kanal kısaltma filtreleri kullanılır. Bu bölümleme, kulak misafiri olan kişinin, bağlantılardan biri üzerinden daha iyi yayılım deneyimlese bile bilgileri doğru şekilde yorumlayamamasını sağlamak için yapılır. Ayrıca, CoMP'un sınırlı spektrum, ana taşıyıcı bant genişliği ve enerji gibi ağ kısıtlamalarını göz önünde bulundurarak farklı kullanıcı ve uygulama gereksinimlerini destekleyebilen proaktif ve verimli bir kaynak yönetimi çerçevesi için CoMP'un genelleştirilmesi önerilmektedir. CoMP şemalarının (koordineli programlama, koordineli hüzme oluşturma, ortak iletim veya dinamik nokta seçimi) ve kümeleme yaklaşımlarının (dinamik veya statik) çeşitli kombinasyonlarının farklı koşullar altında kullanılabileceği gösterilmiştir.

PLS ile devam ederek, işbirlikçi iletişimlerde kimlik doğrulama ve güvenlik mekanizmalarının eksikliği vurgulanmaktadır. Sonrasında, işbirlikçi iletişimde güvenilmeyen rölelere karşı koruma sağlamaya yönelik bir yöntem de sunulmaktadır. Burada, orthogonal frekans bölmeli çoğullama sistemlerinde hızlı Fourier dönüşümünün varlığından yararlanılır. Spesifik olarak, hedef düğüm, döngüsel önek süresi boyunca, röledeki tüm alt taşıyıcılara yayılan ve müdahale kabiliyetini azaltan bir (bilinen) karıştırma sinyali iletir. Ayrıca, kablosuz kanalın gecikmeli Doppler gösteriminden yararlanıldığı, araç her şeye iletişimde frekans bölmeli dupleksleme için bir anahtar

oluşturma mekanizması sunulmaktadır. Son olarak tez, yalnızca mevcut yaklaşımları kapsamakla kalmayan, aynı zamanda yeni nesil PLS yöntemlerinin geliştirilmesini de sağlayan birleşik bir PLS çerçevesi sunmaktadır

Anahtar sözcükler: 5G, 6G, havadan/havaya iletişim, koordineli çoklu nokta (CoMP), kooperatif iletişim, döngüsel önek (CP), karıştırma, karasal olmayan ağlar (NTN), orthogonal frekans bölmeli çoğullama (OFDM), ortogonal zaman-frekans uzayı (OTFS), fiziksel katman güvenliği (PLS), karasal ağlar, araçtan her şeye (V2X).

COORDINATED MULTI-POINT SYSTEMS FOR FUTURE WIRELESS COMMUNICATION NETWORKS

ABSTRACT

Muhammad Sohaib Jamal Solaija

Ph.D. in Electrical, Electronics Engineering and Cyber Systems

Advisor: Prof. Dr. Hüseyin Arslan

July, 2023

The fifth generation signaled a paradigm shift in wireless communication networks by laying emphasis on the connectivity of *things* rather than people by the introduction of services such as ultra-reliable low latency communication and massive machine type communication. This led to new (or more stringent) requirements such as energy/spectral efficiency, connectivity, latency, reliability, security and so on. We look at coordinated multipoint (CoMP) as a potential enabler of fulfilling some of these, particularly the latter ones. First, the use of hybrid aerial-terrestrial network is proposed to improve reliability by exploiting the difference in signal propagation characteristics of the air-to-ground channel compared to the conventional ground-to-ground one. In particular, the higher line-of-sight probability leads to reduced shadowing and higher received signal strength. Proper combining of the aerial and terrestrial segments leads to improved signal quality and reliability. Later, the spatially distributed transmission points (TPs) offered by CoMP are leveraged to provide physical layer security (PLS). Specifically, link-specific channel shortening filters are employed on user data which has been split and transmitted from different TPs. The splitting is done to ensure that the eavesdropper cannot interpret information properly even if it experiences better propagation over one of the links. Moreover, the generalization of CoMP to a proactive and efficient resource management framework capable of supporting different user and application requirements while considering network constraints such as limited spectrum, backhaul bandwidth and energy, is proposed. It is shown that various combinations of CoMP schemes (coordinated scheduling, coordinated beamforming, coherent/non-coherent joint transmission, or dynamic point selection) and clustering approaches (dynamic or static) can be utilized under different circumstances.

Continuing further with PLS, the lack of authentication and security mechanisms in cooperative communications is highlighted. Then, a method for providing protection against untrusted relays in cooperative communication is also presented. Here, the presence of fast Fourier transform in orthogonal frequency division multiplexing systems is exploited. Specifically, the destination node transmits a (known) jamming signal during its cyclic prefix (CP) duration which spreads to all subcarriers at the relay reducing its interception capability. Furthermore, a key generation mechanism for frequency-division duplexing vehicle-to-everything communication is presented where the delay-Doppler representation of the wireless channel is leveraged. Finally, the thesis presents a unified

PLS framework which not only encompasses the existing approaches but also enables the development of next-generation PLS methods.

Keywords: 5G, 6G, aerial/airborne communication, coordinated multipoint (CoMP), cooperative communication, cyclic prefix (CP), jamming, non-terrestrial networks (NTNs), orthogonal frequency division multiplexing (OFDM), orthogonal time-frequency space (OTFS), physical layer security (PLS), terrestrial networks, vehicle-to-everything (V2X).

CHAPTER 1

1. INTRODUCTION

The fifth generation (5G) of cellular networks signaled a paradigm shift in wireless communications. Rather than focusing on increasing the data rates, it emphasized diversifying the supported applications and use cases. While 5G catered to the enhancement of data rates under the enhanced mobile broadband (eMBB) service, it also expanded its vision to incorporate the increasing number of wireless devices and stringent reliability and latency requirements under the massive machine type communication (mMTC) and ultra-reliable low latency communication (uRLLC) services, respectively [3]. This diversity of applications is expected to increase even further in sixth generation (6G), with more stringent requirements of throughput, latency, reliability, energy and spectral efficiency, security, and so on [4].

This diversity is evident not only in the applications and services, but also in the enabling technologies for future wireless networks. For instance, 5G tried to address the different requirements by introducing the concept of numerologies [5], [6]; the lack of available spectrum has led to research regarding spectrum sharing and utilization of higher frequency bands such as millimeter wave (mmWave) [7], visible light communication (VLC) [8] and terahertz (THz) communication [9]; furthermore, the diversity of network infrastructure itself is expected to increase with the incorporation of non-terrestrial networks [10] and reconfigurable intelligent surface (RIS)-aided smart radio environments [11].

The incorporation of these new paradigms, along with the increased heterogeneity of the device capabilities and operating conditions of the network introduces two main challenges (amongst various others). These are (i) the lack of a cohesive/coordinated network and (ii) the inability to ensure security and privacy, particularly for low-end user devices.

Consequently, in this thesis, we look at two main concepts, i.e., CoMP and PLS as their respective solutions.

1.1. Coordinated Multipoint (CoMP)

CoMP was introduced in Long-Term Evolution (LTE) Rel-11, where the goal was to improve the quality of service (QoS) experienced by cell edge user equipments (UEs). Since LTE focused on increasing the data rates and/or spectral efficiency of the network, CoMP was also limited to interference mitigation and throughput/capacity improvement [12]–[22]. However, the expansion of industry verticals and use cases promised by 5G has signaled renewed interest in CoMP. This is primarily due to a metamorphosis of the mentality behind CoMP, where instead of limiting it to multiplexing gains for capacity enhancement, methods are being developed to leverage diversity for reliability and other requirements [23].

The reemergence of CoMP is illustrated by multitude of works in literature targeted at addressing the diverse requirements of 5G and beyond networks such as mobility management [24]–[29], reliability and latency [30]–[34], energy efficiency [35]–[41], and security [42]–[44]. **Table 1.1** summarizes the state-of-the-art work leveraging CoMP principles used to address the aforementioned user requirements. Inspired by these works, we propose generalization of CoMP as a potential flexibility enabler for the next generation wireless networks.

1.1.1. Thesis contributions under CoMP

- Although CoMP systems were primarily proposed to improve the cell edge performance in 4G, their collaborative nature can be leveraged to support the diverse requirements and enabling technologies of 5G and beyond networks. To this end, we propose the generalization of CoMP to a proactive and efficient resource management framework capable of supporting different user requirements such as reliability, latency, throughput, and security while considering network constraints in [45]. This work elaborates on the multiple aspects, inputs, and outputs of the generalized CoMP (GCoMP) framework. Apart from user requirements, the GCoMP decision mechanism also considers the CoMP scenario and network architecture to decide

Table 1.1: Summary of CoMP state-of-the-art categorized according to different 5G and beyond network requirements (CB = Coordinated Beamforming, CS = Coordinated Scheduling, DPS = Dynamic Point Selection, JD = Joint Detection, JP = Joint Processing, JT = Joint Transmission).

Requirement	Contribution/Goal	CoMP Scheme
Throughput/ Data Rates	Conduction of field trials to validate performance of CoMP.	JD [12], [13], CS, JT [12]
	Scheduling and frequency reuse schemes are extended to CoMP environment.	CS [14], JT [15]
	Comparison of different coordination schemes amongst themselves and with non-CoMP transmission.	CS [16], CB [16], [18], JT [16]–[18]
	CoMP performance in HetNets is discussed [19]–[21] and stochastic geometry-based analysis is carried out [22].	JP [19], CB [20] JT [21], [22]
Mobility Support	Soft handover using CoMP.	JT [24], [25]
	Frequent handover mitigation using CoMP.	CB, JT [26]
	Scheduling mechanisms to support mobile users.	CS [27]
	Performance comparison of different handover algorithms in a CoMP setting.	DPS [28]
	Proactive network association [29].	-
Reliability and Latency	Spatial/macrodiversity is utilized to enhance reliability of the communication.	JT [30]–[32], DPS [31], [32]
	Clustering is done considering uRLLC requirements as constraints [33].	-
	Resource allocation is done in a multi-cell network in a coordinated manner.	CS, JT [34]
Energy Efficiency	Clustering is carried out with the goal of improving energy efficiency.	JT [35], [36]
	Selective activation of TPs to reduce energy consumption.	JT [37] DPS [38], [39]
	Wireless power transfer [40] and energy harvesting [41]	JT [40] JP [41]
Security	Directional modulation against eavesdropping.	JT [42]
	Signal misalignment at the eavesdropper by leveraging multiple TPs.	JT [43]
	Beamforming to ensure signal strength/quality at legitimate user only.	CB [44]

upon outputs such as CoMP scheme or appropriate coordinating clusters. To enable easier understanding of the concept, a case study illustrating the effect of different combinations of GCoMP framework's outputs on varying user requirements is presented.

- uRLLC is undoubtedly the toughest service class in 5G-NR from the network service provider's perspective. Different methodologies have been utilized to meet the reliability and latency requirements of uRLLC including proposition of various diversity techniques. The work in [46] envisages a hybrid network using terrestrial and flying base stations to provide ubiquitous and reliable service to uRLLC users. We propose utilizing the macro-diversity in the hybrid environment by exploiting the significant differences in path loss and shadowing characteristics of flying base stations (FBSs) as compared to the terrestrial base stations (TBSs). Preliminary results are presented to this effect and recommendations are made to their inclusion in the networks for supporting uRLLC users in the future.

- Cryptography has been conventionally used to tackle communication security, but it may not be scalable (in terms of key exchange and management) with the increasingly heterogeneous network deployments. PLS provides a promising alternative but struggles when an attacker boasts a better wireless channel as compared to the legitimate user. In [47], a spatially distributed channel shortening approach is leveraged to address this problem. Specifically, the user data is split into multiple parts, where each part is sent using a different transmission point. This ensures that at least one of the illegitimate links experiences worse propagation channel as compared to the legitimate one. Additionally, a channel shortening filter is applied w.r.t legitimate links, which results in inter-symbol interference being introduced at the receiver. Results show significant enhancement of the achievable secrecy capacity as compared to state-of-the-art channel shortening-based PLS methods.

1.2. Physical Layer Security (PLS)

Wireless communication has pervaded all aspects of human existence. The recent pandemic has further cemented its importance, with different facets of our daily lives including (but not limited to) education, retail, banking, healthcare all depending heavily on reliable wireless communication for their continuity despite the challenging restrictions worldwide [48]. While this ubiquitous availability of wireless signals is desirable from a communication (and sensing) perspective, it is becoming increasingly challenging to ensure the privacy of confidential data and information when it is being transmitted openly into the environment [49]. This broadcast nature of wireless communication renders it susceptible to threats such as eavesdropping, jamming, and spoofing. In eavesdropping, the attacker tries to intercept and interpret the ongoing communication between legitimate nodes. In jamming, the attacker's target is to disrupt the communication, while in spoofing, the attacker impersonates a legitimate node for malicious purposes [50].

The conventional security paradigm, i.e., *cryptography* does not scale well enough to address the diversity in applications, devices, and network deployment scenarios. As illustrated in **Figure 1.1**, this is due to the following reasons: firstly, cryptographic security depends on the computational complexity of the key-breaking which is rendered a naive assumption with the advent of quantum computing [51]; secondly, in applications such

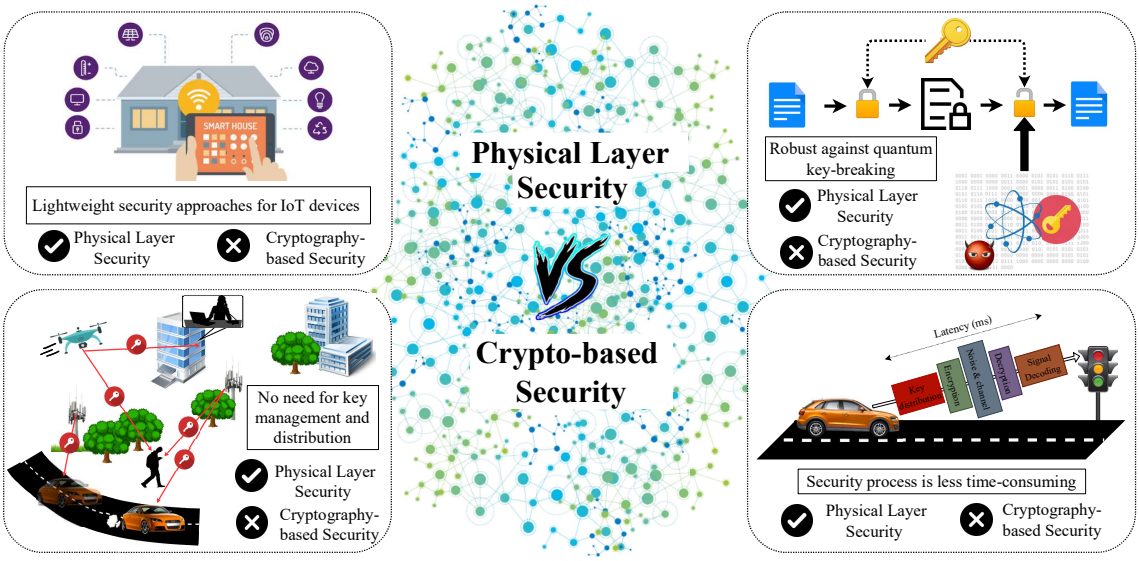

Figure 1.1: Illustration of some wireless scenarios where conventional cryptography-based security struggles.

as Internet of things (IoT)/mMTC the terminal devices are constrained in terms of power and other computational resources necessitating simple and lightweight security mechanisms [52]; thirdly, the high-mobility applications such as high-speed trains, vehicle-to-everything (V2X) communications and non-terrestrial networks (NTNs) manifesting in a continuously changing network topology require renewed key management and authentication procedures [53]; and lastly, for uRLLC/extremely reliable and low-latency communication (ERLLC) applications, latency is a critical issue and conventional cryptographic methods might be too time-consuming to be practical [54]. The next-generation network, therefore, necessitates a new approach that could complement (if not replace) cryptography. PLS is arguably the most compelling candidate; it addresses the quantum threat by providing various alternatives where the security is ensured by providing better link quality for legitimate nodes compared to the illegitimate links [55]; unlike cryptography, which requires computational capabilities at both computing nodes, PLS also supports *asymmetrical* security mechanisms where the processing may be kept on the base station (BS)/access point (AP) side, rendering it suitable for IoT terminals [56]; PLS also simplifies the key management by allowing communicating nodes to extract keys from the channel observed between themselves, eliminating the need for secure key exchange [57]; moreover, since key exchange and encryption/decryption are not necessary, PLS boasts reduced latency compared to cryptographic approaches [58]. Consequently, we have made the following contributions to the PLS literature in this thesis:

1.2.1. Thesis contributions under PLS

- Cooperative communication has been widely used to provide spatial diversity benefits for low-end user equipments, especially in ad hoc and wireless sensor networks. However, the lack of strong authentication mechanisms in these networks leaves them prone to eavesdropping relays. In [59], we propose a secure orthogonal frequency division multiplexing (OFDM) transmission scheme, where the destination node transmits a jamming signal over the cyclic prefix (CP) duration of the received signal. Simulation results verify that as long as at least a part of the jamming signal falls to the actual data portion of the eavesdropping relay, it spreads through all the data symbols due to the fast Fourier transform (FFT) operation, resulting in degraded interception at the eavesdropper.

- Key generation for secure communication is challenging in high-mobility scenarios due to the low coherence time. This is further exacerbated in frequency-division duplex systems due to the non-reciprocal wireless channel in uplink and downlink. Our work [60] leverages the symplectic Fourier transform to convert fast-varying time-frequency domain signals to slow-varying delay-Doppler (DD) domain and utilizes the wireless channel representation in the DD domain to generate shared keys. The proposed approach is evaluated in terms of key generation and mismatch rates considering correlated eavesdropper, as well as the various randomness criteria provided by National Institute of Standards and Technology (NIST).

- Despite the plethora of literary works regarding different facets of PLS being present, a unified framework is still absent. In the paper [61], we provide a PLS framework that not only encompasses the existing works but also enables the development of next-generation PLS methods. In line with this, the importance of PLS for emerging technologies such as joint sensing and communication, vehicular communication, non-terrestrial networks, millimeter-wave, terahertz communication, etc. is highlighted. Furthermore, the key challenges and directions for future PLS mechanisms are identified.

CHAPTER 2

2. THEORETICAL PART

In this chapter, we first (in **Section 2.1**) talk about the generalized CoMP (GCoMP) framework. More specifically, the background of coordinated multipoint (CoMP) and its evolution through different 3rd Generation Partnership Project (3GPP) releases is discussed, followed by a review of the literature where CoMP is leveraged for various requirements. Eventually, we present the GCoMP framework along with a description of its inputs and outputs. **Section 2.2** presents the concept of using a coordinated hybrid terrestrial/aerial network to improve the reliability of the network, targeted at supporting ultra-reliable low latency communication (uRLLC) applications by leveraging macrodiversity. **Section 2.3** provides yet another representative case study of CoMP, where the spatially distributed transmission points (TPs) are leveraged to improve the privacy of communication.

Continuing in the same vein, **Section 2.4** provides a physical layer security (PLS) mechanism to combat eavesdroppping relays by leveraging the properties of orthogonal frequency division multiplexing (OFDM) and fast Fourier transform (FFT), while **Section 2.5** discusses the challenge of secure and reciprocal key generation in frequency-division duplexing (FDD) systems before presented an orthogonal time-frequency space (OTFS)-based solution. Finally, the chapter concludes by presenting a unified framework for PLS in **Section 2.6**.

2.1. Generalized CoMP (GCoMP) Framework

2.1.1. Evolution of CoMP

Wireless communication systems have always been hindered by co-channel interference (CCI), particularly at cell edges. This section describes how the CCI problem ignited the

need for coordination in cellular networks leading to the emergence of techniques like inter-cell interference coordination (ICIC), enhanced ICIC (eICIC), and finally CoMP. Towards the end of this section, we highlight fifth generation (5G) enhancements related to CoMP or coordinated networks in general.

Earlier generations of cellular systems increased the frequency reuse distance [62] to mitigate or reduce the CCI experienced by cell edge users. Different reuse mechanisms such as integer frequency reuse (e.g. reuse-3 and reuse-7) [63], fractional frequency reuse (FFR) and soft frequency reuse (SFR) [64] are illustrated in **Figure 2.1**. In general, these mechanisms restrict the resource utilization in the spectral domain to reduce CCI. Despite their simplicity, the aforementioned mechanisms are hampered by their static and standalone nature since there is no provision for the TPs to coordinate with each other. This led to the emergence of the ICIC concept in 3GPP Rel-8, allowing the TPs to allocate transmission resources in a coordinated manner by leveraging different flags, namely relative narrowband transmission power (RNTP), high interference indicator (HII) and overload indicator (OI) [64]. These flags indicate if the interference power on certain resource blocks (RBs) is expected (or measured) to be high, allowing neighbor TPs to schedule resources accordingly. However, even this method fails to control CCI in heterogeneous networks (HetNets) due to the power disparity of TPs. eICIC was, therefore, introduced in 3GPP Rel-10. eICIC also considers time dimension to ensure orthogonal resource allocation in the form of absolute blank subframes (ABSs), where the macro TPs are muted to allow interference-free transmission for micro/femto TPs [65].

The increase in device density, combined with elevated heterogeneity of wireless infrastructure compounded the CCI problem. This necessitated more sophisticated and dynamic coordination approaches. Consequently, CoMP was introduced in the Rel-11 of 3GPP as a mechanism to allow different TPs connected with ideal backhaul to coordinate with each other [66]. CoMP introduces spatial domain to the resource allocation problem, thereby improving spectral efficiency in addition to interference mitigation. **Figure 2.2** illustrates the different CoMP schemes, including coordinated scheduling (CS), coordinated beamforming (CB), joint transmission (JT) and dynamic point selection (DPS). The concept was extended to multiple eNodeBs (eNBs) connected with non-ideal backhaul in Rel-12 [67]. This required the standardization of signaling over X2 interface to enable exchange of *CoMP hypothesis set* and its associated *benefit metric*, including reference

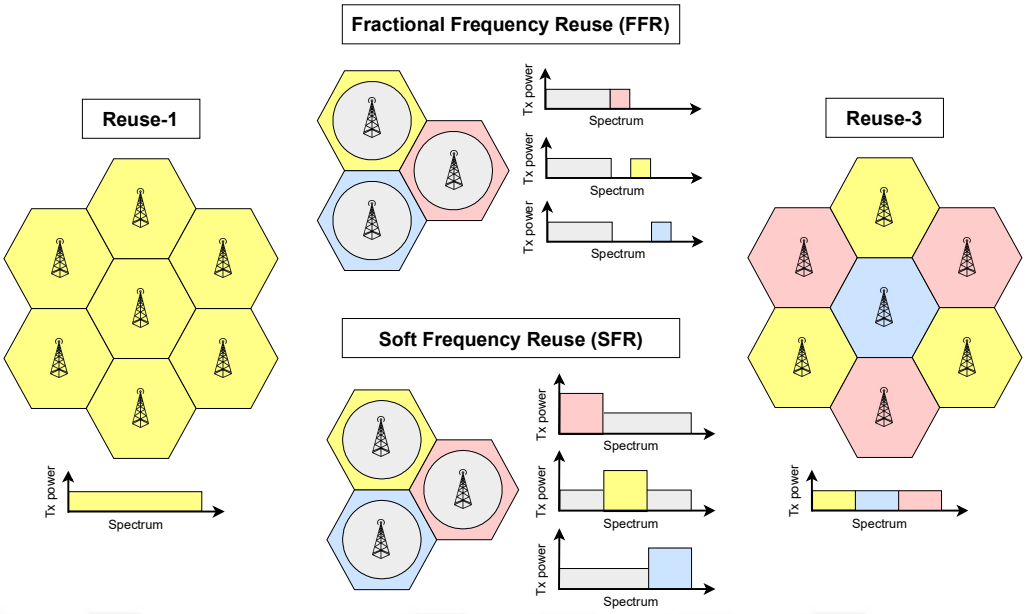

Figure 2.1: Illustration of different frequency reuse techniques for ICI avoidance. Reuse-1 scheme uses the whole spectrum in each cell, while reuse-3 splits the spectrum into three bands and different bands are used in neighboring cells. FFR and SFR split the cell into inner and outer regions, where the neighboring cells use different bands for the latter.

signal received power (RSRP) measurements, between cooperating eNBs. The sharing of this information amongst the coordination cluster helps improve the radio resource management (RRM) [68]. 3GPP Rel-13 provided some enhancements regarding channel state information (CSI) and enhanced RNTP (eRNTP), where the latter is particularly useful for power allocation in a CoMP setting [69]. Rel-14 looked at alternatives to JT due to its stringent synchronization and CSI requirements, leading to discussion around non-coherent JT (NC-JT). The performance results indicated the suitability of NC-JT and CS/CB in low and high traffic load scenarios, respectively [70]. Rel-15 proposed monitoring X2 characteristics and the spatio-temporal traffic variation to update or manage CoMP sets under the self-organizing network (SON) umbrella.

Having revisited the motivation and evolution of ICIC/CoMP, we now turn our attention towards the multitude of technologies introduced to fulfill the myriad of requirements imposed by 5G and beyond networks. Here we try to identify and highlight the paradigms that are relevant to CoMP and have already been discussed in the 3GPP standardization activities:

- *Functionality split between central and distributed units:* 3GPP Rel-14 specifies eight different functionality splits between central and distributed units for 5G [71].

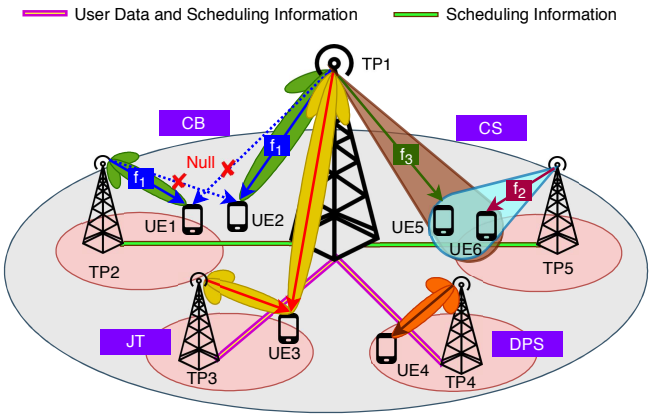

Figure 2.2: Illustration of CoMP schemes. CS/CB require exchange of channel and scheduling information amongst cooperating TPs. JT/DPS, on the other hand, also require sharing of user data to be transmitted.

The functionality split has a major impact on the backhaul and can potentially relax the corresponding requirements regarding overall capacity, delay, and synchronization. This is also applicable to the concept of cloud-RAN (C-RAN) which is a potential implementation of CoMP network. However, a study showing the feasibility of lower split options illustrates the preference of standardization in this regard [72].

- *Non-uniform application coverage:* 5G introduced a variety of services with different requirements, that are expected to further diversify in succeeding generations. Given the current network infrastructure, these applications have different coverage areas. **Figure 2.3** shows the preliminary simulation of coverage areas for different throughput requirements. For a user equipment (UE) at the edge of its application's coverage area, it is similar to being at a cell edge. Since CoMP was introduced to improve quality of service (QoS) at cell edges, the same concept can be extended to support the diverse user requirements of next generation of wireless networks.

- *mmWave and beyond:* The spectrum scarcity issue in sub-6 GHz frequencies and the envisioned extremely high data rate requirements in the future networks have led to the exploration of higher frequency bands (millimeter wave (mmWave), terahertz (THz), and visible light communication (VLC)). However, they are susceptible to higher path loss and blockages. The exploitation of macrodiversity offered by CoMP has been experimentally shown to provide link and capacity improvement in the 73 GHz band [73].

- *MIMO enhancements:* mmWave networks depend on technologies such as

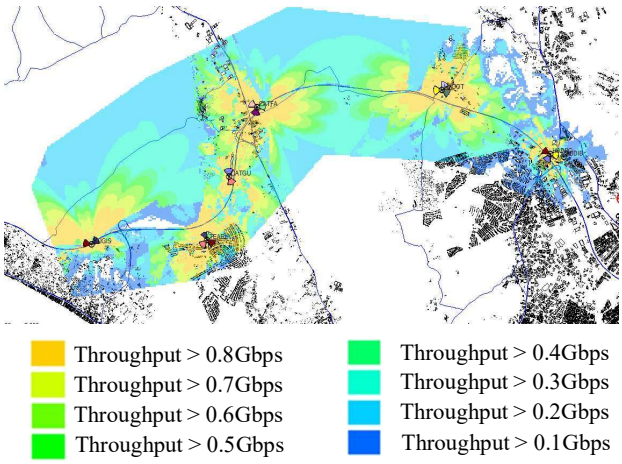

Figure 2.3: Coverage map of Istanbul Çatalca Region - Turkey for different throughput requirements obtained using Atoll radio planning tool.

multiple-input multiple-output (MIMO) and beamforming for their reliable operation. Accordingly, 5G and 3GPP Rel-16 have offered significant MIMO enhancements over Long-Term Evolution (LTE), including multi-panel/transmission-reception point (TRP) operation, which is similar in essence to the CoMP concept. Furthermore, improved (type II) codebook, flexible CSI acquisition and reference signal design (including zero-power signals for interference measurement), and beam management for higher (> 6GHz) bands promise significant boost in MIMO performance [74].

- *Coexistence and convergence of wireless networks:* In a trend which is expected to continue in sixth generation (6G), 5G has tried to incorporate unlicensed spectrum in its fold for improved network capacity, as evident from the presence of work item in Rel-17 [75], [76]. In fact, access traffic steering, switching and splitting (ATSSS) enables the simultaneous use of 3GPP (5G) and non-3GPP (Wi-Fi) access networks with the 3GPP-based core network [77]. Coordination between these networks can enable more efficient resource utilization in the unlicensed and/or shared spectrum.

2.1.2. CoMP for 5G and Beyond Requirements

As mentioned earlier, fourth generation (4G) focused on achieving higher data rates and improved spectral efficiency. Consequently, CoMP was also targeted towards the same goals. However, 5G introduced diverse applications such as uRLLC and massive machine type communication (mMTC) opening up CoMP to leverage its spatial diversity

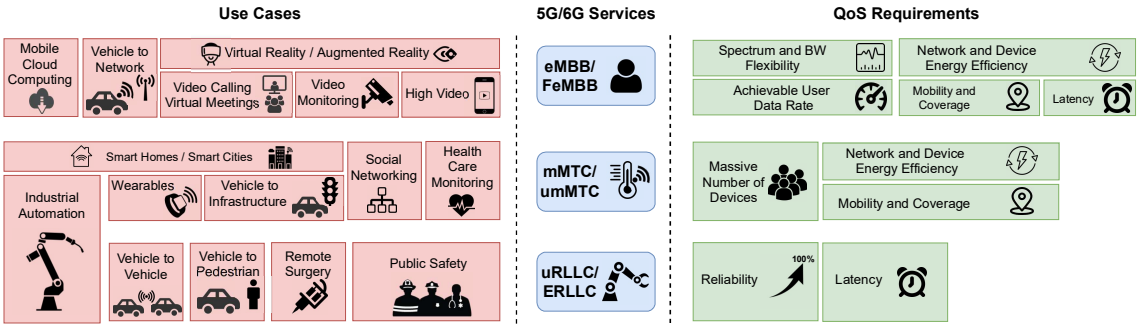

Figure 2.4: Selected 5G/6G use cases, services and requirements

for various other requirements [23]. 6G aims to expand the communication paradigms envisioned by 5G even further, providing the concept of a human-centric digital society that encompasses the various aspects of human life including healthcare, transportation, immersive entertainment, education, financial transactions, agriculture, and industrial automation. Compared to 5G, 6G envisions a 50-100 times increase in data rates and about three times increase in spectral efficiency under further-enhanced mobile broadband (FeMBB), 5-10 fold decrease in latency under extremely reliable and low-latency communication (ERLLC), support of twice the mobility speeds under long-distance and high-mobility communication (LDHMC), ten times higher device connectivity under ultra-massive machine-type communication (umMTC), and 10-100 fold increase in energy efficiency under extremely low-power communication (ELPC) [4], [78]. In addition to the extension of these 5G services, 6G will also open up new paradigms of which security is arguably the most important [79]. **Figure 2.4** illustrates the services and concerning requirements for some selected use cases discussed under 5G/6G visions. The remainder of this section describes some selected works to highlight different approaches used under the context of coordinated networks for the fulfillment of these requirements.

2.1.2.1. Mobility

To ensure continuous connectivity, dual connectivity based solution was considered (though not eventually standardized) in addition to *Make-Before-Break (MBB)* handover technique [80]. CoMP or C-RAN provide a possible realization of multi-connectivity. Additionally, CoMP also reduces the number of handovers as long as the UE is within its coordinating cluster. A CoMP scheme like DPS seems particularly suitable for mobile UEs, owing to the similarity in nature of handover and DPS concepts since both revolve

around the dynamic selection of best suited TP. Along the same lines, the switching aspect of ATSSS is capable of supporting smoother handovers by leveraging Multipath Transmission Control Protocol (MP-TCP) [81].

2.1.2.2. Reliability and Latency

Out of the different services of 5G and beyond networks, uRLLC or ERLLC (in 6G) presents arguably the toughest challenge owing to the targeted reliability with strict latency bounds. There are generally two approaches to address the uRLLC requirements, increasing the reliability of one-shot transmission or lowering the latency between retransmissions. CoMP, with its JT approach, can provide different versions of the transmitted signal at the receiver at the same time reducing the necessity of retransmission and addressing the latency constraint. Properly combining the received copies of the signal can improve the signal-to-interference-plus-noise ratio (SINR) performance and hence the reliability of the system. Macrodiversty is an approach to provide multiple paths for the communication of the same signal, targeted to exploit the variation of path loss and large scale fading in the different paths. An interesting idea related to this is to utilize hybrid aerial-terrestrial networks, which provide additional diversity in the wireless link owing to the different propagation characteristics of the air-to-ground channels [46]. In these networks, the aerial TPs provide a much higher probability of line of sight and reduced shadowing, resulting in improved reliability of communication. An alternative to this is the packet duplication approach supported in Rel-15 [82] which is a higher (packet data convergence protocol (PDCP)) layer complement of the physical (PHY) layer diversity techniques [83].

2.1.2.3. Energy Efficiency

Energy efficient operation is imperative for future wireless networks. There are two aspects of it; firstly, the energy usage needs to be minimized for devices/sensors that are not easily accessible, medical implants being a perfect example; secondly, the overall energy consumption of the network needs to be managed so that the increasingly dense deployments are feasible. In the first case, if there are multiple communicating devices, it is possible to consider DPS with energy conservation as a goal. A similar idea in drone-based disaster recovery scenario is proposed in [84] where the uplink TP is selected from

the UEs while taking into consideration their remaining battery lives. On the other hand, energy harvesting using simultaneous wireless information and power transfer (SWIPT) and TP sleeping are the two prevalent approaches for the second case. For SWIPT, coordinated beamforming can be optimized to provide both minimum SINR and required power transfer to the information and energy receivers, respectively [40]. TP sleeping, while beneficial from an energy conservation perspective, can lead to increased handovers. To cater to this situation, a simple uplink CoMP scheme is devised in [41] where the UE transmits to two cooperating nodes in a heterogeneous network. Another approach for facilitating the TP sleeping is dynamic clustering [36], since static clustering might not be able to support UEs if the network is loaded or the UE distribution is changing.

2.1.2.4. Security

PLS has attained increasing importance in wireless networks due to its ability to secure the link/signal rather than just the data. This is particularly useful for applications such as wireless sensing. However, an overwhelming majority of PLS mechanisms rely on independent channel observations at legitimate and illegitimate nodes. This may not be realistic for mmWave bands and poor scattering environments. In such cases, the spatial diversity offered by coordinating TPs can be exploited to attain multiple/different channel and device fingerprint observations [49]. For instance, in [42] TPs transmit the signal such that data is only decodable at the intersection of their transmission beams providing location-based security against eavesdropping. CoMP has also been utilized for security in underwater communication by ensuring that the signal components sent from different TPs collide at the eavesdropper while remaining collision-free at the intended receiver. This is achieved by controlling the transmission schedule and power [43]. Power control with coordinated beamforming has also been exploited to provide service-based security [44].

Unlike eavesdropping, where the aim of the attacker is to intercept and/or interpret the legitimate communication, jamming is targeted at disrupting the communication. This is generally achieved by the transmission of noise or noise-like signals to reduce the SINR experienced by the legitimate receiver. The spatial diversity offered by the geographically separated TPs may be utilized to combat such attacks.

2.1.2.5. Throughput

As mentioned earlier, the spatial diversity offered by CoMP systems is exploited in various ways. JT-CoMP promises significant gains in terms of network capacity and UE throughput by combining signals from different TPs either coherently or non-coherently. Coherent JT is capable of providing higher throughput as compared to its non-coherent counterpart since it uses a joint precoding procedure while the latter focuses on improving the received signal strength [85]. Multi-TRP MIMO utilizing beamforming at mmWave bands also promises increased data rates. Furthermore, this requirement can leverage the MP-TCP and underlying ATSSS concept to split the traffic over multiple access networks, resulting in improved throughput for the user [77].

2.1.3. GCoMP Framework

Given how the CoMP principle has been utilized to address different requirements of 5G networks, we believe that the scope of CoMP should be widened from mere interference mitigation to intelligent network resource management, helping satisfy these diverse requirements. This section is dedicated to the description of the conceptual GCoMP framework, illustrated in **Figure 2.5**. The first group of elements represents the inputs to the GCoMP decision mechanism. The decision making is the intermediate stage, followed by the outputs at the end. Here, it should be noted that while most options in the inputs/outputs are well-established, we have taken the liberty of identifying some additional ones, shown in red, that are either related to beyond 5G vision or at least recent to CoMP.

2.1.3.1. Inputs

The input elements include UE requirements, CoMP architecture, and scenario. The requirements are considered first since everything that follows revolves around them. Section **Subsection 2.1.2** has extensively discussed the usage of CoMP for different requirements such as throughput, security, reliability, mobility, and energy efficiency.

Following requirements, the second input considered is the architecture. The conventional categories include centralized or distributed coordination. In the former, all administrative tasks are controlled through a central unit, while in the latter, one of the cooperating TPs acts as a master cell and performs all resource management and communication tasks.

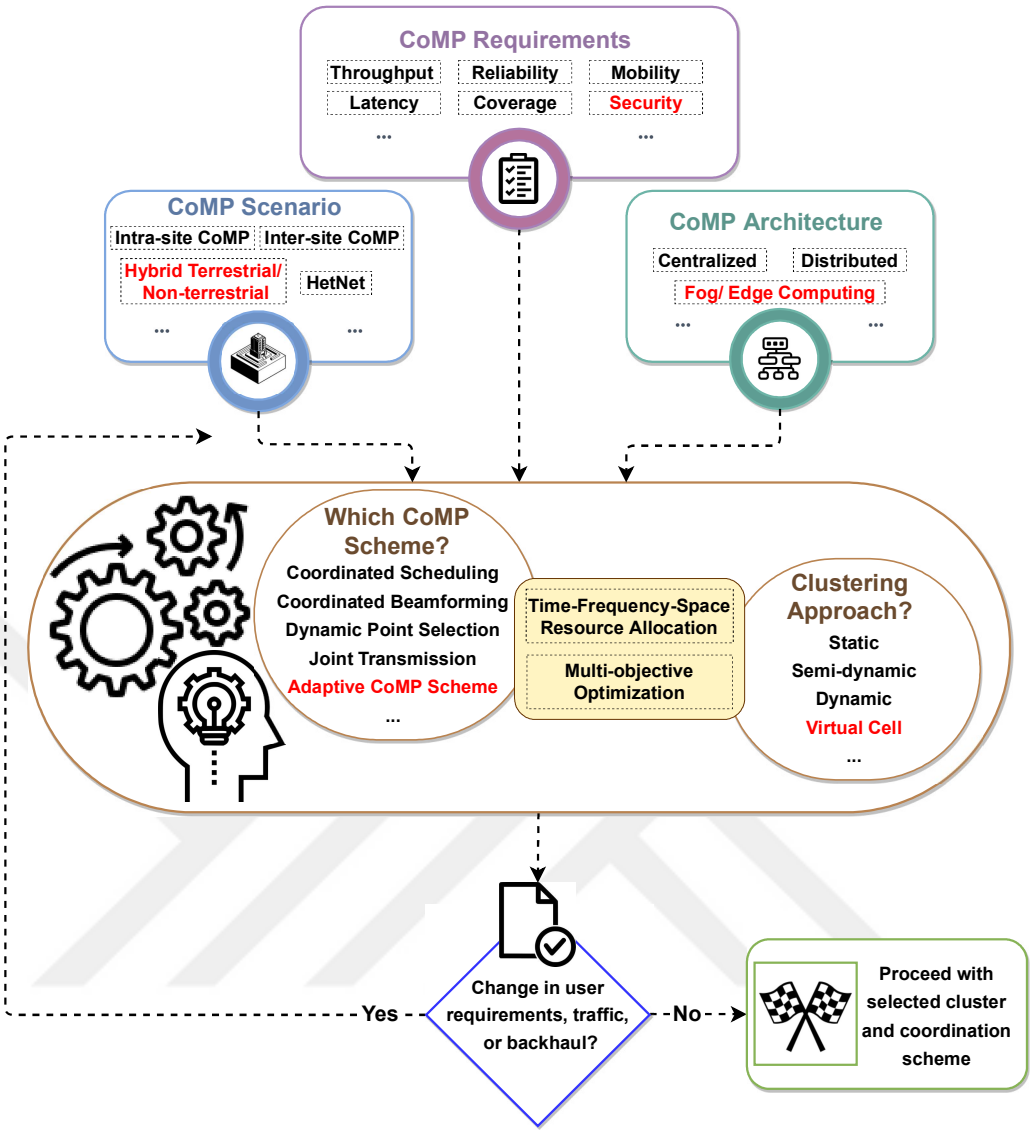

Figure 2.5: GCoMP conceptual framework. User requirements, CoMP architecture, and scenario serve as inputs to the decision mechanism. The outputs of this mechanism include (but are not limited to) selection of CoMP scheme and coordinating cluster.

Here it is pertinent to mention the concept of centralized or C-RAN, which has gained significant traction with operators due to its promise of reduced capital and operating expenditures. Despite its promise, one major challenge for C-RAN is to balance the tradeoff between easier network management offered by centralized control and the increasingly strict backhaul bandwidth and latency requirements. This might be critical for use cases like vehicle-to-everything (V2X) communication. In light of this, recent works have proposed the utilization of fog/edge computing to provide intelligence to components of the network close to the UE [86], [87].

The third input element is CoMP scenarios. 3GPP proposed three different CoMP scenarios for both homogeneous and HetNets [66]. The first scenario is homogeneous intra-site CoMP, in which the coordination takes place between different TPs (sectors). Due to the colocation, there is no additional load on the backhaul. The second scenario is inter-site CoMP which is also implemented on a homogeneous network. It uses high power remote radio heads (RRHs) to expand the coverage. The third scenario is implemented on HetNets and utilizes low power RRHs. Inter-site CoMP and HetNet scenarios require high-speed backhaul links, like fiber, to make the connection between the macrocells and their respective RRHs. In line with HetNets, another scenario that may be of interest is hybrid aerial-terrestrial networks. The wireless propagation channel characteristics of the air-to-ground channel are fairly different as compared to the conventional terrestrial channel, providing a better QoS to the UEs [46]. This can be extended to incorporate the non-terrestrial network or satellite communication scenarios, aimed at improving network coverage [88]. The logical next step to exploiting the variation in the propagation environment is the capability of modifying the environment itself to improve the coverage and user experience. reconfigurable intelligent surface (RIS) is a technology that promises exactly that by selectively modifying the incident signal's properties, such as phase, amplitude, and polarization [89].

Here it is important to categorize the nature of the above-mentioned inputs in terms of their dynamicity. While the architecture is primarily static, the scenario might change due to paradigms like TP sleeping and dynamic deployment of non-terrestrial network entities. UE requirements (unless a device is specialized for a particular application) are expected to change on an even finer timescale, depending on the particular application/service being used.

2.1.3.2. Decision Making

The GCoMP decision making evaluates the above-mentioned input elements, network constraints, and channel conditions to make informed decisions regarding the appropriate resource allocation, namely, selection of the best suited CoMP scheme and coordination cluster. **Figure 2.6** illustrates an exemplary decision making process [90], which starts by identification of the goal/utility function and corresponding constraints. Common examples of utility functions include fairness [91], throughput [92], or combination of the

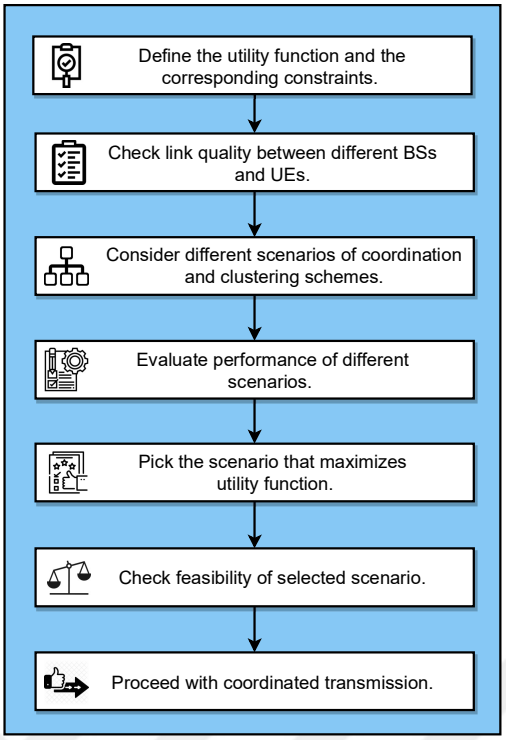

Figure 2.6: Example of a decision making flowchart for GCoMP

two [93], [94]. Generally, in a network comprising of N TPs the goal is to maximize this function over all TPs, which takes the form $F(B_1, B_2, ..., B_N)$, where B_k refers to the k-th TP. This function is commonly assumed to have properties such as, i) F is additive for the coordinating TPs, i.e. $F(B_1, ..., B_N) = \sum_{k=1}^{N} F(B_k)$ and ii) if the TP does not serve any UEs, $F(B_k) = 0$ [95]. The typical constraints, on the other hand, include transmission power [96], available spectral resources [97], and the provisioned backhaul bandwidth [98].

Here, it should be highlighted that there are cases such as uRLLC, where the goals (reliability, latency, throughput) are often competing. As illustrated in **Figure 2.7**, it is possible to optimize any two of the requirements at the cost of the third [1]. This is visible for point A where reliability and latency are optimized, but throughput is compromised. Point B, on the other hand, provides the opposite. In such scenarios, a single optimum solution is not possible. Rather, there is a set of (possibly infinite) Pareto-optimal solutions where improving one objective would lead to degradation in the other(s) [99].

Apart from the aforementioned utility functions and constraints, another factor that needs to be considered is the priority of the users. In the case of wireless standards, priority levels are defined to ensure the necessary QoS for different applications. For instance, in

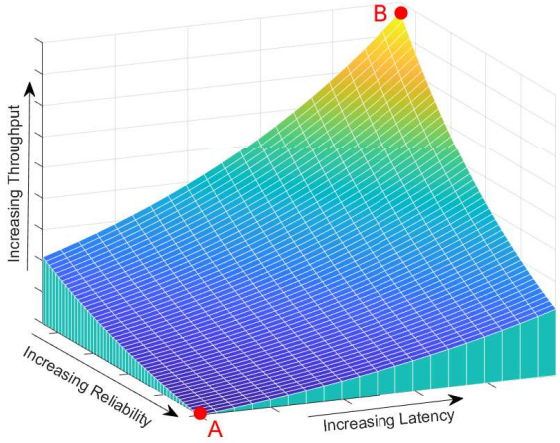

Figure 2.7: A sketch illustrating the tradeoff between latency, reliability and throughput (inspired from [1])

5G these levels are indicated by 5G QoS identifier (5QI) [100]; and in the case of Wi-Fi, user priority (UP) or access category (AC) fields serve a similar purpose [101]. The examples of link quality metrics include SINR, RSRP, received signal strength indicator (RSSI), distance etc. The link quality helps identify coordination clusters which are used to evaluate the performance of different coordination schemes. The combination of clustering mechanism and coordination scheme which maximizes the utility function is then assessed by

$$\Omega^* = \underset{\Omega_i \in \{\Omega_1,\ldots,\Omega_x\}}{\arg\max} \sum_{k=1}^{N} F(B_k)|_{\Omega_i}, \tag{2.1}$$

where Ω^* and Ω_i refer to the optimum and i-th hypotheses, respectively. As long as the constraints mentioned earlier are fulfilled, Ω^* is chosen and the coordinated transmission can be carried out.

In general, the approaches for the decision making process are categorized into *user-centric*, *network-centric*, or *hybrid*. The user-centric approach makes decisions on a per-user basis, targeted at fulfilling that particular UE's requirements. The network-centric decision making, on the other hand, places more emphasis on simplifying the implementation from the network perspective, including the architecture and overhead while trying to optimize the performance of all connected UEs. The overhead includes information (data and CSI) sharing between the nodes and processing of the information necessary for the said decision making. The hybrid approach provides a tradeoff between both the above-mentioned methods by optimizing the decisions for a group of UEs while keeping the

network overhead bearable. The decision to pick any of these approaches itself presents a challenge. One way to address this is to consider the historical user behavior and preferences in a given network. For networks with more consistent user behavior and application requirements, a network-centric approach is more appropriate. In the case of significantly varying user preferences, user-centric decisions have to be used despite their considerable overhead. In the case that users have similar requirements and preferences, they are grouped and facilitated under the hybrid approach. Moreover, since these decisions are dependent upon variable parameters such as UE requirements and spatio-temporal traffic patterns, they need dynamic updates. These updates can either be *periodic* or *triggered*. As the name suggests, the former analyzes the network situation repeatedly after a fixed interval and revisits its earlier decisions, making it suitable for scenarios where the circumstances are expected to change constantly. The triggered updates, on the other hand, are set off by certain conditions. This approach is, therefore, suitable for cases where sporadic variation in the backhaul availability or traffic patterns is expected.

2.1.3.3. Outputs

The first output of the framework is the selection of the appropriate CoMP scheme, which are illustrated in **Figure 2.2**. CS reduces interference by ensuring instantaneous exchange of channel information between coordinating TPs. In the following section, we consider a special case of CS (CS with muting), where apart from the serving TP, all other TPs are muted on the corresponding allocated RBs for a scheduled user. CB allows the edge UEs to use the same frequency resources as long as the beam patterns for different UEs do not interfere with each other. Due to the significant use of beamforming in 5G networks, CB has attained increased importance. JT, arguably the most interesting CoMP technique, constitutes of UE data being transmitted from different TPs, potentially providing macro-diversity against path loss, shadowing, and blockage. Since coherent JT (C-JT) performs joint beamforming, it requires backhaul links with high capacity and low latency as well as strict synchronization among coordinated TPs. NC-JT, on the other hand, provides a complexity-performance tradeoff by removing the burden of joint precoding and strict synchronization while still providing significant gains as compared to other schemes [70]. DPS is a special case of JT, where even though the UE data is available at different TPs,

it is only transmitted from one TP at any given time [85]. All these schemes have different backhaul requirements and provide varying benefits. Therefore, the GCoMP decision needs to consider both, UE's requirements and the available backhaul bandwidth before making a decision. An interesting approach pertaining to the latter consideration is presented in [102], where the system adaptively switches between the CS/CB and JT CoMP schemes depending on the backhaul availability.

The second output identified for this framework is the decision about the coordination cluster, which comprises of the TPs that are supposed to coordinate with each other. In literature, there are three main types of clustering. *Static* clustering, which is primarily based on topology and does not vary according to the nodes or UEs, thereby providing limited performance gains. *Semi-dynamic* clustering - an enhanced version of the former - where more than one static clustering patterns are set up and UEs can select the most suitable cluster, leads to an increase in both complexity and performance. *Dynamic* clustering responds to network and UE mobility changes and reduces inter-cluster interference by updating the clusters dynamically [103]. To identify the coordinated TPs per cluster, a set of solutions is proposed in [104] taking into account real operating conditions such as connectivity and network layout. One of the solutions is to adapt the coordination areas (CAs) depending on the spatial distribution of the UEs in order to avoid concentrations of UEs on inter-CA borders. Another solution is the use of layered CAs where the borders between adjacent CAs are covered by an overlaying CA. Indeed, a coordinated TP can be part of different CAs and partitioning of scheduler resources between the CAs is needed which might cause some peak UE throughput limitations. Therefore, CA layers should be activated only when needed. In addition to the clustering approach, there is the concept of virtual cell [86], where each virtual cell is occupied by a single UE. This UE is served by multiple cooperating TPs leveraging different logical slices of the network.

2.2. CoMP For Reliability

As highlighted in **Subsection 2.1.2.2**, uRLLC is undoubtedly the toughest 5G service to support with stringent latency and reliability requirements. In near future numerous industrial control, traffic safety, remote surgery, autonomous vehicle and drone-based delivery, and internet services will depend on wireless connectivity with guaranteed consistent

latencies between $1 - 15$ms and exceedingly stringent reliability requirements between $99.9 - 99.9999\%$, depending on the particular application [105]. The difficulty in achieving these targets primarily stems from fundamental trade-offs among reliability, latency and throughput which renders maximizing all of them simultaneously impossible [1]. Different methodologies have been proposed in literature over the last few years to find a suitable solution, but the continuous research going on indicates that we are still far from achieving the set goals for this particular service of 5G communications.

As the name uRLLC suggests, reliability and latency are the two critical criteria of this service. Therefore, it is logical that the techniques aim towards improving reliability or reducing latency, since doing both simultaneously is unlikely. As far as the latency reduction is concerned, 5G facilitates it by allowing the use of mini-slots and introduction of multiple numerologies in NR [106]. The use of grant-free transmission in uplink (UL) communication is also targeted to reduce the latency incurred by the scheduling request and its associated feedback in grant-based scheduling. However, this comes at the cost of increased collisions. For this different hybrid automatic repeat request (HARQ) based retransmission schemes are present in literature like *Reactive*, *K-repetition* and *Proactive*. All of these are discussed in [107] and their performance is compared to the traditional grant-based methodology. In addition to grant-based and grant-free schemes, semi-persistent scheduling (SPS) [108] has also been considered which is essentially a hybrid between the two, i.e., a TP can periodically allocate the resources to the users after an initial scheduling request.

For reliability improvement, link adaptation in terms of selecting optimum modulation and coding is discussed in [109]. Increasing diversity helps improve the reliability of a communication link, interface diversity for uRLLC is considered in [110] to achieve the required latency and reliability targets. Network densification might be considered as a technique to help with both latency and reliability enhancement, since increased number of TP would shorten the association distance, provide more resources to the users and possibly allow multiple associations [111]. Dual-connectivity (DC) is being touted as the technique that would primarily be used in the initial implementation of 5G for its co-existence with LTE networks. Dynamic packet duplication in DC architecture can be used to support uRLLC. DC-based solution is also considered for handovers in uRLLC

in addition to *MBB*, *RACH-less* (for synchronized network), *2 Tx/Rx MBB* handover techniques [80]. CoMP and its implementation in the form of C-RAN can be the driving force behind multi-connectivity. Different levels of functionality splits under C-RAN architecture are analyzed for uRLLC provision in [112]. C-RAN is also considered in [113], where a low-complexity centralized cell selection and scheduling algorithm for uRLLC users is proposed. Use of unmanned aerial vehicles (UAVs) for uRLLC is investigated in [114], results showing that a single link is not enough to provide the required reliability for urban environment.

Considering these efforts, it is clear that uRLLC requirements still remain a huge challenge and fulfilling them requires major research and effort. Motivated from that, in this paper, we propose macrodiversity scheme considering a terrestrial and aerial hybrid network for ensuring ubiquitous and reliable service to uRLLC users.

2.3. CoMP For Physical Layer Security (PLS)

As highlighted in **Subsection 2.1.2.4**, CoMP can be leveraged to provide PLS to wireless links, an example of which is provided here. This is based on a rather interesting approach to combat eavesdropping given in [2], which utilizes channel shortening to induce inter-symbol interference (ISI) at the illegitimate receiver, Eve. Channel shortening filters (CSFs) have been conventionally used in multicarrier systems such as OFDM and discrete multi-tone (DMT) to shorten the delay spread of the channel such that it is less than cyclic prefix (CP) in length [115]. In [2], this CSF is designed considering the channel between legitimate transmitter (Alice) and legitimate receiver (Bob). As a result, the channel impulse response (CIR) experienced on this link is shortened, allowing the legitimate devices to use shorter CPs. For Eve, on the other hand, the convolution of CSF with original CIR leads to even longer effective CIR, causing ISI which, in turn, deteriorates Eve's interception capability. However, in the case that Eve is closer to Alice compared to Bob (and consequently has a shorter maximum excess delay), the shortening approach fails. This shortcoming is addressed in the current work by exploiting the spatially distributed TPs afforded by approaches such as CoMP or multi-connectivity.

CoMP, originally introduced for interference mitigation, has been leveraged to satisfy various other communication requirements including PLS against eavesdropping [45]. The

authors in [42], [116] utilize CoMP to address the limitation of directional modulation, while [43] uses coordinated scheduling and power allocation of transmission from distributed antenna elements in an underwater communication scenario to provide security. A dynamic CoMP scheme is proposed in [117] to enhance secured coverage. CoMP is also being used in UAV systems to achieve secrecy [118], where multiple ground nodes cooperatively detect the legitimate information sent from the UAV to enhance the legitimate user's performance in eavesdropper's presence.

In this work, a spatially distributed implementation of channel shortening-based PLS is provided. This helps mitigate the limitation of the existing shortening-based PLS [2] mentioned above. The performance is evaluated in terms of achievable secrecy capacity for both approaches, showing the gains of the proposed approach over existing scheme. However, before going into the specifics of the proposed approach, we would like to provide a brief recap of the channel shortening concept itself.

2.3.1. Overview of Channel Shortening

Multicarrier systems have attained increasing popularity due to their ability to convert frequency-selective fading channels into flat-fading (which allows simpler frequency domain equalization) by dividing the transmission band into smaller bands or subcarriers [119]. This capability has led to the adoption of OFDM and DMT in various cellular, WiFi, and audio/video broadcast standards. However, the advantages of multicarrier schemes can only be realized as long as they allow for a CP or guard duration longer than the delay spread of the multipath channel. If the CP is not sufficiently long, it leads to a loss of orthogonality of the subcarriers resulting in inter-carrier interference (ICI) and ISI. This motivated the design of finite impulse response filters, also referred to as CSFs, that shorten the CIR experienced by a wireless link such that it is less than the duration of the CP [120].

One of the most popular approaches for CSF design, referred to as maximum shortening signal-to-noise ratio (MSSNR), was proposed by Melsa *et al.* [115]. The CSF in MSSNR tries to maximize the ratio of the energy in desired CIR window, $\boldsymbol{h}_{\text{win}}$, of the effective channel to the energy outside this window, in $\boldsymbol{h}_{\text{wall}}$. The energy in both cases can be expressed as

$$\boldsymbol{h}_{\text{win}}^{T}\boldsymbol{h}_{\text{win}} = \boldsymbol{w}^{T}\boldsymbol{A}\boldsymbol{w}, \tag{2.2}$$

$$\boldsymbol{h}_{\text{wall}}^{T}\boldsymbol{h}_{\text{wall}} = \boldsymbol{w}^{T}\boldsymbol{B}\boldsymbol{w}, \tag{2.3}$$

where $\boldsymbol{A}$ and $\boldsymbol{B}$ are symmetric and positive semidefinite matrices, $(.)^{T}$ shows transpose operation, and $\boldsymbol{w}$ represents optimal shortening as long as it satisfies the constraint $\boldsymbol{w}^{T}\boldsymbol{A}\boldsymbol{w} = 1$, while minimizing $\boldsymbol{w}^{T}\boldsymbol{B}\boldsymbol{w}$. The resultant effective channel is then the convolution of the original CIR with CSF (or multiplication in the frequency domain), which can be written as

$$h^{\text{eff}}(n) = h(n) * w(n), \tag{2.4}$$

where $h(n)$ refers to original CIR and $w(n)$ is the CSF. **Figure 2.8** provides an illustration of how the CSF shortens the desired CIR. In this figure, the original CIRs for both, Bob and Eve are assumed to have length, $L = 8$ while the desired CIR length is set as 4. Since it is designed to increase the shortening signal-to-noise ratio (SNR) for Bob only, the effective channels for Bob and Eve differ significantly. It can be seen that the CIR for Bob after shortening is indeed limited to 4 taps (near zero values after that). On the other hand, for Eve a significant amount of energy lies outside the original CIR length, shown as the shaded rectangle, which is exploited in the form of ISI to degrade its decoding capability. It should be noted that the CSF block is part of the transmitter, therefore, received signals at both Bob and Eve pass through the same shortening filter.

2.4. Secure Communication In The Presence Of Eavesdropping Relays

MIMO is considered to be an essential enabler for 5G (and even Wi-Fi) and beyond wireless networks [121]. However, services such as mMTC and Internet of things (IoT) cannot always ensure the availability of hardware capabilities that can support MIMO operation. This led to the emergence of *cooperative communication* paradigm around the turn of the century, where the aim is to improve the QoS of the users through cooperation. Cooperative communication, while generally applicable to different network realizations, is more suited to *ad hoc* and wireless sensor networks (WSNs) compared to the cellular systems [122]. Unlike the latter, the former two systems lack a sophisticated authentication mechanism. This may lead to violation of a user's data confidentiality by the very nodes that are expected to improve the communication via spatial diversity. Accordingly, there exists a plethora of approaches for PLS in cooperative communication, which can

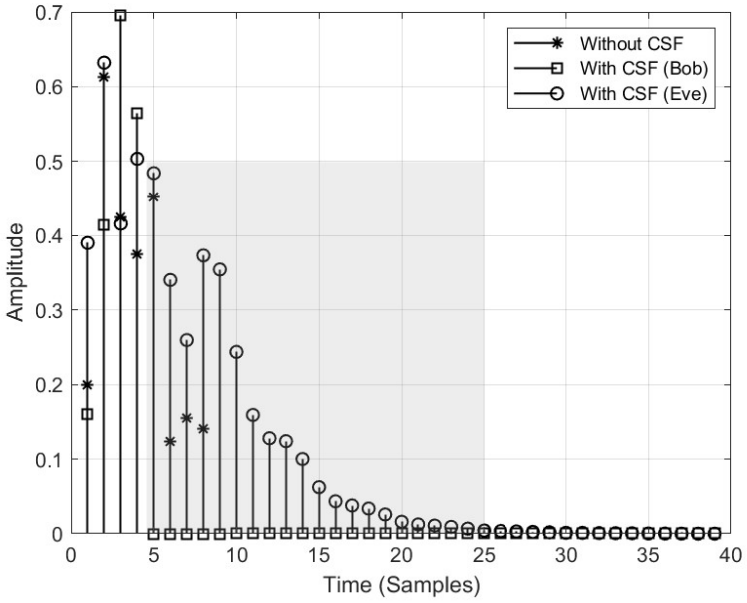

Figure 2.8: Effective CIR after (MSSNR) channel shortening is applied. Original CIR has a length of 8 taps, while the desired CIR length is 4 taps.

be broadly categorized into *cooperative relaying*, *cooperative jamming* and their hybrid combinations. Both these approaches usually comprise of two phases, where the first one is broadcast of information from the source. In the second step, the appropriate relay forwards the message to the destination. In the case of relaying, the selection of the helper (relay) is done to degrade the eavesdropper's interception capability. In the case of jamming, the source itself, the destination, or any other helper node transmits noise-like signals such that the eavesdropper cannot hear the message [123].

Despite the clear advantage in terms of degraded eavesdropping capability [124], the cooperative jamming techniques have various limitations. For instance, in the case of friendly jamming the presence of a trustable node is necessary [125]. Furthermore, the jamming signal from this helper can also degrade the destination's performance. Destination-based jamming techniques resolve this issue by exploiting their prior knowledge of the jamming signal. However, they require full-duplexing capabilities to achieve spatial diversity [126]. In both cases, jamming signals are to be transmitted throughout the first phase (where the source broadcasts the signal) of cooperative communication, which is unsuitable for power-limited devices. To this end, we propose the design of a jamming signal which is only transmitted for part of the broadcast phase, yet its effect is spread throughout the signal duration by exploiting the properties of OFDM signals and FFT operation.

Since the jamming signal is only transmitted during the CP part at the destination, it also eliminates the need for full-duplexing capability.

2.5. Delay-Doppler Based Key Generation In V2X Communication

Key generation from the legitimate wireless link has been widely studied and exploited to encrypt or modify the transmitted signal. A critical limitation in this regard, however, is the need for reciprocity of the channel parameters used for key generation. This condition is only satisfied in time-division duplexing (TDD) systems. While TDD systems have become increasingly popular recently, they inherently incur latency which can be hazardous in certain mission-critical, low-latency applications such as V2X communication. This latency is cut in half in FDD systems that are also used for narrowband IoT (NB-IoT) by 3GPP standardization. In FDD, the users experience different small and large-scale fading due to their dependence on frequency and the fact that uplink and downlink channels are separated by more than coherence bandwidth. Hence, the generation/extraction of matching keys in these systems is quite challenging.

Most of the key generation work in FDD systems involves estimation of the combined (uplink and downlink) channel using some feedback mechanism between the communicating nodes such as pilot loopback [127], combined channel frequency response (CFR) [128] and precoding matrix indicator (PMI) [129]. An alternative is to use frequency-invariant channel parameters such as delay [130] or angle [131]. The former considers a device-to-device (D2D) scenario where the time-varying distance (or propagation delay) is used for key generation. In [131], angle of arrival (AoA) in both elevation and azimuth dimensions is used to generate the key. The angle-based approach is extended to an UAV MIMO system in [132], where the three-dimensional spatial angle between the legitimate nodes is used to generate the key. The eigenvalue reciprocity of the channel's covariance matrix is used in [133], while a reciprocal channel is constructed in [134], which is then used to generate keys.

Amongst the aforementioned works, the combined channel-based approaches suffer from extra latency incurred due to the feedback process. On the other hand, the angle-based methods require a high number of antennas at the communicating nodes. Moreover, the

covariance matrix-based technique offers low key generation rate (KGR) [135]. Therefore, it is necessary to devise novel mechanisms capable of providing reciprocal keys in FDD systems. In line with this, we look to leverage OTFS transmission, which has been recently popularized for high-mobility scenarios, for PLS. Presently, the secrecy performance of OTFS-based transmissions has been studied for uplink satellite [136] and unicast services [137]. The former considers an eavesdropping satellite and a cooperative UAV jammer, while the latter analyzes the impact of the eavesdropper's mobility on secrecy. A channel-based pre-rotation is proposed in [138] which leads to constellation distortion at the eavesdropper. Channel-dependent seed is employed in [139] to generate a Gosudarstvennyi standard-based sequence which is then used to perturb the OTFS modulation and secure the transmission. However, none of these works utilize the delay/Doppler channel representation as the source of shared secret sequence, which is addressed in this work in the following manner:

- This is the first work that uses the delay/Doppler indices of the wireless link between legitimate transceivers to generate the shared private sequences (referred to as "key" henceforth). Since high-speed scenarios are susceptible to fast variation of the channel, an FDD system is considered and OTFS transmission is employed to convert the fast-varying channel to slow-varying in the delay-Doppler (DD) domain. Moreover, the realistic case of integer delay and fractional Doppler shifts is considered, since it is implausible to have long frame duration in systems with low coherence time.

- It is analytically shown how distinct Doppler shifts are encountered at the legitimate receiver versus eavesdropper as a function of the node velocities and angles between the transmitter, receiver, and environmental reflectors. In conjunction with the integer delay and Doppler shifts, the fractional Doppler shifts are used to generate the keys via quantization.

- To provide further insights, the proposed approach is evaluated in terms of KGR, key mismatch rate (KMR), and secret key capacity as a function of the quantization levels and channel correlation. Moreover, the randomness of generated key bits is assessed in light of the statistical test suite provided by National Institute of Standards and Technology (NIST).

2.6. Unified PLS Framework

PLS is not necessarily a new topic. In fact, there is a plethora of academic works. Readers are referred to `https://www.comsoc.org/publications/best-readings/physical-layer-security` for a list of selected readings on PLS that look at the different facets of PLS ranging from information-theoretic foundations to its practical implementation. That said, till now there is no unanimous definition for PLS or an accompanying framework that encompasses the different approaches developed. Accordingly, in this work we contribute the following to the PLS literature:

- Keeping in view the myriads of mission-critical applications expected in 5G and beyond networks, wireless security is a non-negotiable requirement. Even though PLS has primarily been studied to secure communication, it applies to any wireless technology application including sensing. Accordingly, in this work, we provide a generalized framework for PLS that is relevant for all wireless systems.
- We split the PLS fabric into *observation* and *modification* planes and provide a novel manner of categorizing the existing (and future) PLS mechanisms depending on how they leverage the physical properties of the wireless signal and/or radio environment to secure the wireless link(s).
- The different *domains* of PLS are discussed under the modification and observation plane concepts, enabling a vision of future PLS mechanisms for next-generation wireless systems.
- The importance of PLS in paradigms such as non-terrestrial networks (NTNs), uRLLC, IoT, V2X, THz, and joint sensing and communication (JSC) is highlighted, followed by identification of the associated technical challenges.

2.6.1. Overview of Wireless Security Threats

Wireless systems enjoy a uniquely important place in our daily lives. While their ubiquitous presence simplifies countless tasks, the broadcast nature of wireless

transmissions poses inherent security risks, some of which are illustrated in **Figure 2.9**. In this section, we briefly describe the primary motivations behind various attacks before providing some examples from real networks.

2.6.1.1. Classification of Attacks

The preliminary goal of PLS approaches is to make use of the properties of the PHY layer such as randomness of wireless channel and uniqueness of radio frequency (RF) fingerprints to address all the security requirements in wireless systems. These requirements are represented by the CIAA quartet (confidentiality, integrity, authenticity, and availability), fulfillment of which characterizes a secure and reliable communication system. In the following text, we will look at each requirement one by one along with the possible attacks that target them.

Confidentiality is arguably the first requirement that pops into one's head when thinking about communication security. A confidential system aims to limit the disclosure of information only to the legitimate receiver while preventing its interception by malicious entities [140]. The violation of confidentiality, referred to as an *eavesdropping* attack, results in the attacker being able to obtain and decode the secret data/signal content [55]. Conventionally, data encryption is the most commonly used technique for masking important and sensitive contents (where the encryption key may be shared or extracted from the wireless channel). In this case, an eavesdropper might be able to intercept the transmitted signal but cannot obtain any critical information from it [141].

Authentication ensures correct identification of the communicating nodes while integrity ensures that the message/data is not tampered with by the malicious attacker(s). A *spoofer*, on the other hand, attempts message injection, false reporting, data modification, and so on. A man-in-the-middle attack, for instance, is an attack against the integrity of information where, as the name implies, the attacker sits between the communicating nodes and manipulates the transmitted data [142]. To mitigate any inconvenience of such kind, the communicating nodes first perform mutual authentication (i.e., initial handshake) before establishing a communication link for data transmission using unique identities such as medium access control (MAC) and Internet protocol (IP) addresses. This step is to confirm that

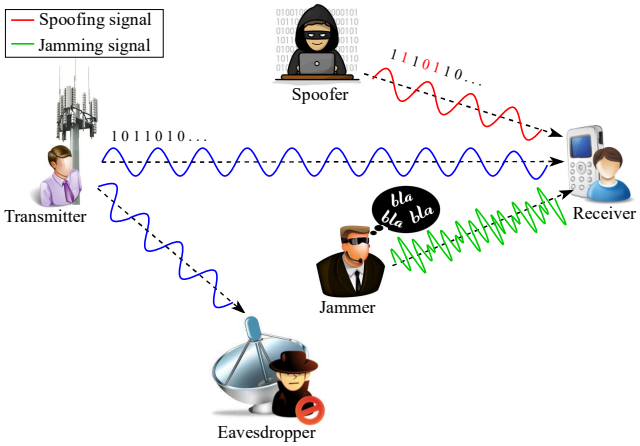

Figure 2.9: Types of PLS threats in wireless network.

the communication request comes from the authorized nodes, distinguishing them from other nodes. It is evident that authenticity and integrity can be fulfilled simultaneously. For the sake of node authentication at the PHY layer, hardware [143], channel [144], and tag-based authentication [145] methods are employed.

Even if the transmitted data is kept confidential and its integrity and node authenticity maintained, it is often useless unless the authorized nodes are capable of accessing a wireless network anytime and anywhere upon request. The violation of availability, referred to as denial of service (DoS), will result in the authorized nodes being unable to access the wireless network, which in turn results in an unsatisfactory user experience. More specifically, a malicious node may launch DoS attack at the PHY layer by generating interference signals for disrupting the desired communication, which is also known as a *jamming* attack. This type of attack is segregated into proactive and reactive attacks [146]. A proactive jamming attacker transmits a jamming signal irrespective of the legitimate data transmission. As opposed to the proactive jamming attack, the reactive jammer starts jamming only over non-idle channels. To mitigate these attacks and ensure availability, we can use redundant communication links that become available when the primary link has been disrupted. Spread spectrum techniques are also used to combat jamming attacks by spreading the signal's energy over time and frequency domains [147].

2.6.1.2. Examples of Real-World Attacks

To enable better understanding for the readers, we provide some examples of security breaches in real-world communication systems. These attacks typically involve low-end IoT terminals normally seen in smart city paradigms such as smart homes, transportation, and grids. Here it should be reiterated that conventional cryptographic approaches are relatively complex and, therefore, ill-suited to such applications.

Intelligent transportation systems (ITSs) envision the integration of sensing, control, analysis, and communication technologies into travel infrastructure and transportation to improve mobility, comfort, safety, and efficiency. As such, they rely heavily on secure V2X communication to ensure their smooth operation. However, malicious adversaries can disrupt their safety functions by injecting false measurements to compromise the security of drivers and pedestrians. In the case of obstacle/object detection, the falsified data might result in drivers making incorrect and unsafe decisions leading to collisions [148]. When launched on a larger scale, these attacks can cause multiple accidents, delays, and traffic jams. If combined with any disaster, it could even hamper the movement and performance of disaster-relief teams, leading to increased casualties.

Besides, the smart grid, which is basically the next generation of power electric system, relies on robust communication networks to provide efficient, secure, and reliable power delivery. Thus, network security is of critical importance in the smart grid. A set of attacks on the smart grid is investigated in [149], ranging from direct load shifting to meter data manipulation. Specifically, at a smaller scale, the adversaries can control certain IoT devices, such as home appliances, in the smart grid and induce an abnormal working state in these devices, e.g., increasing the power consumption. In terms of large-scale attacks, aggressive adversaries can compromise many high-wattage IoT devices to manipulate the power demand in a larger smart grid. The work in [150] demonstrates a large-scale attack model on real-world grids, using a botnet to turn on and off a large number of IoT devices synchronously, resulting in massive power fluctuations with the potential to cause a large-scale blackout.

In addition to the active attacks described above, smart home appliances such as IP cameras, smart motion sensors/speakers, and other IoT devices tend to have access to significant amounts of personal data through various user accounts as well as real-time spatial or positional information, which may be the target of passive eavesdropping attacks. An adversary may learn a user's behavioral patterns as well as their credentials for different accounts. With such information, the adversary can then apply the password dictionary in a brute-force attack to guess the password and compromise the system. This has been demonstrated in a real-world case of IP camera identity leakage [151].

2.6.3. Physical Layer Security Framework: Definition and Domains

The basic idea of PLS is providing unbreakable, provable, and quantifiable secrecy from an information-theoretical point of view [140]. This is generally thought to be achieved through the intrinsic characteristics of the wireless channel such as fading, interference, and multipath propagation [50], [152], [153]. These methods are used to either authenticate the identity of the user or ensure confidentiality of the transmission by ensuring better signal reception at the legitimate receiver compared to the illegitimate/malicious attacker [154], [155]. Apart from the channel itself, other works have also exploited the hardware/RF properties of the transceivers for device authentication [156], as well as physical parameters (such as distance/angle between devices) in the environment to ensure confidentiality [157].

In essence, PLS admits the following approaches to its fold: (a) extraction of secret keys to encrypt/decrypt data bits, (b) modification of physical signal/transmission based on securely shared keys, and (c) modification of physical signal/transmission based on extracted keys. While the current literature boasts various works providing an overview of existing PLS techniques with the focus either on certain attack types or their counter-measures - such as [55], [158] focusing on confidentiality and [159], [160] targeting anti-jamming PLS mechanisms - a singular definition and framework that not only encompasses the existing works but also enables the development of next-generation PLS methods is still lacking. Consequently, in this work, we provide a PLS framework that plugs the aforementioned gap in the literature by elaborating how PLS is achieved by first observing and then utilizing the

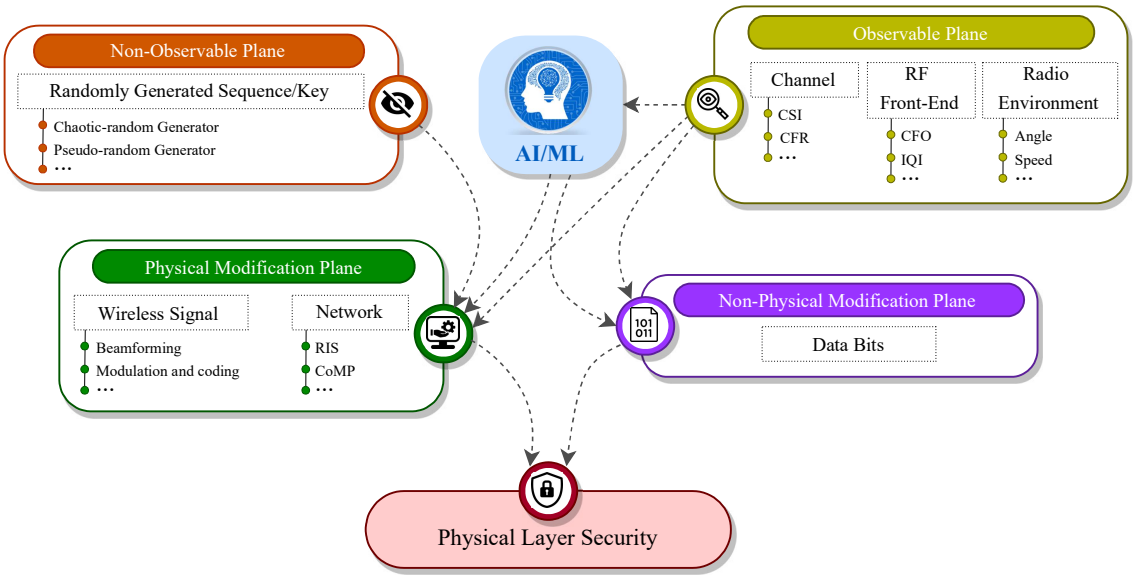

Figure 2.10: Illustration of PLS conceptual framework.

dynamic characteristics of wireless signals, RF front-end of the devices, transmission medium, and radio propagation environment to secure wireless transmissions. Here we would like to clarify that the goal of this particular work is NOT to survey all PLS works, rather we just present selected works relevant to different categories of approaches to illustrate how they fit in with the proposed framework.

Figure 2.10 provides a high-level illustration of the PLS framework. Essentially, an observable plane serves as the source of randomness/uniqueness that can be leveraged to secure or authenticate wireless transmissions. These observations may come from the channel, RF front-end, or the radio environment as long as they follow certain criteria. The parameters extracted from the observation plane (or securely shared sequences) are then used to modify the transmissions on the bit, signal, or network level. However, it should be noted that in any approach either the observation or modification parameters should be physical in nature. For instance, the combination of non-observable shared sequence with bit-level modification is NOT considered to be covered under the PLS umbrella (rather it is considered to be cryptography). The following passage provides more details regarding the modification/observation planes with selected examples from the literature, while a summary of the same is provided in **Table 2.1**.

Table 2.1: Examples of existing PLS schemes categorized according to PLS's threats, countermeasures and definition.

Threats	Countermeasures	Physical Modification	Observable Parameter	Example
Eavesdropping	Signal design	✓	✗	Constellation rotation using pseudo-random sequence [161], [162] and Chaotic-random sequence [163].
		✓	✓	Using channel information for constellation rotation [164], modulation selection [165], symbol interleaving [166], channel shortening filter design [2].
	Key generation	✗	✓	Generating channel-based key to secure the transmitted bits [167].
	Interfering signal	✓	✓	Design channel-based alignment signal [168].
		✓	✗	Adding pseudo-random artificial noise [169].
	Beamforming	✓	✓	Design channel-based linear precoding matrix [170].
	Cooperative communication	✓	✗	Utilizing cooperative jamming [171], [172], and CoMP [43].
Spoofing	RF/Hardware-based	✗	✓	Identify the receiver devices based on hardware features, e.g., IQI and power spectral density [173].
	Channel-based	✗	✓	Identify the receiver devices based on location features, e.g., RSSI and CSI [174], [175].
	Authentication tag	✓	✓	Generating channel-based authentication tags [176].
Jamming	Cooperative communication	✓	✗	Cooperative communication using trusted relays [177].
	Spread spectrum	✓	✓	Generating channel-based frequency hopping sequence [178].
		✓	✗	Utilizing pseudo-random frequency hopping sequence [147].
	Beamforming	✓	✗	Implementing directional antenna [179], and RIS [180]

2.6.3.1. Observation Plane

The *observation* plane consists of the various parameters related to the wireless propagation environment that serves as a source of entropy and randomness which can be leveraged to secure the wireless link. These parameters should comply with the following properties:

- **Measurability**: This term indicates the extent to which the observable parameter is capable of being noticeable, visible, and discernible. Specifically, it must be quantifiable, i.e., it can be measured using a scientific process.
- **Reciprocity**: This expression implies that the observable parameter's response measured at location A is theoretically identical to the response measured at location B, considering that the wireless transmission takes place between location A and B.
- **Uniqueness**: For a particular transmission, the observable parameter should

be unique, distinctive, and solitary in its characteristics. For instance, a third party that lies away from the legitimate transceivers should obtain a parameter uncorrelated to that between the legitimate parties.

– **Randomness**: From a statistics perspective, the observable parameter should have no apparent order and its individual values are uncertain and unpredictable. Specifically, the values of the observable parameter can be randomly modeled.

In the following text, we will evaluate the different domains, i.e., wireless channel, RF front-end, and radio environment, one by one in light of the same criteria.

2.6.3.1.1 Channel: As a wireless signal passes through the propagation environment, the interaction between the signal and objects in the environment manifests in the form of phenomena such as absorption, reflection, refraction, and diffraction. These phenomena are rendered time-variant and random due to mobility in the environment [181]. From the communication perspective, the random behavior of the channel becomes challenging, especially in rich scattering environments since the coherence distance, time and bandwidth become limited. On the other hand, this is invaluable from the PLS perspective as the channel observations of legitimate and illegitimate nodes become independent (as long as they are half-wavelength apart).

Here it is important to look at the wireless channel in terms of the ideal properties of the observable plane parameters. Even though the interaction between the wireless signal and the environment is fairly complex, various models have been developed to provide a mathematical representation of the influence that the environment has on the signals. As such, various quantities such as RSSI, CSI, CIR, and CFR are used to measure the channel. For the sake of modeling and analysis, the channel is generally represented as a finite impulse response (FIR) filter. If all other parameters (especially frequency) are kept constant, the channel is reciprocal, i.e., the channel response is the same in both uplink and downlink directions. In fact, reciprocity is one of the main motivations for the use of TDD systems. Moreover, the propagation environment consists of several objects with different reflection/absorption capabilities, leading to multipath propagation, i.e., when different replicas of the signal

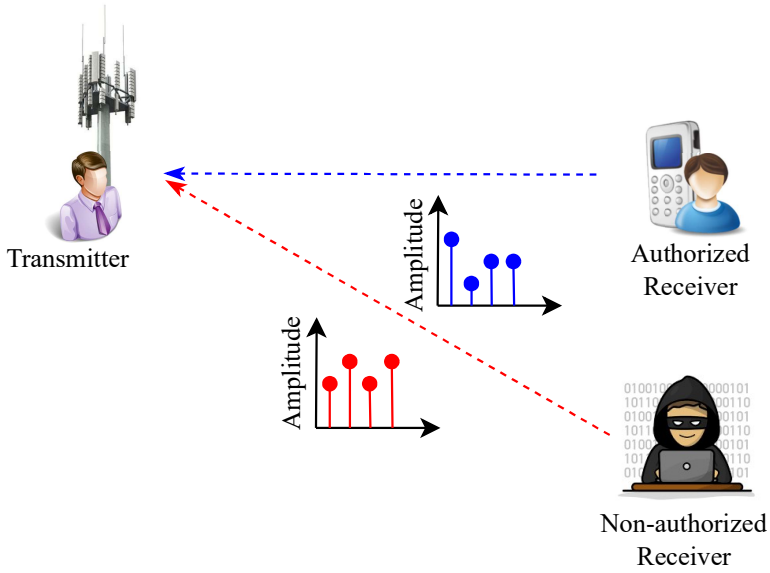

Figure 2.11: Difference in observed channel parameters such as CIR's amplitude (shown) and phase (not shown) can be used for link/device authentication.

arrive at the receiver with varying power levels and phases. These multipath components (MPCs) are modeled to be random and may add up constructively or destructively [182]. This randomness in turn means that the observed channel parameters are unique for different wireless links (as shown in **Figure 2.11**), and can therefore be used for link authentication. For instance, in [183] an machine learning (ML)-assisted wireless fingerprinting approach is proposed to complement higher-level authentication where the identity of each node is validated by its wireless channel properties. It should be noted that the uniqueness of the channel depends on the richness of the environment which, in turn, is a function of transmission parameters like carrier frequency. In case the propagation environment has poor scattering, the assumption regarding the independence of legitimate and illegitimate channels may not hold [184]. Consequently, in such cases, it is advisable to complement channel-based PLS techniques with other approaches that consider RF front-end or radio environment map (REM) information, as discussed later.

One of the major advantages of exploiting wireless channel for PLS comes from the fact that channel estimation is an integral part of wireless communication. Since the wireless channel is highly dynamic, the communicating nodes need to know the effect that the environment has on the signal so that it can be removed, and a clean signal can be recovered at the receiver. The PLS methods, therefore, do not

cause unnecessary overhead in terms of channel estimation. Consequently, wireless channel and its properties have been widely used in PLS for link adaptation [185], channel-based key generation [186], node authentication [187], and interfering signal injection [188].

In link adaptation, the goal is to utilize the independence of channel fading experienced by the legitimate and illegitimate nodes. In this category of approaches, the transmission parameters are adapted to optimize the communication over the legitimate link. Since the transmitted signal is adapted and optimized specifically for the legitimate receiver, it provides inherent security against any other user without requiring any additional processing or computation at the former [55]. Examples of link adaptation-based PLS approaches include subcarrier allocation [166], adaptive modulation and coding [185], power allocation [189], pre/post-coding [190], etc. As illustrated in **Figure 2.12**, key generation has four main steps. The first step is called channel probing where both users obtain their measurements of the shared channel. This is followed by quantization, where the analog measurements are converted to binary values. The quantization level is usually dictated by the SNR level of the measured channel. Quantization is followed by the information reconciliation step to take care of any disagreement/mismatch in the earlier measurements. Since this step involves the public exchange of information between the legitimate nodes, it is possible a malicious node might also extract some information. Therefore, to ensure the security of the generated key, privacy amplification is employed where any compromised information/bits from the keys are removed [191]. In node authentication, the spatial decorrelation of the wireless channel between legitimate and illegitimate nodes is exploited to verify the identity of the user. Generally, node authentication consists of training and message transmission phases. In the former, a database of the channel fingerprint is built, while in the latter the actual transmission is tested against the database to corroborate that the current and prior transmissions are carried out by the same user [192]. Here, it should be noted that for channel-based authentication to be useful, both training and transmission phases need to occur within the coherence time of the channel. Interfering signal injection (discussed in detail later) includes techniques where intelligently designed signals

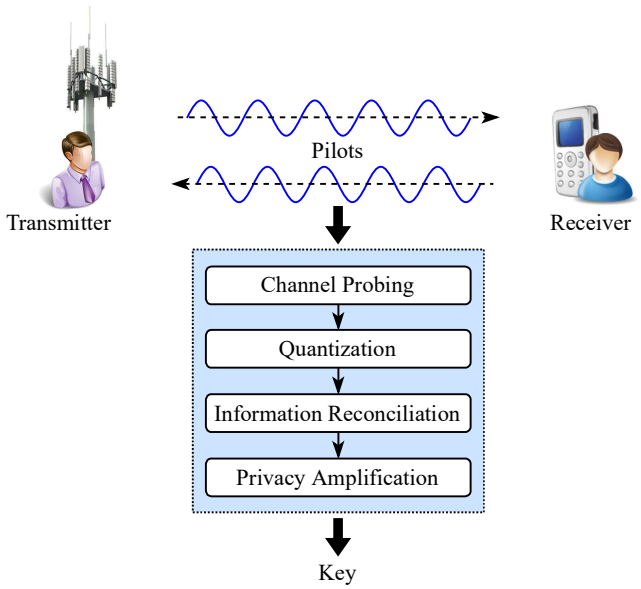

Figure 2.12: Basic steps for wireless channel-based key generation

are added on top of the transmitted data while taking into consideration the legitimate channel to ensure that they do not interfere with the legitimate reception.

Here, it should be reiterated that the channel observations are in fact a function of the transmission parameters used. For instance, path loss depends on the carrier frequency, with higher frequencies such as mmWave and THz undergoing significantly increased attenuation compared to the conventional systems. Since the classical channel models were developed for sub-6 GHz bands, they are unable to capture the propagation at these higher bands. As [193] illustrates, non-line-of-sight (NLoS) environment can not be modeled by a Rayleigh distribution at 28 GHz while a similar observation for THz bands is provided in [194]. Given that propagation in mmWave and THz bands is similar to each other [195], while being vastly different from conventional systems, it is necessary to develop and utilize more appropriate (and accurate) models capable of representing the heterogeneous networks expected in beyond 5G networks. Consequently, based on two-wave with diffuse power (TWDP) model [196] - which provides a physical explanation of why Rayleigh/Rician fading might not completely capture wireless fading - other models such as N-wave with diffuse power (NWDP) [197] and fluctuating two ray (FTR) [198] have been developed. NWDP generalizes TWDP to include N dominant MPCs in addition to the diffused components. The impact of the number, amplitudes, and total power

of these dominant MPCs on PLS metrics such as secrecy outage and capacity is provided in [197]. The authors analytically show that a more unbalanced distribution of amplitudes amongst the dominant MPCs of legitimate link compared to illegitimate one can significantly increase secrecy. The security analysis for FTR is found in [199], where the authors validate that increasing (decreasing) SNR of the legitimate (illegitimate) link leads to secure communication, and light shadowing in the eavesdropper's link improves secrecy capacity. In addition to the diffuse component-based models, other generalized models have also been proposed recently. κ-μ fading model, which provides a generalized representation of line-of-sight (LoS) environment, has been analyzed from secrecy capacity and secrecy outage probability in [200]–[203] where [201], [202], and [203] focus on single-input single-output (SISO), single-input multiple-output (SIMO) and MIMO systems, respectively. Secrecy outage for α-η-μ and α-κ-μ in presence of a passive eavesdropper is provided in [204]. It should be noted that α-η-μ model is used to represent the NLoS propagation with its non-linearity and non-homogeneous nature, while α-κ-μ models propagation where LoS link also exists. Secrecy capacity and outage analysis of the even more general α-η-κ-μ model, which has been shown to fit well with the measurements at mmWave frequencies [205], has been provided in [206]. (For more details regarding the performance of PLS methods under generalized fading models, readers are referred to [207].)

2.6.3.1.2 RF Front-end: In addition to the wireless medium itself, the RF front-end also suffers from imperfections leading to impairments such as clock jitter, phase noise, carrier frequency offset (CFO), in-phase/quadrature imbalance (IQI), non-linearity of the power amplifier, and antenna imperfections [208]. Since these impairments vary from device to device, they can be considered as device "fingerprints" that may then be used to distinguish between different devices [156]. As such, RF fingerprinting is one of the popular PHY layer authentication mechanisms (see **Figure 2.13**), targeted at eliminating (or at least detecting) any attacks on the node identity or message integrity. Another benefit of using RF fingerprint is how they complement the channel-based authentication. This is illustrated in [209], where device authentication is carried out using the device fingerprint

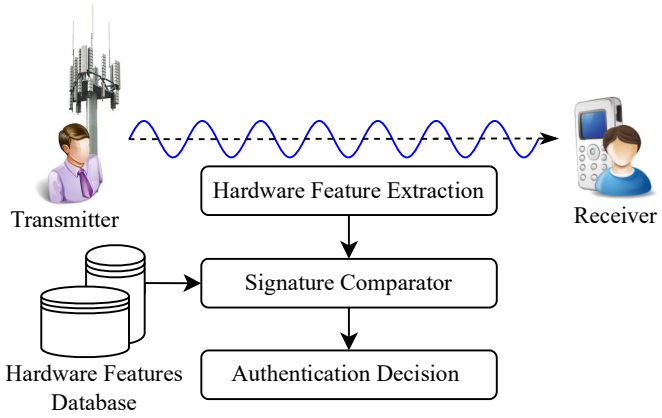

Figure 2.13: The RF impairments serve as potential "fingerprints" for wireless nodes.

while channel-based key generation is applied for secure communication in IoT devices. In general, while the channel-based methods are considered to be more appropriate for indoor and relatively stationary environments (so that authentication is not needed too frequently), the RF-based approaches can be leveraged in mobile environments due to their stability.

One of the challenges faced in RF-based PLS, however, is the reliability of the fingerprint in real network conditions. For instance, a single impairment may not provide enough dynamic range to enable distinction between devices. Different approaches to address this have been studied with [210] using a weighted combination of multiple device characteristics, while [211] discusses a collaborative approach to where observations from multiple nodes are used to authenticate a device. Similar to channel-based PLS, a major motivation for using RF impairment-based security solutions is the fact that they need to be identified/measured anyway to ensure reliable communication. However, a major issue in this regard arises when the hardware impairments have a similar effect on the signal as certain channel-related phenomena. For instance, mobility in the environment leads to Doppler spread/shift which is, in essence, a change in the frequency as seen by the receiver. This is similar in effect to the local oscillator imperfection leading to CFO and imperfect frequency synchronization. In such scenarios, one approach might be to try and separate the channel effects from device impairments utilizing the fact that the former are varying on a much smaller time scale while the latter are more stable [212]. An alternative

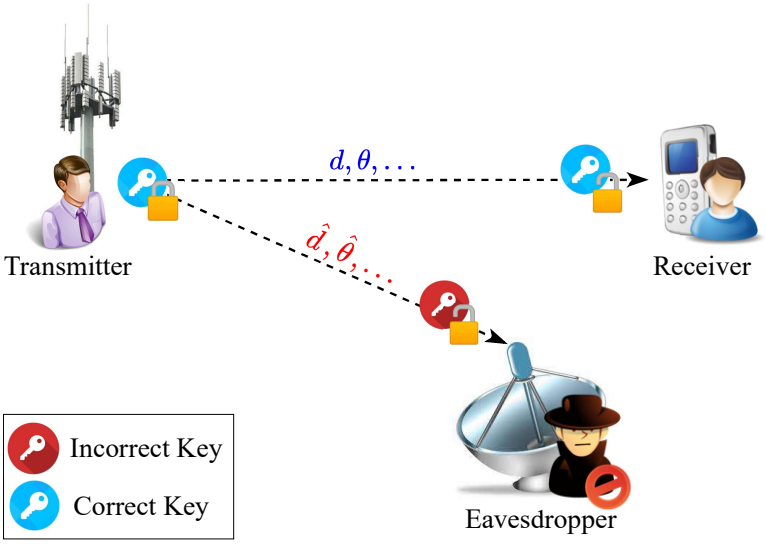

Figure 2.14: The physical parameters observed from the environment (such as distance or angle between the nodes) serve as the source of keys to be used for PLS.

to this is to incorporate both the channel and RF-based impairments into a time-varying device fingerprint, as illustrated in [213], where the CFO due to oscillator mismatch is combined with channel induced Doppler into a time-varying CFO used for authentication of the device. A similar approach is used in [214], [215]. In the former, imperfect or "chaotic" antenna geometries and activation sequences are used for authentication while in the latter beamspace representation of the mutual coupling between multiple antennas of a mmWave MIMO system is used for the same purpose.

2.6.3.1.3 Radio Environment/Sensing: As wireless signal traverses the air, it experiences different phenomena (such as absorption, reflection, refraction, diffraction, etc.) due to the objects and their properties in the surrounding environment. Similar to the independence of the channel in a rich scattering environment, the surrounding objects and their properties might also be independent and therefore, serve as an environment fingerprint for different links. Properties such as distance, speed, angle, size of objects, or their constituent materials exemplify the different observable parameters that can be considered to either authenticate or secure a wireless link [216]. **Figure 2.14** illustrates how different physical parameters can be used to generate keys in the network.

The most popularly used environment-related physical measurements for PLS include the distance or angle between the communicating nodes. For instance, the AoA-based key generation is employed in [131], where azimuth, elevation, or both angles are used to generate the secret key. The authors argue that AoA-based approach exhibits a lesser mismatch rate compared to channel-dependent key generation, rendering it more suitable for low SNR scenarios. Moreover, [157] proposes key generation based on the relative location of the communicating nodes. Since the relative location or distance is a reciprocal quantity, it eliminates the need for sharing the entropy source between the devices. There are various ways of calculating the distance, such as received signal strength (RSS) or time difference of arrival (TDoA)-based approaches [217]. As in the case of RF-based approaches mentioned earlier, it is possible to use parameters obtained from the radio environment or sensing in conjunction with channel knowledge, as is the case illustrated in [218]. It should be pointed out that in our generic PLS framework the sensing is not limited to RF domain. It is also possible to incorporate the information learned from external sensors including (but not limited to) cameras, LiDar, humidity/temperature sensors, etc.

2.6.3.2. Modification Plane

In the previous subsection, we looked at the *observation* plane which serves as the source of randomness/entropy which can then be exploited to secure the wireless link. The exploitation can be realized on the bit, the signal, or the network domain, which collectively make up the *modification* plane.

2.6.3.2.1 Data Bits: Wireless security mechanisms have conventionally been employed at the bit level. Classically, data is secured by converting the message or *plaintext* to *ciphertext* using some encryption mechanism [219]. Here it is important to make the distinction between cryptography and key-based PLS. In both cases, the transformation takes place at the bit level. In the former case, the key may or may not be shared between the communicating nodes in the cases of symmetric and asymmetric encryption, respectively. Either way, the encryption is done on the basis of a known/shared sequence. Since this process, including the key

sharing/management, is generally carried at higher layers, it is not covered under the PLS paradigm. On the other hand, PLS incorporates the key-generation mechanisms depending on the observable parameters related to the wireless channel and the radio environment around the communicating nodes as discussed in the previous section. Since both transceivers observe the same channel/environment from which the key is extracted, there is no need for key exchange in PLS mechanisms [220]. In addition to key-based PLS, channel coding has also been utilized to provide security at the bit level. While various realizations of this exist (including polar [221], low-density parity check (LPDC) [222] and other genres of codes [153]), one of the critical limitations of coding-based mechanisms is that the eavesdropper's (wiretap) channel needs to be degraded as compared to the legitimate link [223].

It should be noted that modification on the bit level is merely targeted at protection against eavesdropping. Jamming and spoofing are not addressed under this paradigm, which also happens to be a significant limitation of the standard cryptographic security solutions.

2.6.3.2.2 Wireless Signal: The majority of the work pertaining to PLS arguably falls under the wireless signal domain. Here it should be noted that in the context of *modification* plane, wireless signal covers all the blocks between the coded bitstream of data and the antenna at the transceivers. In the case of eavesdropping, this category of security solutions essentially aims to provide better data decoding capability at the legitimate receiver compared to the malicious attacker. This can either be done by intentionally degrading the performance of the eavesdropper or by improving the QoS for the legitimate receiver. Methods such as adaptive resource allocation [185] or **beamforming** [224] in the direction of legitimate node inherently provide some PLS since they are aimed at improving its link quality. Although the design of beamforming can be done according to different criteria (linear [225], [226] or nonlinear [227], [228]), a common goal is to direct the legitimate signal towards the legitimate receiver, while reducing the signal strength at the eavesdropper direction by making use of the spatial degree of freedom. A challenging issue in guaranteeing PLS arises if the eavesdropper is located closer

to the transmitter than the legitimate receiver. In this context, the secrecy performance of spatial beamforming may not be satisfactory. On the other hand, there are various realizations where **the interfering signal** may be generated at the eavesdropper such that it lies in the null space of the legitimate receiver, i.e., it does not interfere with the legitimate receiver's signal. For this, certain works assume knowledge about eavesdropper location/CSI and modify signals such that decoding capability at that particular node is degraded. For instance, [229] and [230] assume knowledge of the eavesdropper's CSI while adding artificial noise to the transmitted signal. However, this assumption cannot be counted upon, especially in the case of passive eavesdroppers. The more realistic alternative is to design interfering signals just considering the legitimate link's information. This is evident in [231] where the legitimate transmitter only knows the legitimate channel and has fewer antennas than the eavesdropper. Similar to this, noise-loop modulation is proposed in [158] guaranteeing secure and reliable transmission. In this approach, the legitimate receiver purposely jams the transmission by deliberately introducing noise in the channel leading to the concealment of the information from the illegitimate node, no matter its computational power. Another PLS approach, called **signal design** [232], has shown significant performance gain in preventing reliable data transmission to eavesdroppers by altering the signal structure (e.g., modulation scheme, constellation structure, extra process, etc.) such that an eavesdropper is unable to decode the received signal correctly. Constellation adaptation depending on the legitimate CSI has been proposed in [233] where the constellation order (and mapping) is modified depending on the channel phase. As a result, the eavesdropper is unaware of the modulation scheme/order being used in the transmission block and therefore, incapable of demodulating it as shown in **Figure 2.15**. In addition to channel-based sequences, other shared sequences have also been used for constellation rotation [161], [162]. All these approaches lead to a seemingly chaotic signal [163], characterized by a cloudy/distorted constellation, being observed by the eavesdropper. Channel-based shortening is proposed in [2] where a shortening filter is designed to reduce the effective delay spread at the receiver and the CP is reduced accordingly leading to ISI at the eavesdropper. The authors in [234]

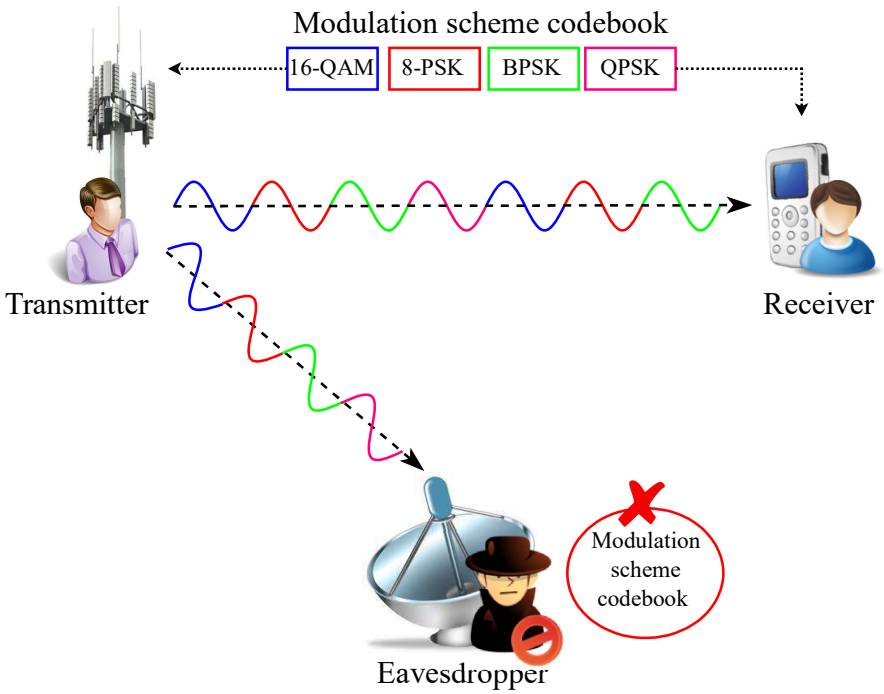

Figure 2.15: The modulation order/scheme is modified according to channel information making it difficult for the eavesdropper to intercept and demodulate the signal.

propose adaptive and flexible PLS algorithms where data and pilots are jointly secured. Particularly, minimum-phase all-pass channel decomposition is exploited, where the proposed algorithms precode the data and pilots using the all-pass component of the channel which is random enough to provide security without causing peak-to-average power ratio (PAPR), thus not harming the performance of the legitimate user. Apart from the channel knowledge, RF impairments have also been used to secure communication. For instance, in [235] the authors leverage the CFO by pre-equalizing its combined effect with the channel to provide secure communication. Since CFO of the legitimate link is independent of and unknown to the eavesdropper, the eavesdropping quality is degraded.

In terms of jamming, the most commonly utilized **spread spectrum** approach is to dynamically change the frequency at which the legitimate transmission is taking place to disrupt the jamming. The frequency hopping can be done on the basis of a pre-shared sequence [147], or alternatively, a channel-dependent sequence can be utilized [178]. While these approaches might be sufficient for rudimentary jamming attacks where the attacker does not have the capability to monitor and adapt to frequency hopping, more sophisticated and intelligent jammers capable of monitoring

the transmission can still be problematic. To address such attacks, a rather interesting approach is developed in [236] where the legitimate transmitter leverages deep reinforcement learning to first understand the jammer's strategy and then find the optimum countermeasure. It adapts its own transmission parameters in addition to harvesting the energy from the jamming signal. This does not only waste the attacker's power resources but also enables the legitimate node to augment its own transmission via ambient backscatter communication.

As far as spoofing is concerned, most PLS solutions target the authentication of the communicating node (and thereby the message itself) using either the wireless channel [175] or RF impairments [173]. Neither of these approaches requires any modification of the transmitted signal. However, a handful of works have proposed the addition of an **authentication tag** to the wireless transmission. The tag, independent of the message, is encrypted and embedded into the transmitted signal and used to differentiate the legitimate device from an illegitimate one [237].

It is evident from the above discussion that a plethora of signal modification PLS solutions have been developed against eavesdropping. Moreover, modification of the signal parameters is arguably the only effective approach to mitigate jamming. On the other hand, signal modification is not necessarily the best (or most popular) approach for protection against spoofing.

2.6.3.2.3 Network: The network in the context of the *modification* plane refers to the different nodes present in the environment. This may include relays in a cooperative communication scenario, base stations (BSs) in a CoMP architecture and RISs in smart radio environments. The cooperative communication paradigm has gained increasing popularity since it enables otherwise resource-constrained devices to reap the diversity benefits of MIMO technology in a distributed manner with the help of helper nodes or relays [122]. The cooperative communication process usually has two phases, where the first phase involves the broadcast transmission from the source (to both relay and destination), while in the second phase the relay retransmits the signal towards the destination [238]. These systems are regularly deployed in ad hoc or WSNs, where the decentralized structure, coupled with device limitations renders the authentication more burdensome compared to conventional

cellular or Wi-Fi systems. The lack of authentication leads to the possibility of malicious attackers posing as relays to adversely affect the communication. Accordingly, several approaches relying on cooperative relaying and jamming have been developed to alleviate the issue of untrustable relays [124]. In cooperative relaying, if there is the possibility of eavesdropping, trustworthy relay(s) are selected to avoid interception of the message. However, this might inhibit the diversity benefit which is the primary motivation of cooperation. Alternatively, in cooperative jamming, a known jamming signal is transmitted by either source, destination, or a helper node to disrupt the potential eavesdropper's interception. In the case of destination-based jamming [126], while the need for a helper is eliminated, the system cannot take advantage of the diversity unless the destination has full duplexing capability. Moreover, jamming, in general, is a power-hungry approach. An interesting workaround to this problem is provided in [59] exploiting the properties of FFT operation in OFDM transmissions, where the destination node transmits a jamming signal only during the CP duration of the broadcast phase. The FFT operation causes this jamming signal to spread throughout all the subcarriers at the relay, causing ICI and reduced interception. Since the signal is only transmitted for a limited (i.e., CP) duration the proposed solution is more power-efficient and does not require full duplexing capability.

Unlike cooperative communication, CoMP is strictly a cellular concept developed to mitigate the inter-cell interference, particularly for small cells and heterogeneous network deployments. CoMP was initially introduced for LTE in 3GPP Rel-11 [66], with various enhancements in the succeeding releases. While it is not the primary driver behind CoMP, a handful of works have looked at CoMP from other perspectives including PLS [45]. In an underwater communication scenario, the transmissions from multiple distributed antenna elements are scheduled (and their power controlled) such that the received signal at the legitimate receiver is clean and non-overlapping (from the different antenna elements) while the packets from different antenna elements overlap and interfere at the eavesdropper [43], as shown in **Figure 2.16**. The distributed BSs are also utilized to overcome the limitation of directional modulation where the eavesdropper lies in the same direction as the legitimate receiver [116]. This concept has also been extended to sparse environments, where

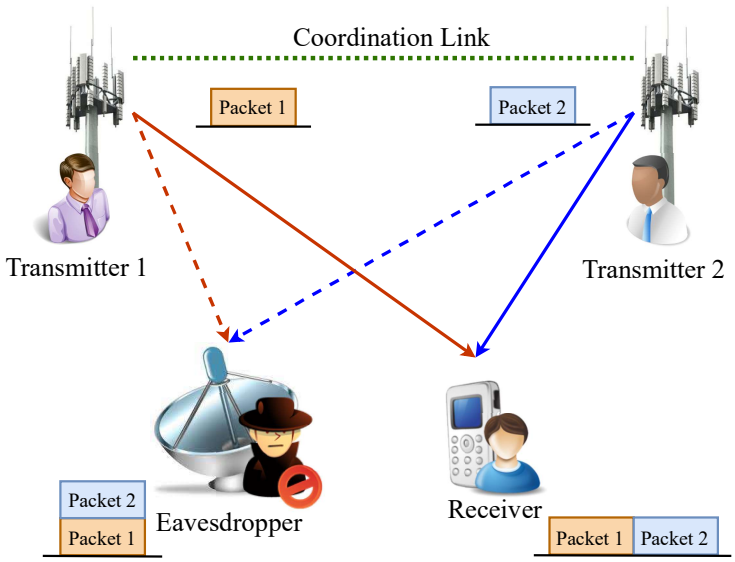

Figure 2.16: Intentional misalignment of the received packets (sent from different antenna elements) at eavesdropper to degrade its interception capability

coordination ensures that the transmitted message is only recoverable at the intersection of the transmissions from cooperating BSs [42]. The multipoint (or multi-landmark) is also extended to authentication, where RSSI observations are obtained at various physical locations to confirm the identity of a user [239]. The presence of multiple antennas at each landmark also provides better spatial resolution to further improve the accuracy of authentication.

In conventional wireless systems, the propagation channel is a function of the surrounding radio environment. It is, therefore, assumed to be uncontrollable and the transceivers can only try to compensate/mitigate this effect. Given that information-theoretic PLS requires the legitimate user's channel to be better than the illegitimate one's, the uncontrollable nature of the channel can be a hindrance to ensuring the security of communication [240]. However, the smart radio environment paradigm empowered by RISs envisions wireless channel as a controllable entity [241], which opens various new avenues for PLS using RISs. The authors in [242] further explore RISs in beamspace context and show how the channel is converted from a design problem with unknown gains into a design element with controlled gains. Having a controlled object in the environment opens a new dimension in addressing current and future problems in the wireless network. For instance, the scatterers in RIS can

be programmed to fast fade the channel of an eavesdropper, while maintaining a stable channel for intended users. Essentially, there are two main ways in which RISs can be exploited for secure communications, i.e., either by improving the secrecy rate/capacity of legitimate users or by enabling covert communications to hide the ongoing communication from the illegitimate user.

A survey of the former approaches is provided in [243], where various scenarios, systems models, optimization problems, and methodologies are discussed. RIS enables joint active/passive beamforming at the transmitter and RIS, respectively, using a large number of antenna elements available at the latter. This has been used to protect the communication from eavesdropping in [244], even in the presence of a stronger eavesdropper channel compared to the legitimate one in a LoS propagation environment. Joint beamforming is also discussed in [245], where authors motivate the use of RIS in mmWave and THz bands in the presence of a passive eavesdropper. RIS, in conjunction with artificial noise, is discussed in [246], where multiple eavesdroppers are present in the vicinity of the RIS. The impact of RIS on secrecy outage and average secrecy capacity in a vehicular paradigm is studied in [247], where the authors consider two scenarios, i.e., when the RIS is adjacent to the transmitter, and secondly when it is mounted on a building on the roadside. In [248], RIS is exploited to provide secure connectivity in D2D scenario where the direct link between users is unavailable.

RISs have also been purported as enablers for covert communication. For instance, [249] considers the case where a *warden* tries to detect the communication while an eavesdropper aims to intercept it. In such a system (or adversary) model, not only is the secrecy capacity to be optimized but also the received power at the warden needs to be minimized. In [250], adversarial machine learning is employed for deep neural network (DNN)-empowered illegitimate receiver to ensure that the adversarial perturbations in transmissions have an adverse effect on its detection capability, while the legitimate receiver can still detect the communication successfully. An RIS-based transmitter is proposed in [251] for a JSC system to embed communication symbols in the radar waveform in a covert manner. A hybrid relay/RIS is proposed in [252] where a joint power allocation and relay/reflection coefficient

selection problem is formulated to ensure reception of the transmission at the legitimate receiver while ensuring its covertness from the warden.

Additionally, RISs have been exploited in [180] to protect communication against jamming attacks. In particular, the joint optimization of beamforming and power allocation is studied with the goal of ensuring that the QoS requirements of the users are met in the presence of a multi-antenna jammer. Moreover, as mentioned earlier, from the PLS perspective a rich scattering channel is more desirable as it provides more randomness. One of the potential benefits of using RISs is controlling the variation in the channel over time, which can then be used for various purposes including PHY layer key generation [253].

The network-based PLS generally utilizes the macro-diversity to increase the reliability of a user's communication link while degrading the attacker's efficacy. These methods are primarily applicable to eavesdropping and jamming attacks, with limited effort to utilize cooperation in the networks for authenticating users.

2.6.3.3. From Observation to Modification Plane

As mentioned earlier, there are two primary components of the PLS framework discussed in this work. The first, i.e., the observation plane is the source of unique randomness that can be exploited by the second, i.e, modification plane to secure wireless transmissions. However, this raises the question about the decision mechanism that serves as the bridge between the aforementioned planes. In essence, what parameters should be observed in a given scenario, how long should they be observed, how should they be processed and analyzed, and consequently which approach in the modification plane should be utilized. Given that even for the same user, the security requirements may vary depending on the application being used, it is imperative that the system is capable of adapting in real-time. As such, the role of artificial intelligence (AI) and SONs becomes extremely critical. The original concept of adaptive or "cognitive" PLS was introduced in [254], further motivated in the context of V2X communication in [53], and finally a framework was provided in [49]. Like much of next-generation systems, optimized PLS is dependent on learning on the fly. The role of AI extends from signal analyses to modeling

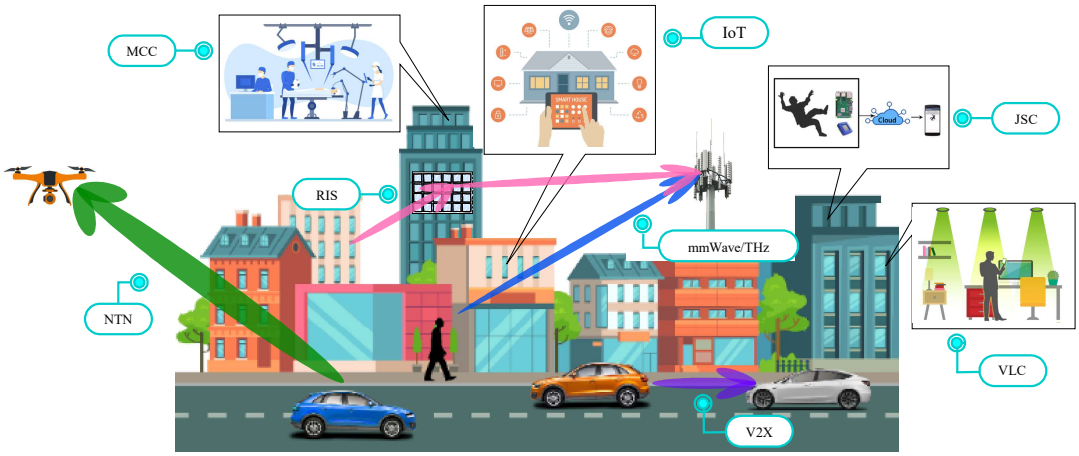

Figure 2.17: An illustration of the emerging technological trends for beyond 5G network paradigms where PLS might prove critical.

the behavioral characteristics of the users in the observation plane. The information of the environment is then utilized to identify any anomalies that exemplify the presence of malicious entities [212]. Following that, the appropriate selection of PLS mechanism, resource allocation, signal processing method, node selection (in network domain) needs to be carried out. However, it should be highlighted that AI itself suffers from various potential threats in the form of adversarial ML, and countermeasures must be taken to mitigate them [255].

2.6.4. Latest Trends and Future Directions for Physical Layer Security

Starting from 5G, each generation of wireless networks is expected to further diversify its use cases and applications. As a result, new technological paradigms are also expected to arise. In this section, we look at some 5G and beyond archetypes (shown in **Figure 2.17**) from a PLS perspective.

2.6.4.1. Joint Sensing and Communication

Sensing (radar) and communication are two of the foremost wireless technologies that have developed independently for decades. However, with the increase in the number of devices and applications for both, as well as the mutual reliance, there has been a push towards JSC in recent years. This is primarily driven by spectrum scarcity, power limitations, and general similarities in the hardware. The joint design, however, has certain drawbacks as it leads to degradation in performance of

either communication or sensing compared to the conventionally stand-alone systems [256]. Since sensing involves the transceivers acquiring information about their targets using wireless transmissions and their reflections [257], it raises serious concerns about user privacy and its vulnerability to any malicious nodes in the surrounding. In [49], the authors present a framework for JSC/radio environment security in addition to exploring the suitability of existing PLS methods for sensing. For sensing, the attacks might target the sensing process, nodes, or the environment. In a process-oriented attack, the main goal is to manipulate the wireless sensing process. Low probability of intercept (LPI)-based [258] and randomized probing-based [259] solutions are used, for instance, to defend against spoofing attacks on sensing system. Node-oriented attack targets the different nodes that are part of the radio environment awareness and mapping process. These nodes may support communication, sensing, or both. The attacker might be interested in information such as node's identity, data, velocity, angle, location, RF characteristics, power, and waveform used [260]. The environment-oriented attacks are on the physical-radio environment. This includes changing the LoS/NLoS characteristics, channel richness and sparsity, urban/rural categorization, mobility, physical objects, communication infrastructure, radio capable devices, interference, and so on. For instance, RIS can be used by the attackers to generate a fake multipath channel or absorb signals to misrepresent the coverage area [49]. While JSC has received significant attention from the design and optimization perspective, there is a glaring gap in the literature regarding its security provisioning. We believe that the PLS framework provided in **Subsection 2.6.3** delivers the necessary structure which can be extended to cover the sensing aspect of wireless systems.

2.6.4.2. RIS-empowered Smart Radio Environments

As mentioned earlier, RIS has great potential for enhancing the security of wireless communications. However, despite its promise, there are significant challenges related to CSI acquisition, phase noise/errors, and channel correlation, that need to be addressed before its full potential can be realized. For instance, the joint active/passive beamforming at the transmitter and RIS, respectively, requires the CSI of the eavesdropper (w.r.t. transmitter and RIS) but given that eavesdroppers are

often passive, this is not a reasonable assumption [261]. Related to this, there is the issue of outdated CSI and how it might impact the RIS's performance (in terms of capacity) which is tackled in [262], where the authors consider different (centralized and distributed) deployment scenarios. The obtained results show improved results for centralized architecture when RIS is closer to either communication node, while decentralized deployment leads to higher capacity when RISs are further away from these nodes. It should be kept in mind that the achievable capacity for any link is directly connected to PLS performance via its secrecy capacity. Another common assumption regarding RISs is the continuous nature of phase shifts that can be induced by its elements. However, as highlighted in [263], this is not the case. Rather, these phase shifts are intertwined with the amplitude response (or reflection coefficients) and, therefore, must be optimized jointly [264]. The results here also indicate that despite the imperfect assumption regarding phase shifts, the asymptotic results converge to the continuous phase shift capacity for a large number of reflecting elements suggesting that overall capacity or secrecy capacity gains in the case of PLS can still be achieved. The problem of phase errors from the perspective of diversity order is also investigated in [265], with the authors concluding that full diversity order can be achieved over independent fading channels with RIS as long as the absolute phase error is less than $\pi/2$. However, this raises the question regarding how valid the independent fading assumption itself is. Some recent works have attempted to tackle this issue, where [266] shows that the conventional independent and identically distributed (i.i.d.) Rayleigh fading model is not realistic for RIS and provides an alternate model for spatial correlation that can be used in future studies. This is then used as a baseline in [267] where temporal evolution of channel is also considered and degrees of freedom for finite spacing between the reflecting elements are analyzed. Their exact impact on the achievable capacity (or secrecy capacity), however, remains to be studied. An additional concern regarding RISs is their limited granularity in frequency domain due to lack of digital/RF chains. This can cause interference when users/networks use adjacent channels, leading to inadvertent disruption of communication and even limit the RIS's performance in terms of frequency-selective scheduling [268].

2.6.4.3. Higher Frequency Bands (mmwave and sub-THz)

The rising popularity of augmented/virtual reality applications necessitates higher bandwidths to ensure a smooth quality of experience (QoE) for the users. However, the amount of spectrum in the conventional cellular bands (up to 6 GHz) is already crowded. Consequently, higher frequency bands including mmWave and THz have garnered increasingly more attention from both academia and industry. These frequency bands have significantly different propagation characteristics compared to sub-6 GHz frequencies, with severe propagation losses being observed [269]. Moreover, such systems will use extremely directional narrow beams. Apart from strengthening the communication, directional transmission has the inherent advantage of security from any attacker lying outside the beam [153], [270]. The security of such transmissions can be further strengthened by the use of multiple propagation paths [271] and spatio-temporal array architectures [272]. The narrow beams and directional transmission, however, render reliable connectivity very challenging due to their small coverage area. Given that applications such as virtual reality cannot afford a connection being dropped, it is understandable that the mmWave/THz systems will be complemented by sub-6 GHz bands rather than operating in a standalone manner.

As discussed earlier, various models including NWDP, FTR, and the different variants of κ-μ have been proposed to represent the fading in mmWave/THz frequency bands. While the studies in references [200]–[206] provide theoretical analyses of several PLS metrics under the aforementioned fading models, there is still a paucity of PLS techniques that leverage these generalized models to improve the security performance of wireless systems in the higher frequency bands. Moreover, PLS mechanisms are required which can support nodes operating at distinct frequency bands with significantly varying channel propagation characteristics.

2.6.4.4. Visible Light Communication

With the revolution of the lighting industry and large unexploited visible light spectrum, VLC has been proposed as an auspicious and disruptive technology for 5G and beyond based on low-cost light-emitting diodes (LEDs), where the light is used for both illumination and data communication purposes simultaneously. VLC systems

are more immune against interference and less susceptible to security vulnerabilities which is inherited from the fact that light does not penetrate through any opaque objects such as walls [273]. Therefore, it is reasonable to consider the VLC channel perfectly secure, at the physical layer, in a single user and/or private room scenario. However, in public areas such as classrooms, libraries, hallways, or planes, securing VLC networks is required [274]. In these public areas, possible eavesdroppers may exist and try to attain confidential information [275]. As [273] points out, the fundamentals and techniques of PLS developed for conventional RF systems, discussed in **Subsection 2.6.3**, cannot be directly applied to VLC systems. This is primarily due to: (1) the variability of the standard specifications in transmission protocols and modulation schemes, and (2) the more deterministic nature of VLC channels. As such, typical techniques such as coding, multi-antenna schemes, relays/cooperation, and authentication do not apply to VLC systems [276]. For a comprehensive study of literature on securing VLC systems, readers are referred to [273], where different types of VLC systems are studied considering different network parameters such as the characteristics of VLC channel, the availability of CSI, the geometry of the communication environment, and the type of signaling used.

2.6.4.5. Non-Terrestrial Networks

Academia, industry, and standardization bodies have increased their activities related to NTNs as a potential enabler for ubiquitous connectivity, with the users clamoring for reliable service and coverage irrespective of their location [10]. Empowered by various deployment options such as satellites, high altitude platform systems (HAPS), and UAVs, NTNs are primarily used to expand the coverage in order to deliver connectivity to regions that are unreachable by conventional networks (i.e., isolated areas, marine vessels, airplanes) [277]. As stated in [278], the unique characteristics of NTNs make the problem of ensuring secure communication different from that of purely terrestrial networks (TNs). NTNs (at least the satellites) are primarily deployed in LoS scenarios, where the reduced propagation losses lead to increased coverage footprint. However, the increased coverage footprint also

results in greater vulnerability to eavesdropping attacks. In [279], the authors propose the use of polarization domain to effectively prevent the eavesdropper from detecting the communication signal. A dual-polarized antenna was designed in fixed downlink satellite communication that enabled legitimate receivers to obtain polarization information. A significant challenge in devising security mechanisms for NTN emerges in the case of hybrid networks, which comprise both terrestrial and non-terrestrial components [280]. This scenario is studied in [281], [282], where the former adapts relay selection and user scheduling to ensure confidentiality of the communication and the latter analyzes the secrecy performance of the link between a multi-antenna NTN and terrestrial recipients via multiple cooperative relays in the presence of several eavesdroppers.

2.6.4.6. Ultra-Reliable Low-Latency Secure Communications

5G introduced the mission-critical communication (MCC) paradigm under uRLLC services to facilitate applications such as industrial automation, smart grids, augmented/virtual reality and remote healthcare systems [283]. Apart from the obvious requirements related to reliability and latency, these applications also require high security owing to their critical nature. For instance, any manipulated/disrupted control message in applications such as remote surgery may lead to loss of life. Cryptography-based approaches may not be feasible since they violate the ultra-low latency requirement due to the high-complexity signal processing required by encryption/decryption and other key management and distribution tasks [58]. Meanwhile, the relatively short channel block-length also limits the usage of complicated encryption/decryption algorithms in MCC [54]. As a result, security at the PHY layer has garnered considerable attention as a tool to offer low-complexity security mechanisms and lightweight encryption schemes for MCC applications [284]. It should, however, be kept in mind that not all PLS methods are applicable to the MCC paradigm. For instance, multi-antenna-based beamforming techniques, discussed in **Subsection 2.6.3**, require accurate CSI which is hard or infeasible to obtain in uRLLC due to the ultra-low latency requirement. In such cases, location-based beamforming provides a desirable alternative [58]. An interesting thing to note here is the inherent trade-off between reliability and latency, which renders

optimizing both extremely difficult [1]. The work in [285] extends this optimization problem to also include security as an optimization parameter. Consequently, it is important to develop future PLS methods that take reliability and latency requirements as inherent constraints.

2.6.4.7. Massive Connectivity and IoT

IoT technology enables physical objects to sense, communicate, and perform certain actions on demand, which can facilitate a multitude of applications, such as smart home, smart city, and ITSs. Since IoT is becoming increasingly prevalent in our daily lives, the security of IoT network is indispensable. PLS techniques can improve the security of IoT networks from three main aspects: firstly, IoT devices may be fast-moving and continually switching between different access points (APs)/BSs. This will result in frequent authentication requests leading to a delay beyond the latency tolerance of next-generation scenarios/applications [57]. PLS simplifies the handshake process by using, for example, RF fingerprinting to provide a method of direct identification for the authentication process. Secondly, IoT is being deployed in all sectors at a massive scale which makes it difficult to efficiently distribute and manage the secret keys [286]. PLS offers an exciting alternative where all communicating nodes can directly extract the keys from their environment/channel, thus eliminating the need for key distribution and management. Lastly, IoT devices cannot afford complicated processing to maintain security [56]. While certain PLS methods such as beamforming [224], noise aggregation [287], cooperative jamming [288], and artificial noise injection [188] require additional hardware, processing, and energy resources, PLS also provides certain asymmetric PLS mechanisms where the load of designing a secure transmission is moved to BS/AP side and no additional processing is required at IoT node itself. That being said, most of the existing PLS mechanisms do not take into consideration the energy efficiency or try to jointly optimize it with security performance. The authors in [289], on the other hand, propose a user association approach that maximizes the secure throughput while minimizing energy consumption in an ultra-dense network. It is, therefore, likely that asymmetric, lightweight, and low-power PLS mechanisms

will attain increasing popularity in next-generation networks provided their performance is validated in realistic settings.

2.6.4.8. PLS in the Age of Edge Computing

Mobile edge computing (MEC) is touted to be a potential enabler for both mMTC/IoT and uRLLC applications by reducing the need for backhaul bandwidth for the former and cutting down the latency for the latter. The transference of computing capabilities closer to the user means real-time applications such as extended reality (XR) can be realized without the signal having to traverse all the way to the center of the network. Similarly, the amount of data to be sent to the central network can be reduced by doing preliminary analysis/processing at the edge servers/devices. However, the presence of additional network nodes outside the physically secure information technology (IT) center of the network introduces vulnerabilities to the privacy of user data from potential eavesdroppers, necessitating PLS methods tailored to MEC scenarios. One such scheme involving transmission of jamming signals from MEC servers is given in [290], where full duplexing capability is used to mitigate self-interference. A downlink (DL)-driven authentication mechanism using CSI fingerprint to counter any spoofing attacks is proposed in [291]. The impact of MEC on PLS, or how the former can enable and empower the latter, however, remains to be studied.

2.6.4.9. V2X Communication

V2X communication encompasses different facets of vehicular communication depending on what the connected vehicle communicates with, including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrians (V2P) and vehicle-to-network (V2N). In general, vehicles and end devices interact and exchange data with each other in order to improve road safety. Therefore, they need to be connected in a reliable and timely manner, where the confidentiality and security of messages are vital [292]. V2X communication is particularly vulnerable to the data exchange being intercepted and private information about identity, position, and trajectory of the users being exposed [293]. PLS has been discussed as a potential solution to these problems [294]. However, one of the biggest challenges in this

regard is to adapt to the varying security requirements as a function of the application, location, utility, environment, and other contextual information about the user. As [295] points out, it is not possible to provide appropriate security for different V2X applications and scenarios, suggesting applying different PLS techniques in a cooperative manner. An intelligent framework for this is provided in [53], however, any further studies or feasibility analysis of such an approach remains missing.

2.6.4.10. Adversarial ML and Explainable AI

The increasing complexity of wireless systems in terms of waveforms, propagation environments, and resource allocation has left the network operators and architects with no choice but to turn towards AI/ML to improve network performance. Some examples of this include the use of DL in Citizens Broadband Radio Service (CBRS) band to detect the presence of incumbent users, and the optimization of network slicing to improve network resource utilization. Both of these applications have shown to be vulnerable to adversarial ML, where the *black-box* nature of AI has been utilized to target the learning process and consequently render decisions adverse to the legitimate users/network [296]. Apart from approaches that involve pre-emptive training to mitigate possible adversarial attacks [297], [298], an alternative is to move towards explainable AI (XAI) to improve the level of users' trust towards such systems by providing interpretable explanations of the decisions taken by the machine. However, there remains a trade-off between explainability and performance for cases where mathematical models are absent [299]. Moreover, as [300] points out, unless the models are explicitly designed to be transparent, the explanation or interpretability remains a subjective function of the user's knowledge of the specific domain. Accordingly, it is important to design/tailor the AI/ML models with prior knowledge of the wireless communication domain.

2.6.4.11. Cross-Layer Security

Typically, the network protocol stack layers are protected with a set of independent and uncoordinated security mechanisms ignoring their cross-layer interaction. However, independent security solutions at different layers might lead to conflicting actions and result in performance degradation. For instance, intricate attacks

exploit multiple vulnerabilities of various layers leveraging isolation and lack of awareness and cooperation between them. Therefore, proper interaction and co-ordination among different protocol layers help in developing a robust detection system suitable for wireless networks. Such interactions are the key elements to building cross-layer architectures [301]. However, a limited number of works have been reported on this topic so far. For example, cross MAC/PHY layer security is proposed in [302]. Automatic repeat request (ARQ) (as MAC operation) and maximum-ratio combining (MRC) (as PHY operation) have been jointly exploited to enhance the confidentiality of wireless services requested by a legitimate user against eavesdropping attack. The potentials of application (APP) and PHY layers can also be explored to enhance security. Such as in [303] where employing authentication and watermarking strategies at the APP layer along with the coding and signal processing at the PHY layer can lead to considerable secrecy gains. Any further security interaction study between other layers and PHY layer remains missing.

CHAPTER 3

3. EXPERIMENTAL PART

This chapter lays the groundwork of the performance results obtained for the various contributions of this thesis. Specifically, the system model used and the proposed approach are discussed. Firstly, a simple case study is presented in **Section 3.1** to illustrate the generalized CoMP (GCoMP) concept, and highlight how it takes into account the user requirements, network resource availability, and backhaul or energy constraints. In **Section 3.2** presents the simplified network architecture as well as large-scale fading models for aerial and terrestrial links, followed by a description of the proposed approach to attain increased reliability. **Section 3.3** then describes a coordinated multipoint (CoMP) system as well as the justification of using channel shortening filters (CSFs) from multiple transmission points (TPs).

In **Section 3.4**, the system model for amplify-and-forward (AAF) relaying is presented along with details of the proposed jamming strategy. Finally, **Section 3.5** describes the delay-Doppler (DD) channel representation and key generation based om their indices, followed by a security analysis that shows the inability of eavesdropper to observe similar channel parameters as legitimate nodes.

3.1. Generalized CoMP (GCoMP) Framework

The diverse user requirements are represented by different applications [100]. The variation of available network resources is represented by the number of resource blocks (RBs) considered in each scenario, and the significance of GCoMP itself is shown by comparing the performance of the different combinations of coordination schemes and clustering approaches.

3.1.1. System Model/Assumptions

We consider an urban micro environment where the TPs and user equipments (UEs) follow Poisson point process (PPP) distribution with densities λ_B and λ_U, respectively [304], [305]. Total transmit power per TP, P_b^{Tx} (for b-th TP), is taken to be constant and equally distributed over all RBs. The power received at u-th UE for a transmission from b-th TP, $P_{b,u}$, is given by [306]

$$P_{b,u} = P_b^{Tx} - (36.7 \log_{10}(d_{b,u}) + 26 \log_{10}(f_c) + 22.7 + \sigma), \tag{3.1}$$

where $d_{b,u}$ represents the distance between b-th TP and u-th UE, f_c is the carrier frequency, and σ is the standard deviation of the zero-mean log-normal shadowing distribution.

Since the primary goal of GCoMP is to decide upon the clustering and coordination scheme, we look at the performance of their various combinations. In the case of clustering, we consider the possibility of using both static and dynamic clusters in each scenario. For the static case, conventional methods include determining the clusters which reduce outage, maximize the mean signal-to-interference-plus-noise ratio (SINR), or minimize the average interference [307], [308]. Since the interference, outage or SINR inherently depend upon the distance between TPs, we have leveraged simple clustering methods from the domain of pattern recognition where the physically closest C_{max} TPs are grouped together, with C_{max} representing the maximum cluster size. This has the added advantage of simplifying the implementation. For the dynamic case, clusters are formed on a per-user basis, where the b-th TP is considered to be part of the u-th UE's cluster depending on the fulfillment of the following criteria [304]

$$P_{b,u} \geqslant P_{min}, \tag{3.2}$$

and

$$P_{ser,u} - P_{b,u} \leqslant P_{diff}, \tag{3.3}$$

where P_{min} is a predefined threshold for including a TP in the cluster and P_{diff} is the maximum difference between received power from the serving TP, $P_{ser,u}$, and the candidate TP. Another parameter regarding the clustering is the (maximum) size of the cluster itself. A larger cluster size generally improves the coordination

performance at the cost of additional information exchange overhead [103].

In addition to clustering, coordination scheme selection is the other significant output of the GCoMP framework. For the performance analysis in this section, we have considered two coordination schemes, namely coordinated scheduling (CS) with muting [95] and joint transmission (JT) [304]. While the latter work only considers a dynamic clustering approach, we have also used the same JT mechanism for static clustering in our simulations. Furthermore, we have also considered the case of hybrid/adaptive coordination, where both of these schemes are simultaneously used in the network. For this purpose we adapt the method proposed in [309] to use a heuristic received signal strength indicator (RSSI) threshold in line with [117]'s approach to select between CS and JT schemes. The general expression for the SINR experienced by the u-th UE can be described as

$$\gamma_u = \frac{\sum_{t \in \mathcal{T}_u} P_{t,u}}{\sum_{b \in \mathcal{B}, b \notin \mathcal{T}_u, \mathcal{M}_u} P_{b,u} + N_0 B_T}, \tag{3.4}$$

where $\mathcal{B}$ is the set of all TPs in the coverage area, $\mathcal{T}_u$ and $\mathcal{M}_u$ are the sets of transmitting and muted TPs in u-th UE's cluster, respectively, N_0 is the noise power spectral density and B_T represents the total system bandwidth. Here it should be noted that in the case of CS with muting, $\mathcal{T}_u$ consists of a single TP while $\mathcal{M}_u$ comprises of all other TPs in the cluster. This means that each UE is served by a single TP and the corresponding RBs of all other TPs in the cluster are muted. In case of JT, $\mathcal{T}_u$ comprises of all coordinating TPs while $\mathcal{M}_u$ is an empty set, where the same RBs of all the coordinating TPs are used to serve the particular UE using zero-forcing (ZF) precoding [304], [305]. In the adaptive scheme, the decision whether a TP transmits to particular UE or not depends on the received power(s). For instance, b-th TP can be included in u-th UE's $\mathcal{T}_u$ if it satisfies the condition

$$P_{ser,u} - P_{b,u} \leqslant P_{th}, \tag{3.5}$$

where P_{th} is the received power threshold for adding a coordinating TP to the $\mathcal{T}_u$. As such, depending on the $P_{b,u}$ values the adaptive scheme can assume any configuration from CS to JT.

Given the SINR expression in **(3.4)**, the throughput of u-th UE from one RB can be

obtained using the Shannon's capacity formula, given as

$$R_u = B_{RB} \log_2(1 + \gamma_u), \tag{3.6}$$

where B_{RB} is the bandwidth of one RB. For a given required throughput of the u-th UE, $R_{req,u}$, the number of required RBs is given by

$$RB_u = \frac{R_{req,u}}{R_u \mid \mathcal{T}_u \mid}, \tag{3.7}$$

where $\mid . \mid$ represents cardinality of a set. These RBs are allocated to the UE as long as they do not overload the TP, i.e., the number of allocated RBs does not exceed the available RBs. This is ensured by keeping the load of b-th TP, given by the following equation, less than or equal to one

$$l_b = \frac{\sum_{u \in \mathcal{A}_b} RB_u}{RB_{\circ,b}}, \tag{3.8}$$

where $RB_{\circ,b}$ and $\mathcal{A}_b$ represent the available RBs and associated UEs of the b-th TP. The formulas for energy efficiency and required average backhaul bandwidth per TP are given by **(3.9)** and **(3.10)** below:

$$EE = \frac{\sum_{u \in \mathcal{A}} R_u}{\sum_{u \in \mathcal{A}} \sum_{b \in \mathcal{T}_u} \frac{RB_u P_b^{Tx}}{RB_{\circ,b}}}, \tag{3.9}$$

and

$$BH = \frac{1}{\mid \mathcal{B} \mid} \sum_{u \in \mathcal{A}} \sum_{b \in \mathcal{T}_u} R_{req,u}, \tag{3.10}$$

respectively, where $\mathcal{A}$ is the set of connected UEs in the network. As evident from the above expressions, energy efficiency is calculated as a function of the transmitted power. Other sources of power consumption such as precoding computation are NOT taken into account here. Similarly, backhaul requirements are also computed only considering the data sharing between the TPs for coordinated transmissions.

3.1.2. Problem Formulation

Our goal in this work is to pick the clustering and coordination scheme combination that maximizes (minimizes) the number of connected (unconnected) users, considering the energy efficiency and backhaul bandwidth constraints. Here it should be

noted that the users are connected only if the network is capable of fulfilling their throughput requirements. The overall problem can be mathematically formulated as

$$\begin{aligned}\Omega^* &= \underset{\Omega_i \in \{\Omega_1,\ldots,\Omega_7\}}{\arg\max} \left.\frac{|\mathcal{A}|}{|\mathcal{U}|}\right|_{\Omega_i} \\ &= \underset{\Omega_i \in \{\Omega_1,\ldots,\Omega_7\}}{\arg\min} \left(1 - \left.\frac{|\mathcal{A}|}{|\mathcal{U}|}\right|_{\Omega_i}\right) \\ &\text{subject to} \quad EE \geq EE_\circ, \\ &\qquad\qquad BH \leq BH_\circ,\end{aligned} \tag{3.11}$$

where $\mathcal{U}$ is the set of all users in the coverage area, $EE_\circ$ and $BH_\circ$ represent energy efficiency and backhaul constraints, respectively, and Ω^* is the optimum choice out of the following CoMP hypotheses:

$$\Omega = \begin{cases} \Omega_1 & : \text{No coordination} \\ \Omega_2 & : \text{CS scheme with static clustering} \\ \Omega_3 & : \text{Adaptive scheme with static clustering} \\ \Omega_4 & : \text{JT scheme with static clustering} \\ \Omega_5 & : \text{CS scheme with dynamic clustering} \\ \Omega_6 & : \text{Adaptive scheme with dynamic clustering} \\ \Omega_7 & : \text{JT scheme with dynamic clustering} \end{cases} \tag{3.12}$$

The simulations are carried out in MATLAB® environment and the simulation parameters used are summarized in **Table 3.1**. In line with the results observed in [304] we have selected a maximum cluster size of 3, since the coordination benefit diminishes with a higher cluster size. An example snapshot of the generated network layout is shown in **Figure 3.1**. To depict realistic network traffic, we have considered applications belonging to the guaranteed bit-rate (GBR), non-GBR and delay-critical GBR categories. **Table 3.2** lists the requirements for the particular applications selected from these categories [100]. Furthermore, we have also incorporated the effect of varying availability of network resources in terms of RBs by opting for $25, 50, 75, 100$ RBs/TP for all scenarios.

Table 3.1: Simulation parameters.

Parameter	**Value**
Simulation environment	Urban mirco
Carrier frequency (f_c)	5 GHz
RB bandwidth	180 kHz
Number of RBs/TP	20, 50, 75, 100
System bandwidth (B_T)	5, 10, 15, 20 MHz
Shadow fading standard deviation (σ)	4 dB
Total transmit power/TP (P^{Tx})	41 dBm
Noise power density (N_0)	-174 dBm/Hz
Max. cluster size (C_{max})	3
Min. received power to include in cluster (P_{min})	-110 dBm
Max. received power difference from serving TP (P_{diff})	20 dB
TP transmission mode threshold (P_{th})	10 dB
TP density (λ_B)	80 TP/km^2
UE density (λ_U)	800 UE/km^2
Simulation area radius	0.5 km

Table 3.2: User/application priorities and requirements

Service/ Application	**Resource Type**	**Priority Level**	**Throughput Requirements**
V2X Messages	Delay-critical GBR	18	5.4 kbps
Conversational Voice	GBR	20	40 kbps
Conversational Video	GBR	40	2.5 Mbps
Buffered Video	Non-GBR	60	2 Mbps

3.2. CoMP For Reliability

3.2.1. System Model and Assumptions

To assess the performance of coordination in a hybrid system, we consider a terrestrial cellular system assisted by aerial platforms (see **Figure 3.2**). In the system, the target coverage region is cell 1, where the randomly distributed ground users are served by terrestrial base station (TBS 1). Cell 2 and cell 3, served by TBS 2 and FBS, respectively, and positioned symmetrically for fair comparison, are considered in order to investigate the effect of terrestrial-terrestrial and terrestrial-aerial collaborations on macro-diversity performance. The coverage area in cell 1 can be

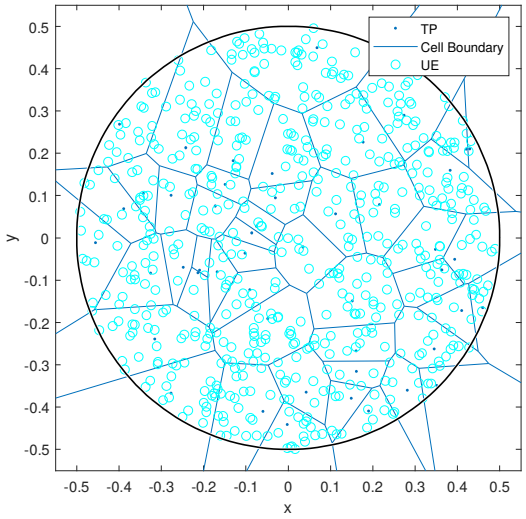

Figure 3.1: An example of the generated network layout, cell boundaries following Voronoi tessellation.

divided into three sub-regions (shown by hexagonal regions in **Figure 3.2**) according to the received power. In line with this, as an exemplification layout, the UEs 1, 2 and 3 are considered in the three regions. In this primary study we do not concern

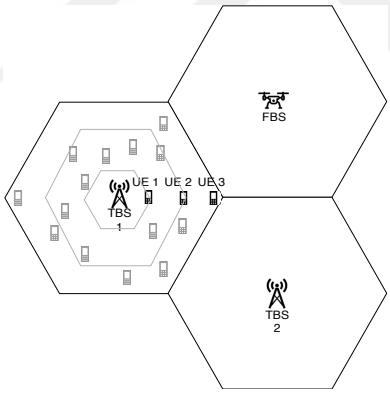

Figure 3.2: An illustration of the considered hybrid network layout.

ourselves with the energy utilization of the FBS, therefore we consider it to continuously working. The location of TBS is fixed and the FBS is assumed to be able to change its height at the same location. To simplify our problem, we consider the frequency reuse-3 case, which means all the BSs are using orthogonal frequency resources without interfering with each other.

3.2.1.1. Probability of Line-of-sight (P(LoS))

The key characteristic of a communication link utilizing FBS is the provision of a higher $P(LoS)$, which consequently provides improved channel conditions, particularly against shadowing effects. $P(LoS)$ is defined as a function of the elevation angle (θ) between the UE and BS, and environment dependent parameters. $P(LoS)$ curves for different environment are presented in [310], which are then approximated to a Sigmoid function (S-curve) in [311] as follows

$$P(LoS, \theta) = \frac{1}{1 + a \exp(-b[\theta - a])}, \quad \textbf{(3.13)}$$

where a and b are empirically determined coefficients for the S-curve derived in [311]. In our work, this curve is used for calculation of line-of-sight (LoS) probability for both terrestrial and flying BSs.

3.2.1.2. Pathloss Model for FBS

For FBS, the pathloss and shadowing is modeled as a sum of the free-space pathloss according to Friis equation and excessive pathloss which represents the additional log-normal shadowing factor. The expression is as follows [311]

$$PL_{FBS}^{\xi} = 20 \log d + 20 \log f + 20 \log(4\pi/c) + \eta_{\xi}, \quad \textbf{(3.14)}$$

where ξ belongs to (LoS, NLoS) propagation links, d is the 3-D distance between the BS and UE in meters and f is the carrier frequency in Hz and c is the speed of light in m/s. η represents the log-normal shadowing with non-zero mean and an elevation-dependent variance [312].

3.2.1.3. Pathloss Model for TBS

For TBS, we consider the alpha-beta-gamma (ABG) model, which can be generally expressed as [313],

$$PL_{TBS}^{\xi} = 10\alpha_{\xi} \log d + \beta_{\xi} + 10\gamma_{\xi} \log f + \chi_{\sigma\xi}, \quad \textbf{(3.15)}$$

where ξ belongs to (LoS, NLoS), f is the carrier frequency in GHz and d is the 3-D distance between the UE and the TBS in meters. α and γ represent the distance and

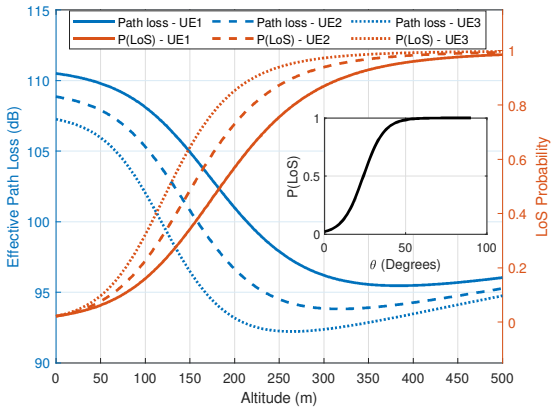

Figure 3.3: Average pathloss and P(LoS) for the defined user locations is plotted as a function of the FBS altitude. Inset figure shows P(LoS) as function of θ for urban environment

frequency dependence of the pathloss, respectively, β is an offset value and χ_σ is the shadowing standard deviation. We notice that, similar to the case of FBS, for TBS the pathloss is divided into LoS and NLoS components, and accordingly the parameters α, β, γ and χ_σ have different values for both cases.

3.2.1.4. Effective Pathloss

The communication links can be either LoS or NLoS, depending on the environment. Since the exact knowledge of environment, building heights, locations etc. is not always available, the randomness is incorporated using probabilistic approach [314]. The overall effect is therefore a combination of LoS and NLoS components, weighted according to their respective probabilities, which gives us the effective pathloss. The expression of this effective pathloss is given below [311]

$$\Lambda = \mathbf{P}(LoS) * PL_{LOS} + \mathbf{P}(NLoS) * PL_{NLoS}. \tag{3.16}$$

The effective pathloss for both FBS and TBS is calculated according to their individual LoS and NLoS components described in **(3.14)** and **(3.15)**, respectively. In line with this, **Figure 3.3** illustrates the LoS probability and effective pathloss (without shadowing effect) as a function of FBS altitude for the three selected users in urban environment. Also, the inset figure shows the LoS probability as a function of the elevation angle, calculated according to **(3.13)**.

3.2.2. Proposed Macro-Diversity Scheme

As mentioned earlier, the basic aim of this work is to exploit the air-to-ground channel characteristics to provide diversity against pathloss and shadowing. That being said, it is important to keep in mind that FBSs have their own limitations, considering which it is not possible to expect them to support constant network traffic. However, FBSs could be used to assist or support the TBSs for mission critical applications pertaining to the uRLLC service of 5G-NR. Using FBS in conjunction with conventional TBSs would provide added diversity against large scale fading effects of the channel. This is similar to the concept of macro-diversity or site-diversity, with one critical difference, i.e., in traditional macro-diversity scenarios the channel models for the different sites remain similar. However, in the case of FBS-TBS, the channel models vary considerably, potentially allowing significantly more diversity gain.

In line with this perspective, for ensuring a lucid understanding of the fundamental issues, we consider a very simple scenario consisting of two TBSs and one FBS, as well as only combining of two links for a particular user at the same time. This would allow us to compare the performance of TBS-TBS and TBS-FBS combined links. For this work we consider the use of maximum-ratio combining (MRC) since it is one of the most popular diversity combining techniques in the literature and promises optimum performance provided noise variance for both links is similar.

Instead of deriving the MRC expression from scratch, we use the results for average output SNR of a dual-branch diversity combining system under the effects of log-normal fading as presented in [315]. It is shown that the SNR for the different branches also follows a log-normal probability distribution function (PDF). The final expression is given below [315]

$$\begin{aligned} \overline{\gamma}_{MRC} &= \overline{\gamma}_1 + \overline{\gamma}_2 \\ &= \exp\left(\frac{\mu_1}{\zeta} + \frac{\sigma_1^2}{2\,\zeta^2}\right) + \exp\left(\frac{\mu_2}{\zeta} + \frac{\sigma_2^2}{2\,\zeta^2}\right), \end{aligned} \tag{3.17}$$

where $\overline{\gamma}_{MRC}$ is the average output SNR after combining, ζ is a constant that equals $10/\ln 10$, $\overline{\gamma}_i$ represents average SNR of the i-th branch, μ_i and σ_i^2 are the mean and variance values of the associated log-normal SNR distribution. It is pertinent

to mention that since the goal of this study is to observe the advantage of hybrid networks in terms of protection against pathloss and shadowing, we have not considered small-scale fading in any of the propagation links.

In the following chapter we will show with simulation results that FBS-TBS combination improves the reliability of the system as compared to TBS-TBS combining.

3.3. CoMP For Physical Layer Security (PLS)

To recap, the goal of this work is to leverage the spatially distributed TPs provisioned by CoMP to provide secure communication in wireless systems. This section firstly looks at the proposed approach and its relevant system model before discussing the necessary performance analysis.

3.3.1. System Model and Proposed Approach

As shown in **Figure 3.4**, a downlink communication system is considered where K single-antenna TPs coordinate to communicate confidentially with Bob in the presence of Eve. Both Bob and Eve are randomly located within the coverage area of the coordinating TPs and experience independent and uncorrelated frequency-selective Rayleigh fading channels. In this work, spatially distributed channel shortening technique is proposed to enhance physical layer security (PLS). In contrast to single-link channel shortening [2], the proposed technique ensures that Eve experiences longer delay spread over at least one of the links which will lead to inter-symbol interference (ISI) and degrade its interception capability.

At each time slot, the transmitted data, X, is split into K parts where the k-th data split, $X_k \subset X$, is transmitted independently from k-th coordinating TP. The i-th received symbol at either Bob or Eve, $Y_r(i)$, can be expressed as

$$Y_r(i) = \sum_{k=1}^{K} H_{r,k}^{\text{eff}}(i) X_k(i) + V_r(i), \tag{3.18}$$

where $r \in \{b, e\}$, depending on whether the receiver is Bob or Eve, $X_k(i)$ is the i-th transmitted symbol from k-th TP and $V_r(i) \sim \mathcal{N}(0, \sigma_{n,r}^2)$ is additive white Gaussian noise (AWGN) with zero mean and $\sigma_{n,r}^2$ variance. $H_{r,k}^{\text{eff}}(i) = H_{r,k}(i)\, W_{b,k}(i)$ represents effective channel of $r - k$ link where $H_{r,k}(i)$ is the N-point fast Fourier

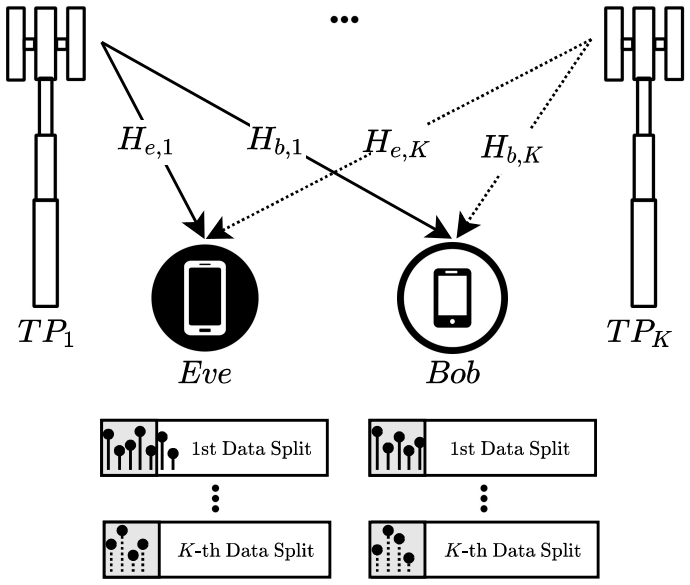

Figure 3.4: Illustration of the utilized system model.

transform (FFT) of the k-th TP's channel impulse response (CIR) and $W_{b,k}(i)$ is the CSF's coefficient based on the link between Bob and k-th coordinating TP.

3.3.2. Performance Analysis

To simplify the analysis, we consider the case of two coordinating TPs ($K = 2$) that serve a legitimate user in a confidential manner. As illustrated in **Figure 3.5**, data from the source is split into two parts, with each part going to one TP. Both TPs contain the CSF block, which is designed in accordance with the legitimate link. Accordingly, **(3.18)** can be rewritten as

$$Y_r(i) = H_{r,1}^{\text{eff}}(i)X_1(i) + H_{r,2}^{\text{eff}}(i)X_2(i) + V_r(i), \tag{3.19}$$

where, in order to make sure that at least some portion of each modulated symbol passes through the link which is worse for Eve compared to Bob, real-imaginary data splitting technique is used. Here, each symbol is split into its real and imaginary parts. Accordingly, $X_1(i)$ and $X_2(i)$ represent the real and imaginary parts of the transmitted symbol, $X(i)$, i.e.,

$$X_1(i) = \mathcal{R}\{X(i)\}, \tag{3.20}$$

$$X_2(i) = \mathcal{I}\{X(i)\}, \tag{3.21}$$

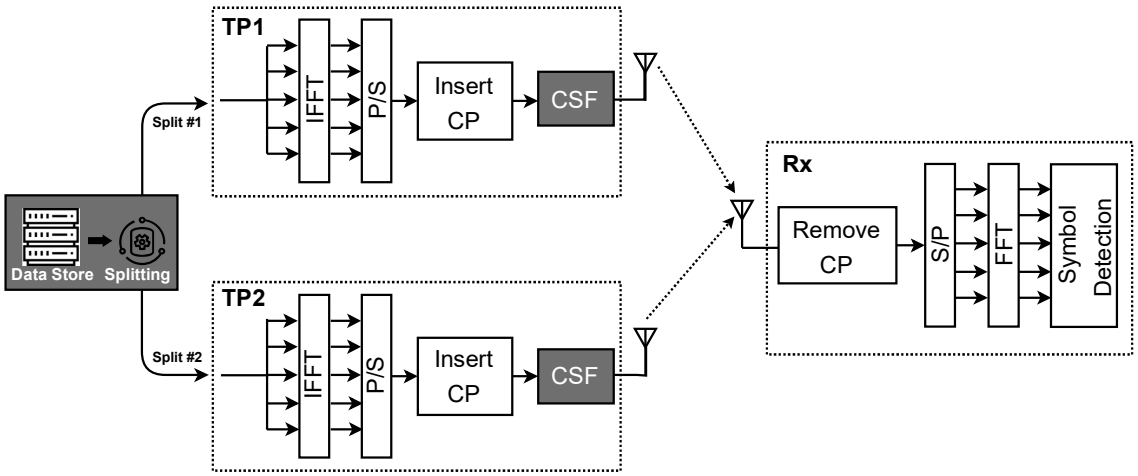

Figure 3.5: Illustration of the Tx/Rx block diagrams for the proposed method for two coordinating TPs ($K = 2$). Gray shaded blocks represent the additional stages compared to conventional orthogonal frequency division multiplexing (OFDM) transmitter.

each of which is then transmitted through one of the TPs. It is worth mentioning that spatially distributed channel shortening is applicable to any data splitting technique.

The performance evaluation of the proposed approach has been carried out in terms of achievable capacity for both Bob and Eve, using Shannon's capacity formula given in **(3.6)**. Here it should be noted that in this work co-channel interference is not considered. Rather, the interference (γ_r) constitutes the ISI and inter-carrier interference (ICI) generated due to insufficient cyclic prefix (CP). γ_r can, therefore, be given by

$$\gamma_r = \frac{P_r^{Rx}}{\sigma_{I,r}^2 + \sigma_{n,r}^2} \tag{3.22}$$

where P_r^{Rx} is the signal received power considering the contributions of real and imaginary links. In this work, we assume $P_r^{Rx} = 1, r \in \{e, b\}$. The interference and noise powers are denoted by $\sigma_{I,r}^2$ and $\sigma_{n,r}^2$, respectively. Based on the derivation in [316] for a large FFT size, $\sigma_{I,r}^2$ can be modeled as

$$\sigma_{I,r}^2 = \sum_{k=1}^{K} \sum_{l=1}^{L} |h_{r,k}^{\text{eff}}(l)|^2 \left(2\frac{\Xi_l}{N} - \left(\frac{\Xi_l}{N}\right)^2 \right), \tag{3.23}$$

where

$$\Xi_l = \begin{cases} \xi - \dfrac{\tau_l}{T_s}, & n_\epsilon T_s > \tau_l \\ \dfrac{\tau_l - T_{cp}}{T_s} - \xi, & 0 < n_\epsilon T_s < -(T_{cp} - \tau_l) \\ 0, & \text{Otherwise.} \end{cases} \tag{3.24}$$

Here the subscript l represents the l-th multipath component, N is the FFT size, ξ is the excess number of CIR samples beyond CP, τ_l is the delay of the l-th multipath component, T_s is the time interval between consecutive samples and T_{cp} is the CP duration. As mentioned earlier, spatially distributed channel shortening ensures that Bob's links are interference-free (i.e., $\sigma^2_{I,b} = 0$), and only Eve's links will suffer from ICI and ISI (i.e., $\sigma^2_{I,e} \neq 0$).

3.4. Secure Communication In The Presence Of Eavesdropping Relays

In this work, the idea is to exploit the use of FFT in OFDM systems to generate interference at the eavesdropper thereby degrading its interception capability. More details regarding the system model and proposed approach are provided in the remainder of this section.

3.4.1. System Model

Without loss of generality, we assume a dual-hop half-duplex relay-aided system with AAF protocol [238]. As shown in **Figure 3.6a**, it consists of a source that wants to communicate with a destination in the presence of an untrusted relay, where each node consists of a single antenna. Here, the goal is to use the advantages provided by the relay without letting it decode any information. The system is based on OFDM modulation with N subcarriers. The channels corresponding to source-destination (H_{sd}), source-relay (H_{sr}), and relay-destination (H_{rd}) links are assumed to be slowly varying Rayleigh fading with L exponentially decaying taps. A CP of length L is introduced to convert the multipath frequency channel into flat fading subchannels. At the transmitter, the frequency domain OFDM symbols $\mathrm{S} = \begin{bmatrix} S_0 & S_1 & \dots & S_{N-1} \end{bmatrix}^{\mathrm{T}} \in \mathbb{C}^{[N\times 1]}$ are passed through the inverse fast Fourier transform (IFFT) process as $s[n] = \sum_{k=0}^{N-1} S_k \exp^{\frac{j2\pi nk}{N}}$ and a CP of length L is added. The transmitted signal

with CP can be written as $\mathrm{s} = [s[N-L+1], \ldots, s[N-1], s[0], s[1], \ldots, s[N-L], s[N-L+1], \ldots, s[N-1]]$. Finally, the source node broadcasts the information to relay and destination. The received signal at the destination in the frequency domain on k-th subcarrier can be represented by

$$\begin{aligned} Y_{sd}(k) &= \sqrt{P_1} H_{sd}(k) S(k) + V_{sd}(k), \\ k &= 1, \ldots, K;\ n = 1, \ldots, N, \end{aligned} \tag{3.25}$$

where $H_{sd}(k)$ is the channel frequency response (CFR) of the k-th subcarrier between source and destination, the transmitted power by the source is represented by P_1, $S(k)$ is the symbol transmitted by source node on k-th subcarrier, and $V_{sd}(k)$ represents AWGN on the k-th subcarrier with variance $N_0/2$. Similarly, the received signal at relay is given by

$$Y_{sr}(k) = \sqrt{P_1} H_{sr}(k) S(k) + V_{sr}(k), \tag{3.26}$$

where $H_{sr}(k)$ is the CFR of the k_{th} subcarrier for source-relay and $V_{sr}(k)$ represents the AWGN. The relay node will normalize the received signal before retransmission by the factor [238]

$$\beta(k) = \sqrt{\frac{1}{P_1 |H_{sr}(k)|^2 + N_0}}. \tag{3.27}$$

Finally, the received signal at destination from the relay can be given as

$$Y_{rd}(k) = \sqrt{P_2} H_{rd}(k) \Big(\beta(k) Y_{sr}(k) \Big) + V_{rd}(k), \tag{3.28}$$

where $H_{rd}(k)$ is the frequency domain channel attenuation on the k-th subcarrier between relay and destination, the transmitted power is represented by P_2, and $V_{rd}(k)$ shows AWGN on the k-th subcarrier. The receiver will finally combine $Y_{rd}(k)$ signal with $Y_{sd}(k)$ given in **(3.25)** by applying MRC and decode the information [317].

3.4.2. Proposed Approach

This section presents the details of the proposed algorithm. The basic idea here is to devise a method that enables us to utilize the advantages of the untrusted relay while keeping the information secure from being eavesdropped on by the same node. Moreover, we want to achieve this goal without using an external helper or full-duplex receiver. It should be noted that in the case of half-duplex destination,

diversity gain is nullified since the destination transmits jamming signal throughout the first phase rendering it incapable of receiving the broadcast copy of the signal. The proposed approach, on the other hand, provides the required spatial diversity obtained from the signals received in both phases while ensuring that the relay is unable to intercept the data signal. This is achieved by the transmission of jamming signal over the CP duration of the received OFDM signal in the first phase.

The proposed algorithm has two phases.

- **Phase-1**: Source transmits a communication signal while destination sends a jamming signal during a portion of signal duration.
- **Phase-2**: The relay forwards a signal that it receives during phase-1 to the destination for final combining and decoding at the destination.

The following text provides details of the aforementioned phases of the proposed approach.

3.4.2.1. Phase-1

In phase-1, the source node broadcasts an OFDM signal to destination and untrusted relay over multi-path Rayleigh fading channel. The received signals at destination and relay are given in **(3.25)** and **(3.26)**, respectively. The relay forwards the received signals using AAF protocol to the destination in phase-2 to enhance the reliability of communication. However, there is a possibility that the relay may try to intercept and decode the data signal for malicious purposes. To ensure reliable communication while ensuring security from the untrusted relay, we propose that the destination transmits the jamming signal over the CP duration of the received signal right before receiving the OFDM signal. Even though the jamming signal overlaps with only a portion of the time-domain transmitted signal, its effect spreads over all the data-containing subcarriers once the FFT process is applied at the relay. This received signal at the relay, containing the jamming signal arriving from the destination is given by

$$\begin{aligned}\hat{Y}_{sr}(k) &= \sqrt{P_1}H_{sr}(k)S(k) + V_{sr}(k) \\ &\quad + \sqrt{P_j}H_{rd}(k)J(k) + V_{rd}(k),\end{aligned} \tag{3.29}$$

where $J(k)$ is the jamming signal and the power of the jamming signal transmitted by the destination is represented by P_j. It should be noted that **(3.29)** contains the additional jamming term compared to **(3.26)**, hence the term $\hat{Y}_{sr}(k)$ is used instead of $Y_{sr}(k)$.

Figure 3.6 provides a temporal illustration of phase-1 and how the signals arrive at both destination and relay. The transmission from the source initiates at time t_0. The signal arrives at relay and destination nodes at times times t_1 and t_2, respectively. The destination then transmits the jamming signal, equal in length to the CP itself and represented by a checkered block in the figure, immediately upon receiving its signal. The jamming signal reaches the relay at t_3. The starting point of the jammed portion of the relay's signal in time can be calculated as

$$t_d = t_3 - t_1 = \frac{d_{sd} + d_{rd} - d_{sr}}{c}, \tag{3.30}$$

where d_{sd} indicates the distance between source and destination, d_{sr} is the distance between source and relay, and d_{rd} is the distance between relay and destination. As mentioned earlier, as long as part of the jamming signal overlaps with the data portion at the relay, its decoding capability is degraded. The overlap itself is ensured by the propagation delay between the transceivers.

3.4.2.2. Phase-2

In phase-2, the relay transmits the signal to the destination after employing AAF protocol. The received signal at the destination from the relay without jamming is given by **(3.28)**. Replacing $Y_{sr}(k)$ with $\hat{Y}_{sr}(k)$ in **(3.28)** and expanding it gives us

$$\begin{aligned}\hat{Y}_{rd}(k) = \sqrt{P_2}H_{rd}(k)\big(&\beta(k)\sqrt{P_1}H_{sr}(k)S(k) \\ &+ V_{sr}(k) + \sqrt{P_j}H_{rd}(k)J(k) + V_{rd}(k)\big).\end{aligned} \tag{3.31}$$

The receiver will first remove the jamming signal from $\hat{Y}_{rd}(k)$. Since the jamming signal is known at the destination and CP is discarded in the receiver anyway, the jamming signal does not affect the signal of the legitimate receiver. However, some reflected components of the jamming signal may leak into the actual data and cause a self-interference. In this study, we assume that the receiver is able to cancel that interference by estimating the channel around itself. Afterwards, it employs MRC

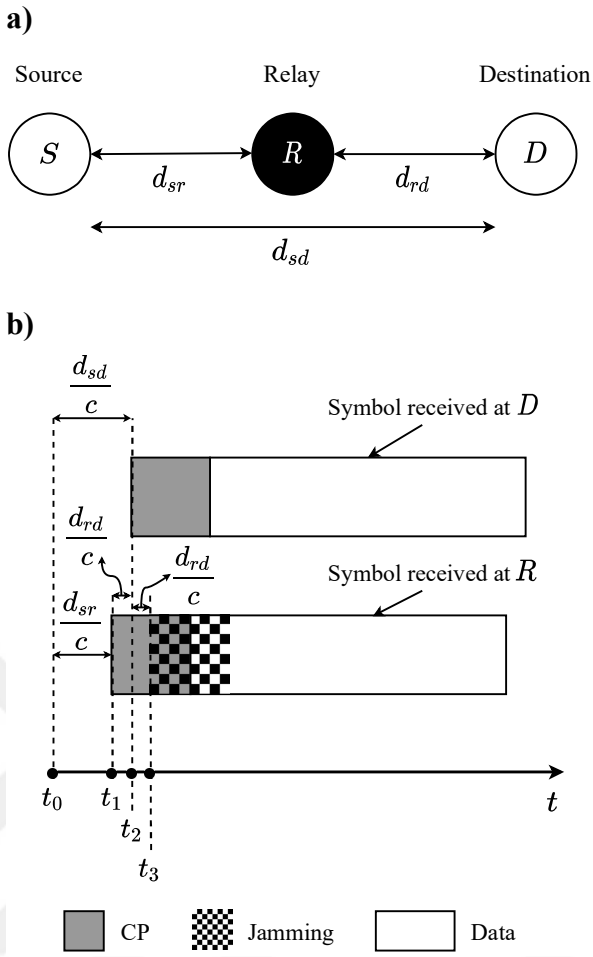

Figure 3.6: Illustration of the proposed approach in a relaying scenario. (a) A typical dual-hop relay aided system comprising a single source, relay and destination each. (b) The user signal is transmitted from source (S) at time t_0, reaching the relay (R) and destination (D) at times t_1 and t_2, respectively, while the jamming signal is transmitted by D at t_2 and reaches R at t_3.

[317] to combine the resultant signal with the $Y_{sd}(k)$ that it received during phase-1 (after sending the jamming signal).

Here it is important to highlight that unlike conventional PLS techniques [55], the proposed method does not require channel state information at the transmitter [318]. This renders the proposed approach suitable for scenarios where the transmitter/source node has limited capabilities in terms of computation, channel estimation, etc. Moreover, the proposed method does not impose any limitation in terms of channel selectivity, making it suitable for all environments.

3.5. Delay-Doppler Based Key Generation In V2X Communication

In this section, we first go through the system model considered for delay-Doppler based key generation followed by a discussion of the key generation process itself.

3.5.1. System Model

A system comprising two legitimate transceivers called Alice and Bob, and an eavesdropper called Eve is considered. The environment is mobile, i.e., the terminals and/or scatterers are assumed to be moving (as in the case of vehicle-to-everything (V2X) communication). Then the channel is modeled as doubly-dispersive in the DD domain, given by

$$h(\tau,\nu)=\sum_{i=0}^{L-1} h_i\delta(\tau-\tau_i)\delta(\nu-\nu_i), \tag{3.32}$$

where h_i and L denote the complex channel gain and the number of propagation paths, respectively. $\tau_i = \frac{l_i}{M\Delta f}$ and $\nu_i = \frac{k_i+\kappa_i}{NT}$ denote the delay and Doppler shifts corresponding to the i-th path with l_i, k_i, and $\kappa_i \in [-0.5, 0.5]$ representing integer delay, integer Doppler, and fractional Doppler shifts, respectively. M and N refer to the number of subcarriers and time-domain symbols in a DD frame, respectively. Δf and T denote subcarrier spacing and symbol duration. Orthogonal time-frequency space (OTFS) transmission is adopted, where the DD domain signal is first transformed to time-frequency using inverse symplectic Fourier transform (ISFT), followed by Heisenberg transform to convert it to a time-domain signal. After propagation through the channel, this signal is received as [319]

$$\begin{aligned} Y(l,k)=\sum_{i=0}^{L-1}\sum_{q=0}^{N-1} h_i\Gamma(l,k)\left(\frac{e^{-j2\pi(-q-\kappa_i)}-1}{Ne^{-j\frac{2\pi}{N}(-q-\kappa_i)}-N}\right) \\ \times X_{dd}\left([l-l_i]_M,[k-k_i+q]_N\right)+W(l,k), \end{aligned} \tag{3.33}$$

where X_{dd} and W denote data symbols in DD domain and the AWGN with zero mean and variance σ^2, $\Gamma = e^{\frac{j2\pi k_i(L_{cp}+l-l_i)}{(M+L_{cp})N}}$ where L_{cp} is the length of the appended cyclic prefix, and the term $\frac{e^{-j2\pi(-q-\kappa_i)}-1}{Ne^{-j\frac{2\pi}{N}(-q-\kappa_i)}-N}$ in **(3.33)** is due to fractional shifts of the two-dimensional sinc pulse along the Doppler axis in DD domain, coming from rectangular pulse shaping.

3.5.2. Proposed Key Generation Using Delay-Doppler Indices

3.5.2.1. Probing

For channel estimation, the impulse-based method of [320] is adopted, where a single pilot is surrounded by a guard. Due to the presence of fractional Doppler in our system, this guard extends the entire Doppler dimension. Then, the probing is simultaneously performed in uplink and downlink using the approach provided in [321]. The pilot signal-to-noise ratio (SNR) values, referred to as SNR_p are kept relatively high in DD domain (between $20 - 50$ dB), however this power spreads throughout the time-frequency grid once transformed. For instance, $\mathrm{SNR}_p = 40$ dB for a DD grid with $M = N = 64$ would translate to an SNR of 3.88 dB in time-frequency domain.

3.5.2.2. Normalization and Quantization of the Indices

As shown in **Figure 3.7**, the received pilot symbols are converted back to the DD domain, where the indices of the shifts in both domains (l_i's and k_i's) are used to generate the shared keys by converting the index to its corresponding binary value. The generated key can be represented by $\Psi = [\psi_1, \psi_2, ..., \psi_L]$, where ψ_i represents the key bits generated by the i-th tap in DD domain and has a length of $\log_2(l_{max}) + \log_2(2k_{max})$ bits, where l_{max} and k_{max} are the maximum delay and Doppler shifts, respectively. While integer delays is reasonable for wideband systems, ensuring integer Doppler shifts requires a long frame duration, which is impractical for systems with low coherence duration, such as in the case of V2X communication. Note that the delays given in the tapped delay line (TDL) model [322] used for V2X scenario can be resolved as integers if a $1/3$ or $1/6$ nanosecond resolution is used, which translates to $30 - 60$ MHz bandwidth.

Accordingly, we consider the fractional Doppler case in the current work. This not only allows us to examine a more practical case but also enhances the key generation rate (KGR) with the quantization of the fractional Doppler shift values. The generated key in this case can be represented as $\Psi^{\mathrm{frac}} = [\psi_1^{\mathrm{frac}}, \psi_2^{\mathrm{frac}}, ..., \psi_L^{\mathrm{frac}}]$ where the length of ψ_i^{frac} is given by

$$\log_2(l_{max}) + \log_2(N/\Delta) \tag{3.34}$$

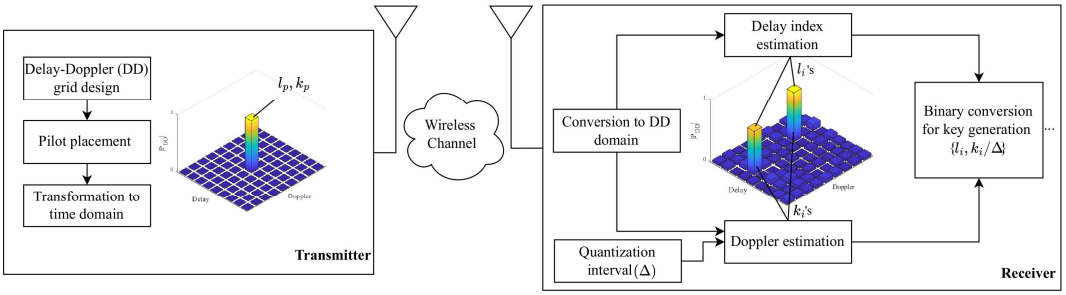

Figure 3.7: A simplified block diagram of the proposed approach.

where Δ denotes the Doppler quantization interval. Note that $N > 2k_{max}$ and Δ is a fractional value, i.e., < 1 which leads to a higher KGR when fractional Doppler shifts are incorporated. Additionally, recall that while the delay is a reciprocal quantity [134], the Doppler shift is a function of the carrier frequency and therefore not exactly reciprocal in frequency-division duplexing (FDD) systems. However, the uplink and downlink Dopplers can be extracted from one another using $\nu_U = \nu_D(f_D/f_U)$ where f_U and f_D are uplink and downlink carrier frequencies, and ν_U and ν_D are their respective Doppler shifts. Consequently, the uplink receiver can calculate the downlink Doppler shift and use it for shared key generation. Key generation generally consists of four steps, i.e., probing, quantization, information reconciliation, and privacy amplification. Our focus in this paper is limited to the first two. For the remaining two, we refer the readers to [191].

3.5.3. Security Analysis

3.5.3.1. Regarding Observed Doppler

As **(3.32)** shows, there is a delay and Doppler shift associated with each path between the transmitter (Tx) and receiver (Rx), which is used to generate the shared key. Unless Eve is adjacent to Bob, it is unable to observe the same parameters. To further illustrate this, consider the case of a Tx communicating with an Rx in the presence of a mobile reflector, as shown in **Figure 3.8**. Let f_0, f_1, f_2 be the respective frequencies transmitted, reflected, and, received at the Tx, reflector, and Rx, that are moving with the velocities v_0, v_1, and v_2, respectively. Then,

$$f_1 = \left(\frac{c \pm v_1 \cos(\theta_1)}{c \pm v_0 \cos(\theta_0)}\right) f_0, f_2 = \left(\frac{c \pm v_2 \cos(\theta_3)}{c \pm v_1 \cos(\theta_2)}\right) f_1, \quad \textbf{(3.35)}$$

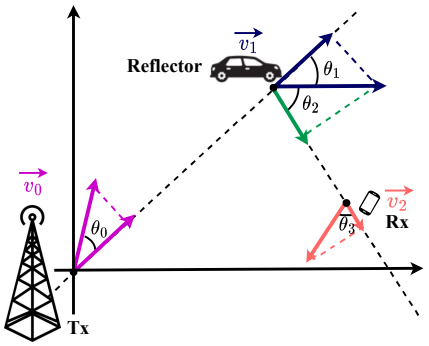

Figure 3.8: Illustration of the Doppler (angular) relations between transmitter and receiver in the presence of a reflector

where c denotes the speed of light, θ_0 is the projection angle of Tx's velocity ($\vec{v}_0$) in the direction of reflector, θ_1 is the angle of $\vec{v}_1$'s component on the Tx-reflector axis, and θ_2 and θ_3 are the projection angles of $\vec{v}_1$ and $\vec{v}_2$ on the reflector-Rx axis, respectively. From **(3.35)**, we find

$$\begin{aligned} \nu &= \Delta f = f_2 - f_0 \\ &= \left[\left(\frac{c \pm v_1\cos(\theta_1)}{c \pm v_0\cos(\theta_0)}\right)\left(\frac{c \pm v_2\cos(\theta_3)}{c \pm v_1\cos(\theta_2)}\right) - 1\right] f_0 \\ &\approx (\nu)\,\frac{f_0}{c}, \end{aligned} \tag{3.36}$$

where $\nu = \pm v_0\cos(\theta_0) \pm v_1(\cos(\theta_1) + \cos(\theta_2)) \pm v_2\cos(\theta_3)$.

As seen above, Doppler shift is a function of the velocity, and the velocity of an object at any given instant can be modeled as the summation of its mean value and the instantaneous variation. Given that the variation may be due to various reasons including road condition, weather, traffic, speed limits, the condition of the car etc., it can be modeled as a Gaussian distribution, $\mathcal{N}(0, \sigma_v^2)$, using central limit theorem (CLT). Specifically, in our case, ν from **(3.36)** can be written as

$$\nu = \bar{\nu} + \varsigma, \tag{3.37}$$

where $\bar{\nu} = \pm\bar{v}_0\cos(\theta_0) \pm \bar{v}_1(\cos(\theta_1) + \cos(\theta_2)) \pm \bar{v}_2\cos(\theta_3)$, $\varsigma \sim \mathcal{N}\left(0, \tilde{\sigma}_v^2\right)$ and $\tilde{\sigma}_v^2 = (\cos^2(\theta_0) + (\cos(\theta_1) + \cos(\theta_2))^2 + \cos^2(\theta_3))\sigma_v^2$. Then, practically the Doppler shift in **(3.36)** for the i-th channel tap is

$$\nu_i = (\bar{\nu}_i + \varsigma_i) f_0/c = \bar{\nu}_i + \tilde{\nu}_i. \tag{3.38}$$

where $\bar{\nu}_i = \bar{v}_i\frac{f_0}{c}$ and $\tilde{\nu}_i = \varsigma_i\frac{f_0}{c}$. As seen from **(3.38)**, the Doppler shift is also

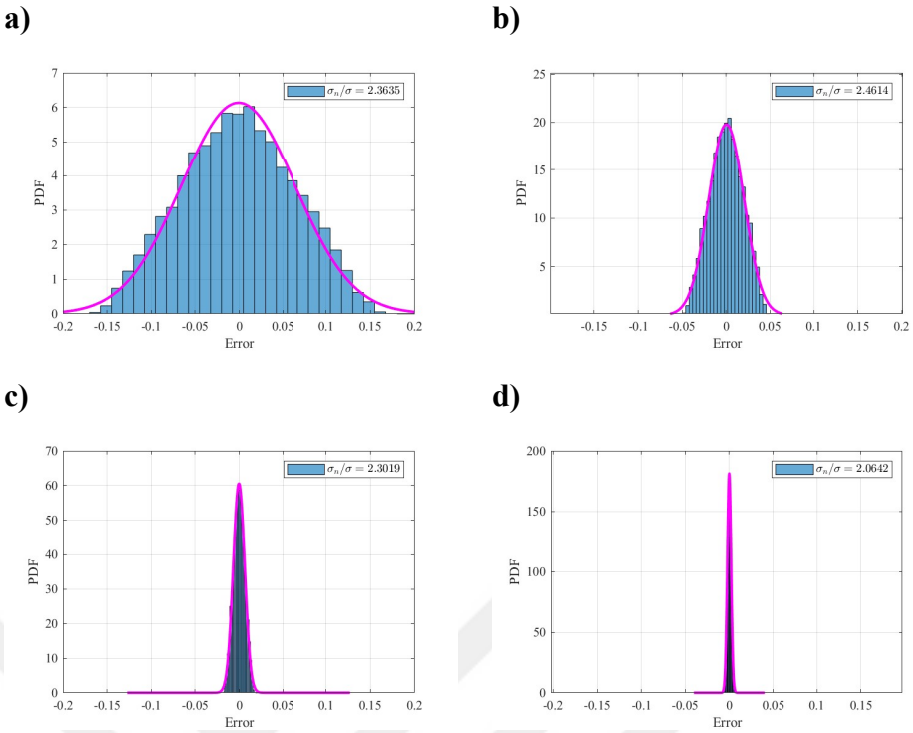

Figure 3.9: The variance of error observed at the receiver for different SNR_p values. (a) $\text{SNR}_p = 20\text{dB}$, (b) $\text{SNR}_p = 30\text{dB}$, (c) $\text{SNR}_p = 40\text{dB}$, (d) $\text{SNR}_p = 50\text{dB}$.

normally distributed as follows:

$$\nu_i \sim \mathcal{N}(\bar{\nu}_i f_0/c, \tilde{\sigma}_v^2 \, (f_0/c)^2). \tag{3.39}$$

Then, the normalized (by c/f_0) and discretized Doppler shift $k_i + \kappa_i$ is also normally distributed as follows

$$k_i + \kappa_i \sim \mathcal{N}(\bar{\nu}_i NT, (\tilde{\sigma}_v NT)^2). \tag{3.40}$$

The discussion illustrates that the observed θ_i's, ν_i's, and consequently the Doppler shift values, ν_i's, at Eve would differ by virtue of its location and speed. This is further analyzed in the following discussion.

3.5.3.2. Key Mismatch Between Alice and Bob

The relative velocity between Alice and Bob, as seen by an uncorrelated observer, is random and given by **(3.37)**. However, for these two nodes themselves, the observed velocity (and resultant Doppler shift) becomes deterministic. Consequently, the mismatch between Alice and Bob in estimating the Doppler shifts raises solely

from the AWGN. The conventional mismatch analysis for coefficient-based key generation methods does not apply to mismatch in the indices. Accordingly, we empirically determine the error in delay/Doppler index estimation at the receiver which is shown to be a zero-mean Gaussian with a variance that is smaller than that of the noise by a factor C (i.e., $\sigma = \sigma_n/C$), which is independent of the DD grid size and channel properties (number of paths) but depends on the SNR and channel estimation method being used. For this work, we take the average of the values shown in **Figure 3.9**, which ≈ 2.3.

The Doppler shift, represented by **(3.39)**, can be shown by the following PDF:

$$f_\nu(x) = \left(1/\sqrt{2\pi\sigma^2}\right) e^{-(x-\mu)^2/(2\sigma^2)}, \tag{3.41}$$

where $\mu = \bar{\nu}_i NT$. Then, considering uniform quantization for the normalized Doppler shift, the probability P_m of a sample lying between quantization levels d_m and d_{m+1} can be written as

$$\begin{aligned} P_m &= \int_{d_m}^{d_{m+1}} \left(1/\sqrt{2\pi\sigma^2}\right) e^{-(x-\mu)^2/(2\sigma^2)} dx \\ &= \left[Q\left(\frac{d_m - \mu}{\sigma}\right) - Q\left(\frac{d_{m+1} - \mu}{\sigma}\right) \right]. \end{aligned} \tag{3.42}$$

Key mismatch occurs when the Doppler shift is in the interval $[d_m, d_{m+1}]$, however, estimated elsewhere. The probability of the estimated Doppler shift falling in the wrong interval can then be expressed as the complement event of **(3.42)** given by

$$P(e|k_i + \kappa_i \in [d_m, d_{m+1}]) = 1 - P_m = P_m'. \tag{3.43}$$

Furthermore, the probability of the key mismatch can be derived from **(3.43)** as follows

$$P(\mathrm{KM}|k_i + \kappa_i \in [d_m, d_{m+1}]) = \frac{1}{N/\Delta} \sum_{m'=0, m' \neq m,}^{N/\Delta} p_b P_m', \tag{3.44}$$

where $\Delta = d_{m+1} - d_m$ and p_b is the number of mismatched bits between m' and m normalized by the total number of bits generated from the Doppler shifts (i.e., $\log_2(N/\Delta)$). The mismatch in delay estimation is also calculated using the same steps as in **(3.42)-(3.44)**. However, since the delays are assumed to be integers, $k_i + \kappa_i$ is replace by l_i, Δ is taken to be unity and the normalization is done by $1/M$.

3.5.3.3. Key Mismatch Between Bob and Eve

The Doppler shift measured between Alice and Eve is different from the one between Alice and Bob even if Eve is spatially correlated with Bob. This is due to random velocity change as discussed in **Subsection 3.5.3.1**. Then, the Doppler shift between Alice and Eve follows the same distribution in **(3.41)** with the same mean but a different variance given by $\sigma_{\text{eve}} = \sqrt{(\tilde{\sigma}_v NT)^2 + \sigma^2}$. The probability P_m^{eve} of a sample lying between levels d_m and d_{m+1}, and the corresponding probability of key mismatch are found as in **(3.42)** and **(3.44)** by replacing σ by σ_{eve}. The delay estimation mismatch for Eve follows the same steps as Bob.

Furthermore, to illustrate the efficacy of the proposed approach, we also consider Eve to experience a channel that is correlated to that of Bob (w.r.t Alice). In this case, the correlated delay and Doppler taps are given by

$$(l_i, k_i)^{e'} = \text{Round}[\rho (l_i, k_i)^b + \sqrt{1-\rho^2}(l_i, k_i)^e]. \tag{3.45}$$

where $(l_i, k_i)^b$ and $(l_i, k_i)^e$ represent the delay-Doppler taps of Alice-Bob and the uncorrelated Alice-Eve links, respectively, and ρ is the correlation coefficient. To generate the correlated Doppler indices, we assume a normal distribution similar to the one in **(3.39)** where the mean value (ν_i) is correlated as

$$k_i^{e'} + \kappa_i^{e'} \sim \mathcal{N}\left((\rho \bar{\nu}_i^b + \sqrt{1-\rho^2}\bar{\nu}_i^e)NT, \sigma_{eve}^2\right). \tag{3.46}$$

3.5.3.4. Secret Key Capacity

The lower and upper bounds of secret key capacity, C_K, are given by:

$$\begin{aligned} I(A;B) - \min\{I(A;E), I(B;E)\} \leq C_K \\ \leq \min\{I(A;B), I(A;B|E)\}, \end{aligned} \tag{3.47}$$

where A, B, E refer to the channel observations at Alice, Bob, and Eve, respectively and $I(X;Y)$ is the mutual information between two random variables (X, Y), defined as [323]

$$I(X;Y) = \sum_{x \in X} \sum_{y \in Y} P_{(X,Y)}(x,y) \log\left(\frac{P_{(X,Y)}(x,y)}{P_X(x)\, P_Y(y)}\right). \tag{3.48}$$

Here, the Doppler distribution for Alice is given by **(3.40)**, and marginal distributions for Bob and Eve are obtained using **(3.42)** (using respective variances). Together, they are used to obtain the joint and marginal distributions for Bob and Eve. The same process is then repeated for the observed delays. Since delay and Doppler observations are independent, we sum the secret key capacity for both to get the overall value.

CHAPTER 4

4. RESULTS AND DISCUSSION

This chapter presents the results obtained (via simulations) for the different contributions presented in this thesis. **Section 4.1** is aimed at illustrating the efficacy of generalized CoMP (GCoMP) in terms of satisfying varying user requirements under dynamic network resources by adapting different coordinated multipoint (CoMP) schemes and clustering approaches. **Section 4.2** discusses the gains obtained in terms of signal-to-noise ratio (SNR) when a hybrid network is used as opposed to a conventional terrestrial one. **Section 4.3** presents the secrecy capacity obtained via the use of distributed channel shortening compared to the conventional approach. Later, the performance comparison of relay and destination (in terms of bit error rate (BER)) is provided for different relay locations and jamming powers in **Section 4.4** to show that the short jamming signal does indeed have a significant impact on the eavesdropping relay's performance. Lastly, **Section 4.5** presents the achievable key mismatch rate (KMR) and secret key rate for the proposed approach. Furthermore, the randomness of the generated key is also evaluated.

4.1. Generalized CoMP (GCoMP) Framework

The performance of the proposed GCoMP framework is evaluated in terms of number of connected users, energy efficiency and the required backhaul bandwidth. To illustrate the effect of varying user/application requirements and network congestion, different services and resource block (RB) availability levels are considered. **Figure 4.1** shows the results averaged over 100 network (and user) realizations for the case where users are equally distributed amongst the four applications

listed in **Table 3.2**. The percentage of unconnected users for different coordination/clustering schemes and the associated energy efficiency and backhaul requirements are shown in **Figure 4.1a**, **Figure 4.1b**, and **Figure 4.1c**, respectively. It is observed that in terms of unconnected user equipments (UEs) dynamic clustering performs better than the static approach for all three coordination mechanisms; coordinated scheduling (CS) scheme performs the worst, joint transmission (JT) scheme offers the best performance and the adaptive scheme provides intermediate results. "No coordination" bisects the two clustering approaches, providing better performance than all coordination schemes with static clustering and worse than all dynamic ones. While the performance of CS being worse than "No coordination" scheme might seem rather surprising, it should be kept in mind that CS and (some) adaptive cases are accompanied by muting of the other transmission points (TPs) in the cluster. This means that overall a smaller number of RBs is used for transmission, leading to reduced energy consumption, as shown in Figure **Figure 4.1b**. Since muting improves the signal-to-interference-plus-noise ratio (SINR) experienced by UEs, it improves the energy efficiency as compared to the "No coordination" case, even though a smaller number of users is entertained. This is also evident in Figure **Figure 4.1c** where CS with static clustering requires the lowest backhaul bandwidth out of all approaches. It is interesting to note that the difference in performance for the various Ω's becomes more evident as the system bandwidth increases. In order to study this effect in more detail, we look at how the performance varies for different user/application requirements.

Figure 4.2 illustrates the scenario where all UEs utilize conversational video and the results seem to follow the same trend as the equiprobable application distribution case. However, it can be seen that the performance of different schemes has a more significant gap in this case (for maximum system bandwidth, B_T), with CS and static clustering leaving 70% UEs unconnected and JT with dynamic clustering leaving around 25% unconnected UEs, as compared to the equiprobable case where the former has about 40% users unconnected and the latter has 20% unconnected UEs. Accordingly, the backhaul requirements for JT are much more pronounced in this case as compared to the previous one. In the case of energy efficiency, even though CS schemes are still the best, this effect is not as pronounced as the first scenario.

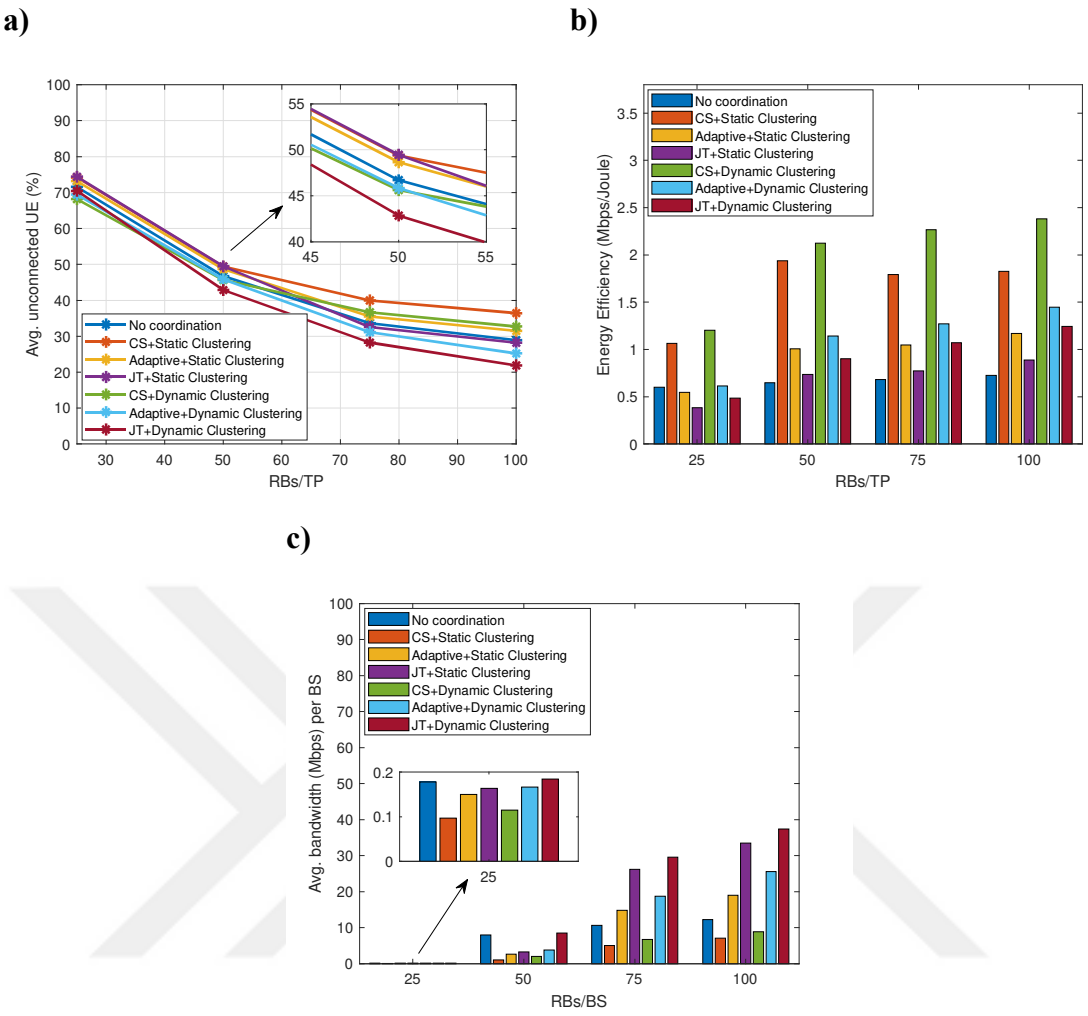

Figure 4.1: Performance comparison of different coordination schemes and clustering approaches when all applications (given in **Table 3.2**) are equiprobable. (a) Number of unconnected users, (b) Energy efficiency, (c) Average backhaul bandwidth required per TP.

Considering how the performance diverged with an increase in application demands, we can expect the opposite to happen when the requirements are lowered. This is validated in **Figure 4.3**, where all UEs are assumed to use vehicle-to-everything (V2X) messaging which has the lowest requirements of the applications mentioned in **Table 3.2**. As expected, the performance of different coordination/clustering schemes seems to converge in this case. Though it should be noted that for 25 RBs, the "No coordination" and dynamic clustering approaches have significant gains as compared to static clustering. Also, the energy efficient nature of CS is more pronounced as compared to both the earlier scenarios.

The GCoMP decision making can be illustrated with the discussion provided above.

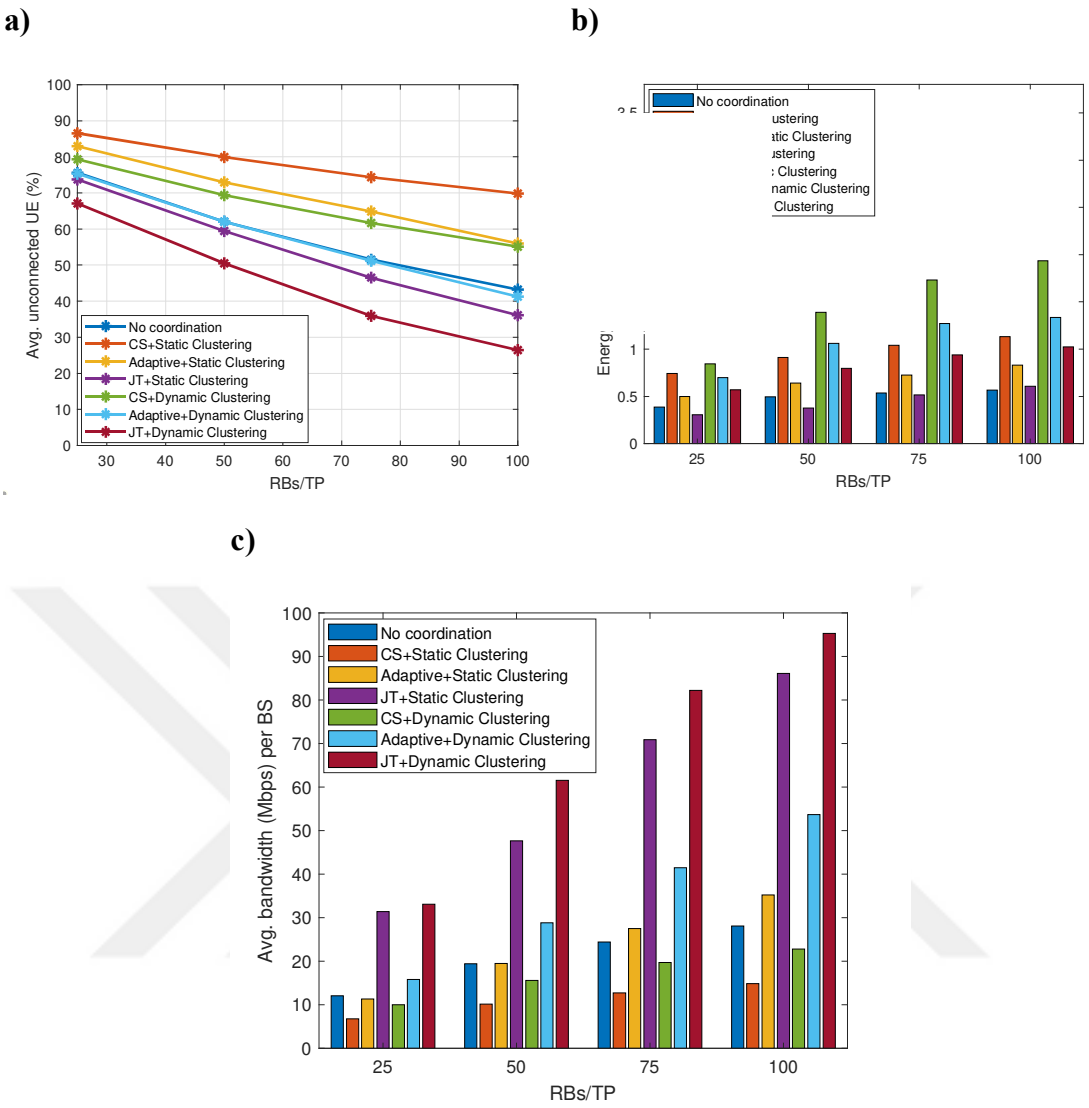

Figure 4.2: Performance comparison of different coordination schemes and clustering approaches when 100% of the UEs use conversational video. (a) Number of unconnected users, (b) Energy efficiency, (c) Average backhaul bandwidth required per TP.

First, it should be noted that the prioritization defined by 5G QoS identifier (5QI) is employed to sort the users and then a network-centric approach is used to maximize the number of connected UEs. Now consider the second scenario (**Figure 4.2**) where 25 RBs are available per TP. If the available backhaul, $BH_\circ$, is limited to 40 Mbps with energy efficiency requirement, $EE_\circ$, of more than 0.5 Mbps/Joule, GCoMP decision mechanism looks at the possible approaches that satisfy the given criteria. In this case, CS with both clustering approaches (Ω_2, Ω_5) and adaptive (Ω_6) and JT (Ω_7) schemes with dynamic clustering are possible candidates. Since

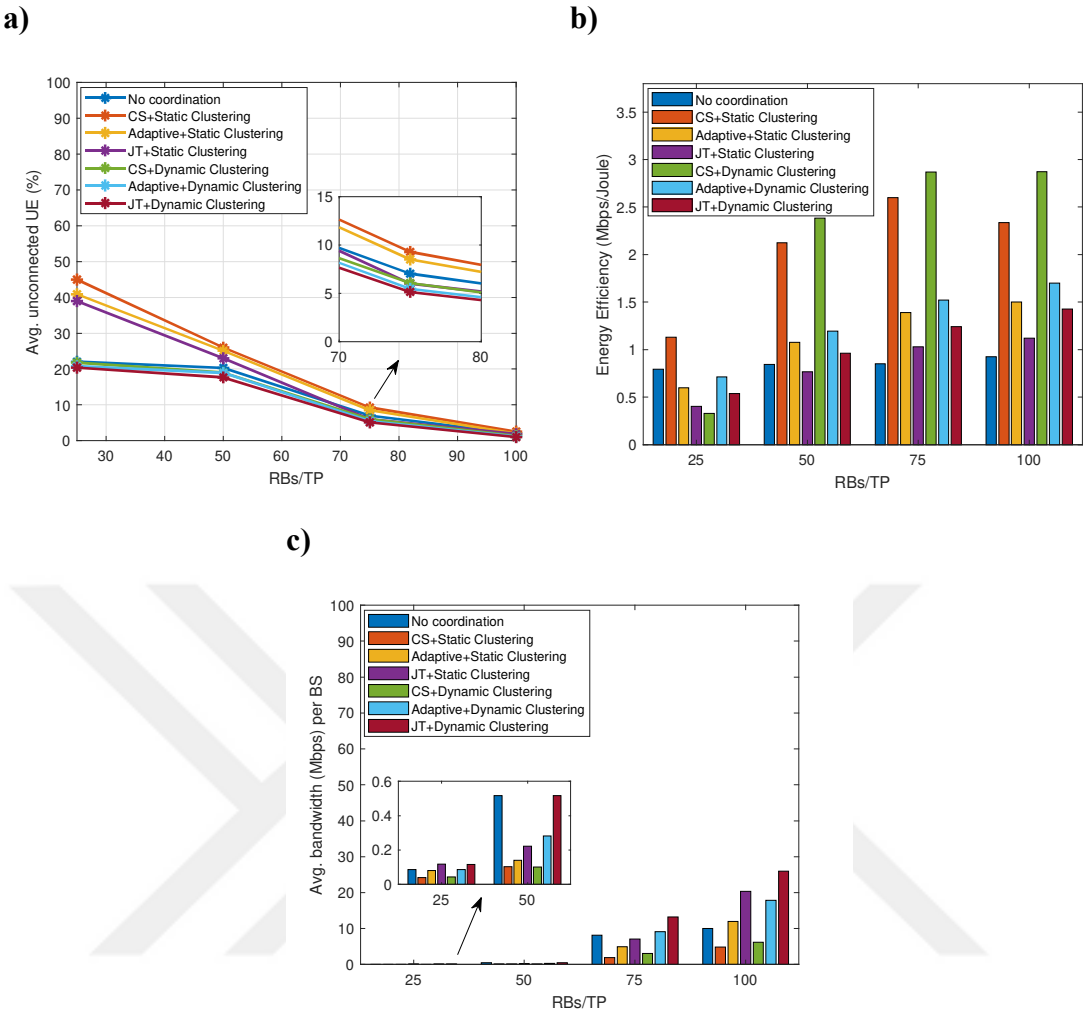

Figure 4.3: Performance comparison of different coordination schemes and clustering approaches when 100% of the UEs use V2X messaging. (a) Number of unconnected users, (b) Energy efficiency, (c) Average backhaul bandwidth required per TP.

the goal is to minimize the number of unconnected devices, JT with dynamic clustering would be chosen, i.e., $\Omega^* = \Omega_7$. Now consider the case where $BH_\circ$ is lowered to 20 Mbps with the same $EE_\circ$. Now the possible candidates include CS with both clustering approaches (H_2, H_5) and adaptive scheme with dynamic clustering (Ω_6). In this case, the latter would be chosen to minimize the number of unconnected users. In case $EE_\circ$ is increased to 0.75 Mbps/Joule, only CS schemes (Ω_2, Ω_5) meet both constraints with dynamic clustering being chosen by the GCoMP framework, i.e., $\Omega^* = \Omega_5$. Given the definite trend in performance, energy efficiency, backhaul, user requirements, and resource availability, it is possible to develop a look-up table kind of strategy that can select Ω^* depending on the distribution of user applications.

Here, we would like to reiterate that this case study and the accompanying simulations present a very simplistic illustration of the proposed GCoMP concept, aimed at providing elementary understanding to the readers. More thorough analysis and contributions, some of which are highlighted below, are required to practically realize such a system in future networks.

4.2. CoMP For Reliability

Since the main contribution of this work is to leverage the difference in large-scale fading characteristics of the aerial and terrestrial channels, we show the achievable SNR for different links and users followed by the same when maximum-ratio combining (MRC) is used to enhance the reliability of the system.

The simulation parameters and assumptions used for all the results presented below are listed in **Table 4.1**. In addition, the obtained results correspond to averaged statistics of Monte Carlo simulations (10,000 trials). Large-scale fading statistics of both TBS 1 and FBS for the network layout presented in **Subsection 3.2.1** are shown in **Figure 4.4**. The dotted lines represent the TBS and the solid lines represent the FBS values. It can be seen that the fading decreases as the height of the FBS increases up to a certain point, after which it stabilizes at first, and then starts increasing. This follows the intuitive explanation that increasing height increases the elevation angle and consequently, the $P(LoS)$, which in turn makes the excessive path loss (η) smaller but after a certain height the distance-dependent path loss becomes more dominant and it offsets the change in η.

It can be clearly seen that the user location has a huge impact on large scale fading for the two different BSs. For instance, in the case of UE 1, TBS consistently remains the better choice in terms of large scale fading. On the other hand, it is visible that for UE 3 FBS provides much less large scale fading as compared to the TBS. This last result may give the impression that FBS are always capable of providing better service to the cell edge user. However, at this point it is imperative to remember the following points regarding FBSs:

- The decrease in fading for FBS would result in increased interference to users of neighboring cells.

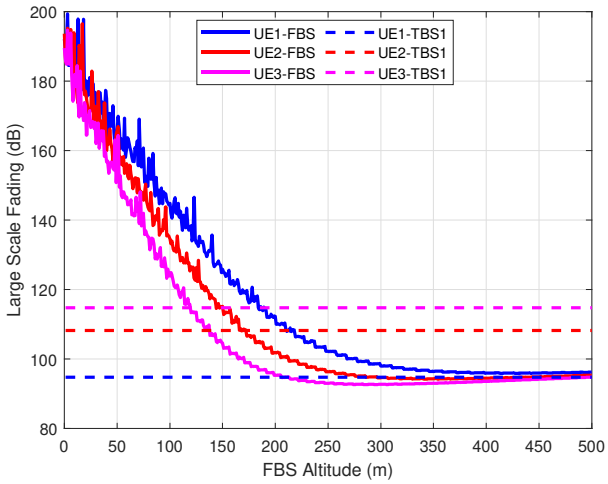

Figure 4.4: Large scale fading comparison between the primary terrestrial base station (TBS1) and flying base station (FBS)

– The FBSs have their own limitations about service provision, the primary one being their power consumption. These FBSs, particularly low-altitude platforms are incapable of staying in the air for more than a few hours [324] and hence unable to provide continuous connectivity.

As far as the interference issue is concerned, it can be mitigated using coordination between the different BSs. This provides the motivation for utilization of centralized control either with CoMP or C-RAN for such hybrid network deployments. Centralized and decentralized interference coordination schemes in a terrestrial/aerial environment are discussed in [325], however, in this case the UAV is considered to be a cellular-connected user.

The power limitation for the FBS, on the other hand, still remains a major issue. While these FBSs can be used to improve the performance in certain scenarios or provide temporary off-loading of the network for maintenance or disaster relief, they are not yet capable of giving full-blown service. Fortunately for us, it is possible to use FBSs intermittently to provide service to mission critical applications like URLLC. This can be done by using diversity combining, as mentioned earlier.

For the purpose of this work, we consider the gain of combining FBS-TBS vs. TBS-TBS in terms of SNR as a measure of the reliability. Having calculated the large scale fading, we calculate the SNR for the users shown in **Figure 3.2** from all BSs. The assumed transmit power, noise spectral density and bandwidth are listed in

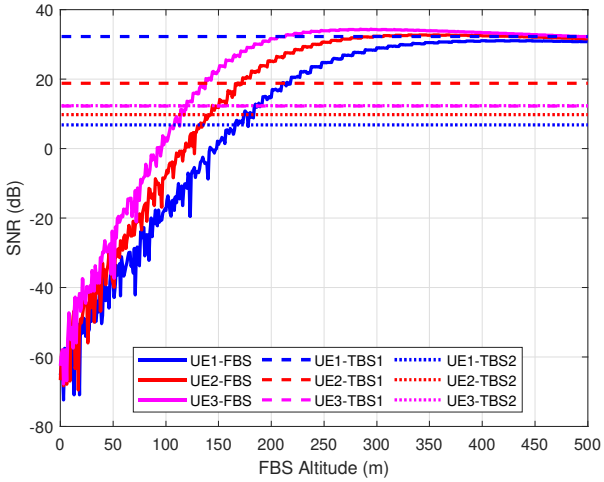

Figure 4.5: SNR comparison between different user-base station links. User link with flying base station (UE-FBS) is shown in blue, link between user and first terrestrial base station (UE-TBS1) is shown in red while user and second terrestrial base station link is shown in cyan (UE-TBS2)

Table 4.1. **Figure 4.5** shows the SNR for different UE-BS links. It can be seen that FBS provides considerably better SNR than the TBS links for UEs 2 and 3, which allows us to intuitively expect that TBS1-FBS combining would give much better combined performance than TBS1-TBS2 combination. The resultant output SNR after MRC is calculated according to **(3.17)** as shown in **Figure 4.6**. As expected the TBS1-FBS link provides the most significant gain for cell-edge user (UE3). TBS1-TBS2 combination improves the SNR by ~3dB while the TBS1-FBS link provides an improvement of ~22dB. For the case of the cell center user (UE1), it is shown that neither of the combining techniques provide any significant advantage. It clearly shows that an adaptive implementation of the combining depending on the user location would both, benefit the user in terms of received SNR (at cell-edge) and save computational and energy costs (in cell-center).

4.3. CoMP For Physical Layer Security (PLS)

The threats to wireless communication are a function of its context including the location of the node, time of day, propagation environment, etc [326]. Intuitively, urban environment poses the most serious threats due to the increased likelihood of having untrustable/eavesdropping nodes in the vicinity of the legitimate receiver. Accordingly, an urban macro environment is assumed for performance evaluation

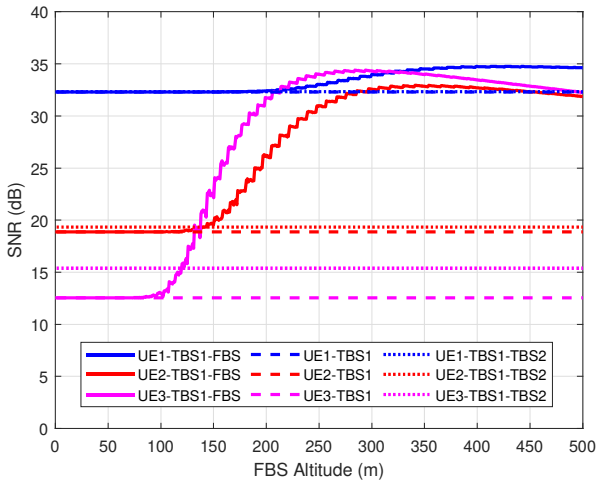

Figure 4.6: SNR comparison with and without MRC combining. Blue, red and cyan colors represent UE1, UE2 and UE3, respectively. The solid lines are the results for MRC combining of TBS1 and FBS, dotted lines are obtained after combining both TBS links while the dashed line represents SNR without any combining

of the proposed approach where we use the tapped delay line (TDL)-model A to represent the delay spread, which is scaled to represent a normal delay profile at the carrier frequency, $f_c = 2$ GHz according to [306]

$$\tau_l^{\text{scaled}} = \tau_l^{\text{model}} \,.\, \text{DS}^{\text{desired}}, \tag{4.1}$$

where τ_l^{model} is the normalized delay of the l-th multipath component, and $\text{DS}^{\text{desired}}$ shows the scaling parameter for the desired environment and frequency. For $\text{DS}^{\text{desired}} = 363$, the maximum excess delay $\tau_L^{\text{scaled}} = 3.5\mu$s. In accordance with fifth generation (5G)'s flexible numerology structure, we assume subcarrier spacing, Δf, to be 30 kHz, fast Fourier transform (FFT)-size, $N = 2048$ and cyclic prefix (CP) duration, $T_{cp} = 2.34\mu$s [327]. Since the maximum delay spread is larger than the CP duration, we use maximum shortening signal-to-noise ratio (MSSNR) channel shortening filter (CSF) to reduce the effective channel impulse response (CIR) length for Bob. These and other simulation parameters are summarized in **Table 4.2**.

Figure 4.7 and **Figure 4.8** illustrate the performance of the proposed algorithm in terms of achievable and secrecy capacities, respectively. Note that secrecy capacity (C_s) is defined as the difference between the capacities of Bob and Eve, i.e., [328]

$$C_s = C_b - C_e. \tag{4.2}$$

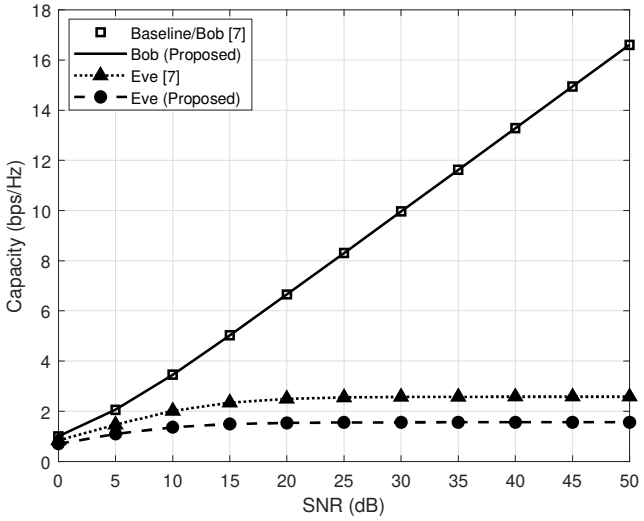

Figure 4.7: Performance comparison of the proposed approach with channel shortening [2], and baseline OFDM in terms of achievable capacity at Bob and Eve in normal, single TP-based channel shortening and proposed approaches.

It can be seen in **Figure 4.7** that the performance of Bob in both cases ([2] and proposed) is similar to the baseline orthogonal frequency division multiplexing (OFDM) since we assume the same cumulative received power in all cases to ensure a fair comparison. On the other hand, Eve's performance is degraded in the proposed approach compared to [2] since the former includes interference from both links according to **(3.22)** and **(3.23)**. It can be seen that the achievable capacity of Bob increases with increase in SNR, while Eve's capacity becomes almost stable after SNR of 20 dB for both proposed and [2]'s approaches. This also results in a continuously increasing secrecy capacity, as shown in **Figure 4.8**. From here, it might be tempting to consider using the proposed approach for high SNR region, however, its performance at lower SNR values (10 and 15 dBs) is also promising. At these SNR values, the proposed approach provides secrecy capacities of 2.09 and 3.54 bps/Hz compared to 1.44 and 2.68 bps/Hz for [2] where Bob's own capacity is 3.45 and 5.02 bps/Hz, respectively. In other words, the proposed approach provides a secrecy capacity that is between 60% and 70% of Bob's capacity while the corresponding numbers for [2] are 41% and 53%, illustrating a gain of around 20% when the proposed approach is used. On the other hand, this gain reduces to about 10% when we consider a higher SNR value of 30 dB.

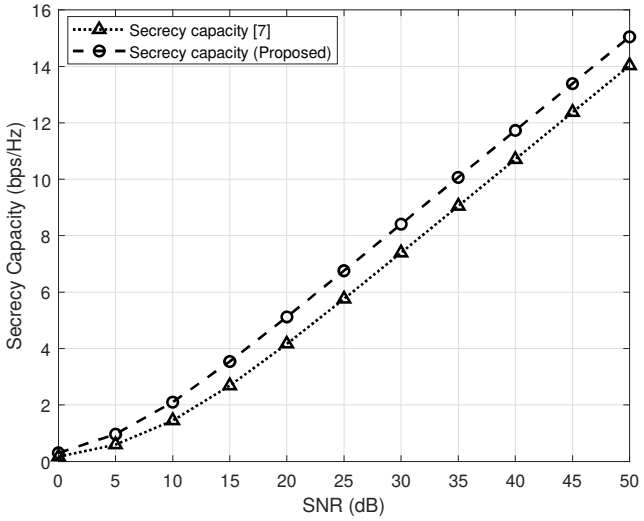

Figure 4.8: Comparison of secrecy capacity between the proposed approach and [2].

4.4. Secure Communication In The Presence Of Eavesdropping Relays

As mentioned earlier, this work considers the presence of a single antenna source, destination, and relay nodes in an urban macro environment. As the ratio between received data and jamming signals depends heavily on the position of the relay, the following path loss model is used [306]:

$$PL = 22\log_{10}(d) + 20\log_{10}(f_c) + 28 + \sigma, \tag{4.3}$$

where d is the distance between the transceivers in meters, f_c is the carrier frequency in GHz, and σ represents the shadow fading modeled as a zero-mean log-normal distribution. The source and destination nodes are assumed to be 1 km apart, with the relay occupying possible positions at multiples of 100 m from them. The transmission power of both source and relay is selected as 23 dBm, which is typical of a cellular UE. Each link experiences a slow Rayleigh fading channel, with an exponentially decaying power delay profile containing a CIR of $L = 32$ taps, which is also the length of the CP used (unless mentioned otherwise). Perfect synchronization and channel estimation are assumed for all links. Noise power spectral density (PSD), N_0, is taken to be -174 dBm/Hz. The simulation results are averaged over 5000 OFDM blocks, where each block contains 256 Quadrature Phase

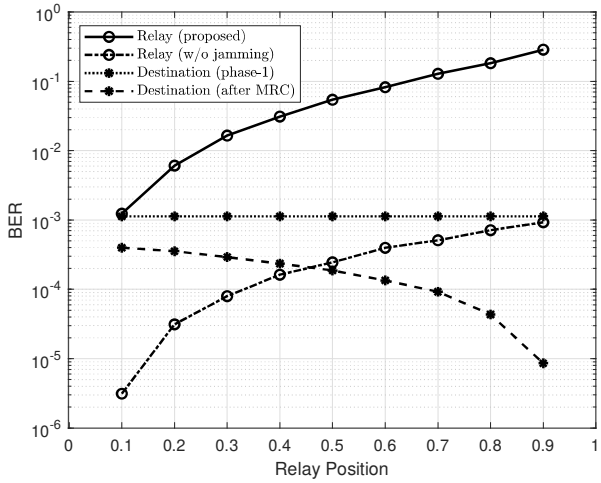

Figure 4.9: BER performance comparison of relay and destination. Relay's performance is seen to be degraded severely with the proposed CP jamming scheme.

Shift Keying (QPSK) symbols. A summary of these simulation parameters is provided in Table **Table 4.3**. It should be highlighted that even though secrecy capacity/outage are popular metrics in physical layer security (PLS), they are limited in practice since they do not take into consideration the receiver structure, transmission parameters or the channel conditions [55]. Accordingly, we opt to use *security gap* in this work, which is quantified in terms of the difference of the BERs observed by Bob and Eve.

Figure 4.9 shows the performance of relay and destination nodes in terms of BER. This is used to represent the *security gap*, which is quantified by the gap in error rates (bit, symbol, packet, etc.) of the legitimate and illegitimate receivers [55]. The horizontal axis represents the position of the relay, where zero is the location of the source itself, while 1 represents the location of the destination. For this simulation, both data and jamming signals are assumed to have the same power levels (23 dBm). The two curves for relay represent the two cases of normal relay operation (without jamming) and with the proposed jamming approach, respectively, while the curves for destination represent its performance in phase-1 (where it only receives the broadcast signal from the source) and when it applies MRC to the two copies received via source and relay. It can be seen that the relay's performance is significantly better than the destination when neither jamming nor combining is performed. This is simply due to the physical closeness of the relay to the source, and the consequent decrease in path loss. It is shown in [329] that distance-based

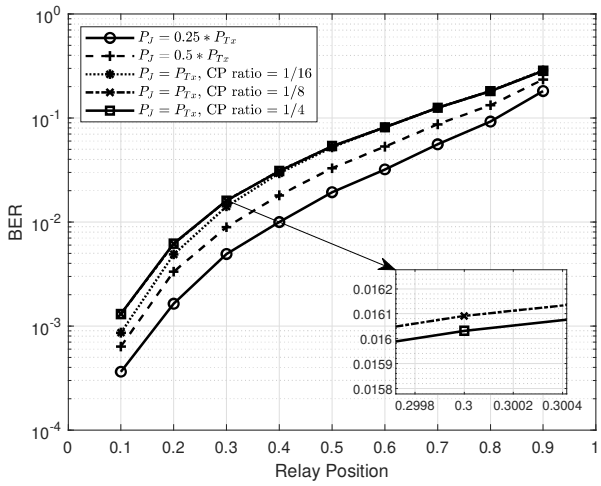

Figure 4.10: Effect of jamming power and CP duration.

cooperative protocol selects the relay closest to the destination as the optimal one. Our results also re-iterate this, as the performance of destination after MRC is significantly improved when the relay moves closer to it. The proposed algorithm also increases the BER of the untrusted relay at this point, leading to an increased security gap.

The interception capability of the eavesdropping relay depends on the jamming signal received. Accordingly, we look at the effect of different power levels of the jamming signals (P_J) as well as its different durations, as shown in **Figure 4.10**. For the former, we have considered three cases, i.e., $P_J = [0.25, 0.5, 1] * P_{Tx}$. It can be seen that variation in P_J has a clearly distinguishable effect on the relay's BER. For instance, when the relay is at the middle of the source and destination nodes, its BER goes from 0.019 to 0.05 as P_J increases from $0.25 * P_{Tx}$ to P_{Tx}. To see the effect of the length of the jamming signal, we looked at three cases where both the length of CP and jamming were varied, i.e., CP ratios of $1/16, 1/8, 1/4$ were used (which were kept equal to CIR itself). It is observed that the length of the jamming signal itself has no visible effect on the BER performance. This observation also encourages us to use the minimum possible CP length in the system without compromising on the security performance of the proposed algorithm.

4.5. Delay-Doppler Based Key Generation In V2X Communication

The performance of the proposed approach is evaluated in terms of KMR and secret key capacity as shown in **Figure 4.11**. Since our focus is on evaluating the key performance, we consider transmission of 10^4 orthogonal time-frequency space (OTFS) frames comprising only the pilot and guards with a grid size of $M = l_{max} = N = 2k_{max} = 32$, in a 4-tap doubly dispersive channel at 5.9 GHz. Note that, for data transmission, grid dimensions $N = 128, M = 1024$ can be used which lead to the same guards (as in our simulations) for the channel model given in [322]. KMR between Alice and Bob as a function of SNR_p and Δ is shown in **Figure 4.11a** and the simulated results for both delay and Doppler show harmony with the theoretical ones (plotted for $\Delta = 0.5$). KMR decreases between Alice and Bob when delay indices are also incorporated, but it increases as Δ is reduced, with $\Delta = 0.5, 0.25, 0.125$ giving KMR values of 1.3×10^{-3}, 2.8×10^{-3}, and 5.9×10^{-3} respectively at $\text{SNR}_p = 40$ dB. However, it should be kept in mind that smaller Δ leads to a larger key generation rate (KGR) per **(3.34)**. **Figure 4.11b** shows the KMR results for Eve. For the uncorrelated case, the KMR lies between 0.47 and 0.49 irrespective of the values of SNR_p or Δ. Even with highly correlated Eve ($\rho = 0.999$), Eve's KMR does not go below 0.24 which is due to the independent instantaneous variation in the velocity (and resultant Doppler shift).

The upper and lower bounds for secret key capacity are plotted in **Figure 4.11c** according to **(4.2)** for different values of Δ. For comparison with [133], the case of one OFDM RB, i.e., $l_{max} = M = 12$ subcarriers and $N = 7$ symbols is also shown. While [133] yields a secret key rate of ≈ 0.8 bits/RB, the proposed approach provides between 9 and 18 bits for the same resources using a single-antenna system. Moreover, the randomness of generated key is evaluated using National Institute of Standards and Technology (NIST)'s statistical suite. **Table 4.4** summarizes the results of the applicable tests for 100 sequences that were 100-bit long. For each of these tests, the number of successful sequences is expected to be ≈ 96 [330]. Some tests, such as random excursion are not included since they lack specific success criteria.

Here it should be pointed out that the generated/shared key is used in various ways

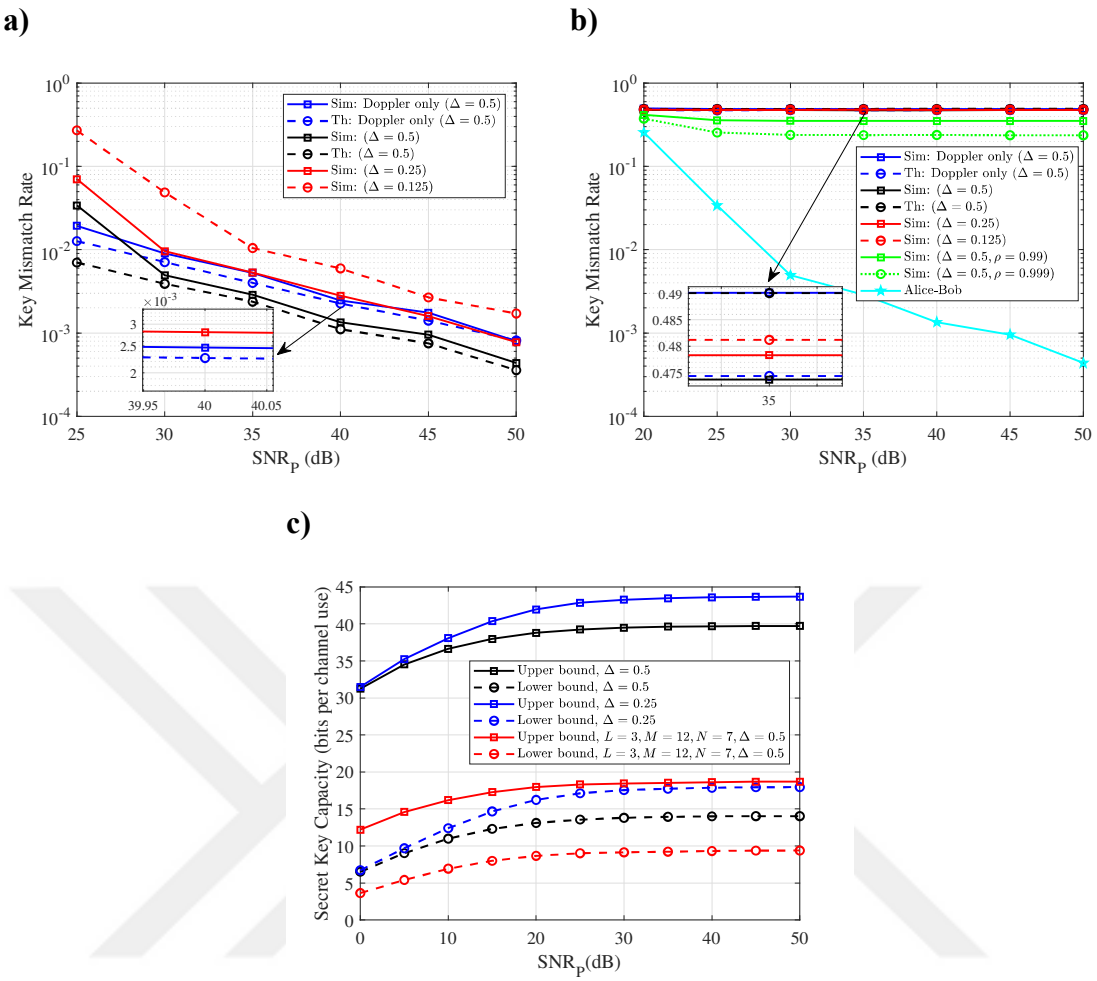

Figure 4.11: Performance analysis of the proposed scheme. (a) KMR between Alice and Bob as a function of SNR for different values of Δ. (b) KMR comparison between Bob and Eve as a function of ρ and Δ. (c) Secret key capacity for different values of L and Δ.

including constellation rotation, artificial interference/noise injection, or as spreading sequence for protection against jamming, etc. For more details about how these can be utilized, we refer the reader to Section IV-D of [55] and references within.

Table 4.1: Simulation parameters for hybrid aerial-terrestrial network in support of uRLLC

Parameter	Value
Environment	Urban
Inter-site distance	500m
f_c	2GHz
h_{TBS}	30m
h_{FBS}	Up to 500m
$\eta_{LoS} \mid \eta_{NLoS}$	1dB | 20dB
$\alpha_{LoS} \mid \alpha_{NLoS}$	2.8 | 3.3
$\beta_{LoS} \mid \beta_{NLoS}$	11.4dB | 17.6dB
$\gamma_{LoS} \mid \gamma_{NLoS}$	2.3 | 2.0
$\sigma_{LoS} \mid \sigma_{NLoS}$	4.1dB | 9.9dB
Noise spectral density N_0	-174dBm/Hz
Transmit Power (TBS and FBS)	23dBm
Bandwidth	10MHz

Table 4.2: Simulation parameters and assumptions for spatially distributed channel shortening

Parameter	Value
Simulation environment	Urban macro
Channel model	TDL-A
Number of coordinating TPs, (K)	2
Carrier frequency (f_c)	2 GHz
FFT size (N)	2048
Subcarrier spacing (Δf)	30 kHz
CP duration (T_{cp})	2.34 μs
Delay spread scaling factor (DS)	363
Desired effective CIR length	2.34 μs (= T_{cp})
Sample interval (T_s)	16.27 ns (= $1/N.\Delta f$)

Table 4.3: Simulation parameters and assumptions for CP jamming against eavesdropping relays in OFDM systems

Parameter	**Value**
Simulation environment	Urban macro
Carrier frequency (f_c)	2 GHz
Shadow fading standard deviation (σ)	4 dB
Source/relay transmit power (P_{Tx})	23 dBm
Noise power density (N_0)	-174 dBm/Hz
Source-destination distance	1000 m
Source-relay distance	(100, 200, ... , 900) m
CIR length (L)	32
Modulation	QPSK
FFT Size (N)	256

Table 4.4: Proportion of sequences successful in NIST randomness tests

Test Name	**No. of Successful Sequences**
Frequency	100/100
Block frequency	100/100
Cumulative sums	100/100
Runs	100/100
Longest run	100/100
FFT	99/100
Non-overlapping template	100/100
Approximate entropy	100/100
Serial	99/100

CHAPTER 5

5. CHALLENGES AND RESEARCH DIRECTIONS

This chapter looks at some of the challenges associated with the contributions of the thesis, i.e., coordinated multipoint (CoMP) and physical layer security (PLS).

5.1. Challenges For (Generalized) Coordinated Multipoint

There are considerable challenges that need to be overcome in order to make generalized CoMP (GCoMP) a reality. Some of these issues are illustrated in **Figure 5.1** and discussed below:

- Owing to the diversity of future wireless networks both in terms of user/application requirements and device/node capabilities, optimized resource allocation is going to become even more challenging [331]. Multi-objective optimization is, therefore, going to be imperative. This also includes the need for improved network slicing capabilities which will be necessary to support future applications [332].

- The spatial diversity afforded by the geographical separation between transmission points (TPs) can be utilized to provide capacity, security, and reliability gains. However, all of these are competing objectives which means one can only be achieved if the others are waived. Optimizing these trade-offs remains a challenge. This might also require multi-objective resource optimization.

- In this work, we have assumed that all the coordinating entities in the network are capable of supporting all clustering approaches and CoMP schemes. However, there might be a scenario where this is not true. Adapting the

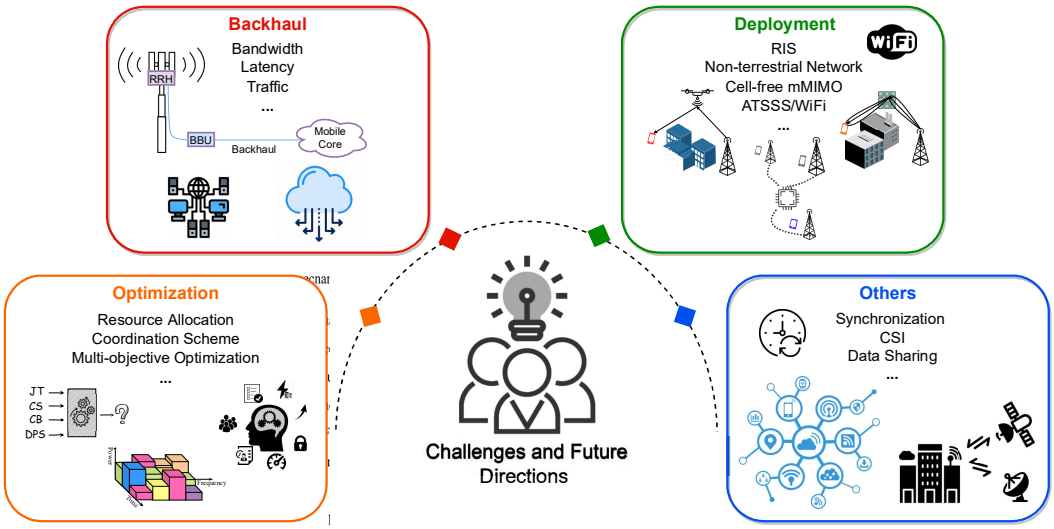

Figure 5.1: Challenges and future directions

GCoMP decisions to accommodate such scenarios remains an open challenge. Moreover, here we have only focused on the backhaul bandwidth and energy considerations in terms of added data exchange between TPs. The analysis in terms of convergence of the CoMP function on an appropriate time-scale, impact on TP complexity and any impact of the network configuration still needs to be carried out [104].

– For any CoMP scheme, timely exchange of information between cooperating nodes and/or central controller is imperative which has been assumed in this work. However, achieving this can be quite challenging in practical scenarios. This issue has been studied in the context of optical networks from the perspective of coordination controller placement [333] and resource (bandwidth) allocation scheme that prioritizes signaling over data traffic [334]. The impact of this latency on GCoMP specifically, however, remains to be studied and suitable mitigation mechanisms should be developed accordingly.

– Significant efforts are being made to improve the compatibility between different wireless radio access technologies. access traffic steering, switching and splitting (ATSSS) is one such example, which promises not only the coexistence but convergence of non-3rd Generation Partnership Project (3GPP) access networks (such as Wi-Fi) with 3GPP's fifth generation (5G) core network [81]. The upcoming amendment of the Wi-Fi standard, i.e., IEEE

802.11TGbe has introduced multi-access point (AP) coordination concept which is similar to CoMP [335]. Furthermore, coordination is also being considered for the purpose of sensing in 802.11's sensing task group, TGbf [336]. This illustrates the need for developing more efficient coordination mechanisms not only for communications but other aspects of wireless networks as well.

– Even though the discussion around sixth generation (6G) is still in its early stages, it is evident that the next-generation wireless networks demand novel paradigms such as reconfigurable intelligent surface (RIS)-enabled smart radio environments [79] and cell-free massive multiple-input multiple-output (MIMO) systems [337], [338]. It might be interesting to consider incorporation of RISs in a CoMP setting. Not only does the use of multiple RISs provide an opportunity for co-channel interference (CCI) mitigation at cell edges [339], but also coordination can help with the biggest challenge in practical RIS deployment, i.e., channel estimation [340]. Since the introduction of RIS and the associated phase shifts contributed by different elements of the surface affect the channel, it would also have an impact on the channel estimation process. The frequency of the channel estimation would depend on the number of RISs, the number of elements in each surface, and the frequency of their update. This process can be streamlined by the use of a centralized/coordinated control mechanism.

– Some of the major roadblocks towards widespread deployment of CoMP in wireless networks include insufficient backhaul, imperfect channel state information (CSI), and clock synchronization [85]. The limited backhaul issue is addressed by quantizing the CSI and data signals or reducing the number of connected users, which leads to significantly diminished throughput, increased end-to-end latency, and lower user density [341]. While optical technology is extensively used for backhaul, it may not scale with the expected densification of future networks. This has led to a discussion around the usage of millimeter wave (mmWave) for integrated backhaul/fronthaul and access operation [342]. However, in this (especially self-backhauling) case, radio resource management (RRM) becomes critical necessitating the

development of flexible and adaptive resource usage methods.

5.2. Challenges For Physical Layer Security

Despite the fruitful research in PLS era, there is a variety of challenges to be tackled in order to make PLS a reality. In this section, we provide and list several open issues and challenges for future works which are as follows:

- A major roadblock in the practical realization of PLS is the limiting assumptions often made regarding the attacking nodes. This may refer to the processing capabilities of the attacker, the number of antennas, active/passive, or individual/collaborative nature. This fact has slowed both the development of proof-of-concept prototypes and the acceptance of PLS approaches to security in reality [343]. Quite often, the attacker is assumed to be similar to a simple legitimate receiver in the network. While this assumption might be valid to ensure the privacy of wireless links from other users in the network, a malicious *attacker* should be considered to be suitably equipped and capable of smartly switching between different types of attacks based on link quality [344].

- For any observable parameter, reciprocity is imperative which has been assumed in this work. However, achieving this can be quite challenging in practical scenarios. For example, time-division duplexing (TDD) system itself is reciprocal, but the channel estimation results at both ends of the link, which are affected by noise and interference may not be consistent [212]. Therefore, when the observable parameter is not the same at both ends, some information needs to be exchanged between the communicating entities for reciprocity compensation, resulting in the potential risk of observable parameter disclosure.

- 5G and beyond paradigms promise ubiquitous connectivity anytime, anywhere including high-speed scenarios. Mobility (particularly high-speed mobility) brings challenges such as Doppler spreading, selectivity of the channel, low coherence time, increased handovers and authentication overhead [345].

The channel selectivity and shorter coherence duration become a more pronounced problem from a PLS perspective. For instance, in physical (PHY) authentication if the legitimate transmitter and receiver lose their connection for more than coherence time, the channel no longer supports verification of the users [184]. In such cases, the authentication procedures need to be re-evaluated or even re-designed.

– With the increasing popularity of concepts such as cognitive/adaptive PLS and PLS for joint sensing and communication (JSC), it is important (and even imperative in some cases) to devise new metrics to quantify security for next-generation wireless networks. While link-level metrics for communication security have been extensively studied [328], there is limited work on quantifying the security of an environment. For instance, [346] proposes a "secrecy map" which provides average secrecy capacity over the whole space for given positions of legitimate nodes without putting any location constraints on the illegitimate node. Considering the importance being given to sensing in beyond 5G networks, it might be prudent to come up with security metrics that can be extended to cover the security of sensing and communication jointly for the whole environment instead of limiting it to specific scenarios in terms of attackers' and interferers' locations or orientations.

– So far, PLS approaches remain limited to the information theory domain, without practical implementations. A limited number of works have been triggering the practical validation of PLS approaches. For instance, the implementation of two PLS techniques is proposed in [347], namely phase enciphered Alamouti coding (PEAC) and artificial noise. The resulting testbed is very complex though, as well as difficult to replicate and validate. Besides, the implementation is only applicable to a situation where the Shannon capacity of the eavesdropper is exactly half the Shannon capacity of the legitimate receiver. However, a proof-of-concept using off-the-shelf hardware to protect the legitimate communication against mobile eavesdropping is proposed in [348]. This is achieved by leveraging the flexibility and control granularity offered by the relatively new concept of spectrum programming [349], by

which it provides the ability to control and degrade the quality of the eavesdropper's channel by virtually manipulating the connectivity of the legitimate receiver.

CHAPTER 6

6. CONCLUSION AND FUTURE WORK

Having looked at different aspects and realizations of coordinated multipoint (CoMP) and physical layer security (PLS) in the previous chapters, we can draw the following conclusions:

- Fifth generation (5G) was characterized by the introduction of diverse services, applications, and user requirements. The trend of expanding wireless paradigms is set to continue with sixth generation (6G), prompting the need for an intelligent and flexible network that can coordinate its resources to improve the quality of service (QoS) provided to the users. Driven by the realization that presently available techniques are unable to achieve this goal, we have proposed the generalization of CoMP concept. The aim is to expand the scope of CoMP from mere interference management at cell edges to enhancing the throughput, decreasing latency, increasing reliability, improving coverage, and providing seamless connectivity to user equipments (UEs) with varying requirements. To this end, a generalized CoMP framework has been discussed in this thesis, which we believe will prove to be a stepping stone towards the realization of fully coordinated next-generation wireless networks.

- The difference in large-scale fading effects of air-to-ground and ground-to-ground channels can be exploited to improve reliability of communication, enabling ultra-reliable low latency communication (uRLLC) services. Our results have shown that FBS-TBS links indeed provide higher reliability than TBS-TBS links, opening a new direction of research that comprises of hybrid networks targeting different applications for 5G and beyond networks. In

this regard, various optimization problems can be investigated. For instance in case of user cell association, in addition to the received power or channel quality, we can consider the cost of making the selection of the FBS as the serving BS for a particular user. This cost can be related to the the energy consumption of the FBS or the interference it causes to the other cells and their users. Keep in mind that some of the optimization problems pertaining to airborne communication networks already studied in the literature include optimized UAV relay placement [350], cell association and power allocation for cellular UAV to mitigate the interference [325], 3D placement of terrestrial and aerial base stations and the user cell association while considering the backhaul [351], as well as FBS placement for maximum coverage [352].

– Leveraging spatially distributed and coordinated transmission points (TPs) helps mitigate the limitation of the existing shortening-based PLS mechanism [2]. The performance is evaluated in terms of achievable secrecy capacity for both approaches, showing the gains of the proposed approach over the existing scheme. It should be noted that this work provides a rudimentary method (and analysis) of leveraging spatially distributed transmission with channel shortening for security. Further studies are required to fully explore the potential of these two mechanisms in securing communication. In this context, one of the future studies that we believe is highly merited is the analysis of the effect of data splitting mechanisms and its dependence on the number of cooperating TPs in improving security. Furthermore, it might also be worthwhile to look at the performance of the proposed method (and any other mechanisms arriving from it) under different propagation environments, line-of-sight (LoS) assumptions, channel estimation errors, scattering levels, etc.

– The presence of untrusted relays in cooperative communication systems represents a legitimate concern. To address this, we have proposed an approach that involves the transmission of a jamming signal from the destination in the interval while it receives the cyclic prefix (CP) part of the signal. Unlike the conventional solutions which require jamming signals to be transmitted throughout the broadcast phase, the proposed method only requires the signal

to be transmitted for a fraction of it. It should be noted that even though this work focuses on the cooperative communication scenario, specifically untrusted relays, the concept presented in this work is much more general and can be applied to the eavesdropping problem in any orthogonal frequency division multiplexing (OFDM) system. Moreover, in such systems the jamming signal may also corrupt the (blind) synchronization attempted by any illegitimate receiver. Further work can also be carried out to optimize the relay placement and jamming power allocation to maximize the security gap in cooperative systems. Moreover, the proposed technique can be used for secure key exchange between the legitimate nodes in the presence of an untrusted relay. Furthermore, the proposed algorithm can also be applied in cases when there is no direct path between source and destination.

– Providing security in general and PLS in specific is particularly challenging for high-mobility scenarios such as vehicle-to-everything (V2X) communication. Recently, orthogonal time-frequency space (OTFS) has gained traction due to its ability to convert the fast-varying propagation to a slow-varying one using the inverse symplectic Fourier transform (ISFT). This work leverages the same property to propose and evaluate a channel-based key generation method that can be used for frequency-division duplexing (FDD) systems, that generally suffer due to lack of reciprocity. The results show a considerable gap in terms of key mismatch rate (KMR) observed at legitimate versus illegitimate receiver while fulfilling the National Institute of Standards and Technology (NIST)-defined randomness criteria for the key itself. This does not exclude the possibility of using the proposed approach in time-division duplexing (TDD) systems. On the contrary, the TDD system can leverage additional features such as the amplitude/phases of the delay/Doppler channel taps. However, the performance analysis of these considering realistic system parameters (including delay-Doppler (DD) grid design) is left for future studies.

BIBLIOGRAPHY

[1] B. Soret, P. Mogensen, K. I. Pedersen, and M. C. Aguayo-Torres, "Fundamental tradeoffs among reliability, latency and throughput in cellular networks," in *IEEE Globecom Workshops (GC Wkshps)*, 2014, pp. 1391–1396.

[2] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of OFDM systems using channel shortening," in *Proc. IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017, pp. 1–5.

[3] M. Series, "IMT Vision–Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond," ITU Recommendation 2015.

[4] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 28–41, 2019.

[5] A. A. Zaidi, R. Baldemair, H. Tullberg, H. Bjorkegren, L. Sundstrom, J. Medbo, C. Kilinc, and I. Da Silva, "Waveform and numerology to support 5G services and requirements," *IEEE Communications Magazine*, vol. 54, no. 11, pp. 90–98, 2016.

[6] Z. E. Ankarali, B. Peköz, and H. Arslan, "Flexible radio access beyond 5G: A future projection on waveform, numerology, and frame design principles," *IEEE Access*, vol. 5, pp. 18 295–18 309, 2017.

[7] Y. Niu, Y. Li, D. Jin, L. Su, and A. V. Vasilakos, "A survey of millimeter wave communications (mmWave) for 5G: opportunities and challenges," *Wireless Networks*, vol. 21, no. 8, pp. 2657–2676, 2015.

[8] L. Feng, R. Q. Hu, J. Wang, P. Xu, and Y. Qian, "Applying VLC in 5G networks: Architectures and key technologies," *IEEE Network*, vol. 30, no. 6, pp. 77–83, 2016.

[9] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78 729–78 757, 2019.

[10] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6G era: Challenges and opportunities," *IEEE Network*, 2020.

[11] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116 753–116 773, 2019.

[12] R. Irmer, J. Droste, P. Marsch, M. Grieger, G. Fettweis, S. Brueck, H.-P. Mayer, L. Thiele, and V. Jungnickel, "Coordinated Multipoint: Concepts, Performance, and Field Trial Results," *IEEE Communications Magazine*, vol. 49, no. 2, pp. 102–111, 2011.

[13] M. Grieger, P. Marsch, Z. Rong, and G. Fettweis, "Field trial results for a coordinated multi-point (CoMP) uplink in cellular systems," in *2010*

International ITG Workshop on Smart Antennas (WSA). IEEE, 2010, pp. 46–51.

[14] X. Li, Q. Cui, Y. Liu, and X. Tao, "An effective scheduling scheme for CoMP in heterogeneous scenario," in *IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications-(PIMRC)*, 2012, pp. 870–874.

[15] J. P. Pérez, F. Riera-Palou, and G. Femenias, "Combining fractional frequency reuse with coordinated multipoint transmission in MIMO-OFDMA networks," in *2013 IFIP Wireless Days (WD)*. IEEE, 2013, pp. 1–8.

[16] D. Lee, H. Seo, B. Clerckx, E. Hardouin, D. Mazzarese, S. Nagata, and K. Sayana, "Coordinated multipoint transmission and reception in LTE-Advanced: Deployment scenarios and operational challenges," *IEEE Communications Magazine*, vol. 50, no. 2, pp. 148–155, 2012.

[17] Q. Zhang and C. Yang, "Transmission mode selection for downlink coordinated multipoint systems," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 1, pp. 465–471, 2013.

[18] A. Khlass, T. Bonald, and S. E. Elayoubi, "Analytical modeling of downlink CoMP in LTE-advanced," in *IEEE 81st Vehicular Technology Conference (VTC Spring)*, 2015, pp. 1–5.

[19] W. Sun and J. Liu, "2-to-*m* coordinated multipoint-based uplink transmission in ultra-dense cellular networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8342–8356, 2018.

[20] J. Giese and M. A. Amin, "Performance upper bounds for coordinated beam selection in LTE-Advanced," in *IEEE International ITG Workshop on Smart Antennas (WSA)*, 2010, pp. 280–285.

[21] C.-H. Liu and P.-C. Chen, "Load-aware coordinated multipoint joint transmission in dense heterogeneous networks: Downlink coverage and throughput limits," in *IEEE International Conference on Communications (ICC)*, 2017, pp. 1–7.

[22] F. Ghods, A. Fapojuwo, and F. Ghannouchi, "Throughput reliability analysis of cloud-radio access networks," *Wireless Communications and Mobile Computing*, vol. 16, no. 17, pp. 2824–2838, 2016.

[23] D. Maladi, *How can CoMP extend 5G NR to high capacity and ultra-reliable communications?*, accessed July 3, 2023. [Online]. Available: https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/comp_webinar_v18.pdf

[24] W. Luo, R. Zhang, and X. Fang, "A CoMP soft handover scheme for LTE systems in high speed railway," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, pp. 1–9, 2012.

[25] M. Boujelben, S. B. Rejeb, and S. Tabbane, "A novel green handover self-optimization algorithm for LTE-A/5G HetNets," in *IEEE International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2015, pp. 413–418.

[26] R. R. Ahmed and D. D. Kouvatsos, "An Efficient CoMP-based Handover Scheme for Evolving Wireless Networks," *Electronic Notes in Theoretical Computer Science*, vol. 340, pp. 85–99, 2018.

[27] A. B. Shams, M. R. Meghla, M. Asaduzzaman, and M. F. Hossain, "Performance of Coordinated Scheduling in Downlink LTE-A under User Mobility," in *IEEE 4th International Conference on Electrical Engineering and Information & Communication Technology (iCEEiCT)*, 2018, pp. 215–220.

[28] C.-C. Lin, K. Sandrasegaran, and Z. Xu, "Performance testing of CoMP handover algorithms in LTE-Advanced," in *Workshop on Advances in Real-time Information Networks*, 2013.

[29] C.-Y. Lin, K.-C. Chen, D. Wickramasuriya, S.-Y. Lien, and R. D. Gitlin, "Anticipatory mobility management by big data analytics for ultra-low latency mobile networking," in *IEEE International Conference on Communications (ICC)*, 2018, pp. 1–7.

[30] M. Khoshnevisan, V. Joseph, P. Gupta, F. Meshkati, R. Prakash, and P. Tinnakornsrisuphap, "5G industrial networks with CoMP for URLLC and time sensitive network architecture," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 4, pp. 947–959, 2019.

[31] F. Salah *et al.*, "Multi-TRxPs for Industrial Automation with 5G URLLC Requirements," 2018.

[32] C. Li, J. Li, P. Gupta, H. Wang, and K. G. Hampel, "Transmission/reception point (TRP) selection for retransmissions in a coordinated multipoint network," Jul. 25 2019, US Patent App. 16/255,665.

[33] V. Joseph and M. Khoshnevisan, "Cluster-set determination for CoMP based on reliability and delay budget in URLLC," Sep. 12 2019, US Patent App. 16/294,080.

[34] V. Hytönen, Z. Li, B. Soret, and V. Nurmela, "Coordinated multi-cell resource allocation for 5G ultra-reliable low latency communications," in *IEEE European Conference on Networks and Communications (EuCNC)*, 2017, pp. 1–5.

[35] E. Katranaras, M. A. Imran, and M. Dianati, "Energy-aware clustering for multi-cell joint transmission in LTE networks," in *IEEE International Conference on Communications Workshops (ICC)*, 2013, pp. 419–424.

[36] Y. Li, Y. Ma, Y. Wang, and W. Zhao, "Base station sleeping with dynamical clustering strategy of CoMP in LTE-advanced," in *IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, 2013, pp. 157–162.

[37] D. Zeng, J. Zhang, L. Gu, S. Guo, and J. Luo, "Energy-efficient coordinated multipoint scheduling in green cloud radio access network," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 9922–9930, 2018.

[38] O. Apilo, M. Lasanen, and A. Mämmelä, "Energy-efficient dynamic point selection and scheduling method for intra-cell CoMP in LTE-A," *Wireless Personal Communications*, vol. 86, no. 2, pp. 705–726, 2016.

[39] A. Jahid, A. B. Shams, and M. F. Hossain, "Dynamic point selection CoMP enabled hybrid powered green cellular networks," *Computers & Electrical Engineering*, vol. 72, pp. 1006–1020, 2018.

[40] D. W. K. Ng and R. Schober, "Resource allocation for coordinated multipoint networks with wireless information and power transfer," in *IEEE Global Communications Conference (Globecom)*, 2014, pp. 4281–4287.

[41] W. Sun and J. Liu, "Coordinated multipoint-based uplink transmission in internet of things powered by energy harvesting," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2585–2595, 2018.

[42] M. Hafez, M. Yusuf, T. Khattab, T. Elfouly, and H. Arslan, "Secure spatial multiple access using directional modulation," *IEEE Transactions on Wireless Communications*, vol. 17, no. 1, pp. 563–573, 2017.

[43] C. Wang and Z. Wang, "Signal alignment for secure underwater coordinated multipoint transmissions," *IEEE Transactions on Signal Processing*, vol. 64, no. 23, pp. 6360–6374, 2016.

[44] U. Ozmat, M. F. Demirkol, and M. A. Yazici, "Service-based coverage for physical layer security with multi-point coordinated beamforming," in *IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2020, pp. 1–6.

[45] M. S. J. Solaija, H. Salman, A. B. Kihero, M. İ. Sağlam, and H. Arslan, "Generalized coordinated multipoint framework for 5G and beyond," *IEEE Access*, vol. 9, pp. 72 499–72 515, 2021.

[46] M. S. J. Solaija, S. Doğan, S. Büyükçorak, and H. Arslan, "Hybrid Terrestrial-Aerial Network for Ultra-Reliable Low-Latency Communication," in *IEEE Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2019, pp. 1–6.

[47] M. S. J. Solaija, H. Salman, and H. Arslan, "Enhancing channel shortening based physical layer security using coordinated multipoint," *arXiv preprint arXiv:2109.14346*, 2021.

[48] H. Ahmadi, K. Katzis, M. Z. Shakir, M. Arvaneh, and A. Gatherer, *Wireless Communication and the Pandemic: The Story So Far*, accessed September 9, 2021. [Online]. Available: https://www.comsoc.org/publications/ctn/wireless-communication-and-pandemic-story-so-far

[49] H. M. Furqan, M. S. J. Solaija, H. Türkmen, and H. Arslan, "Wireless communication, sensing, and REM: A security perspective," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 287–321, 2021.

[50] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[51] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," *arXiv preprint arXiv:1804.00200*, 2018.

[52] Q. Qi, X. Chen, C. Zhong, and Z. Zhang, "Physical layer security for massive access in cellular Internet of Things," *Science China Information Sciences*, vol. 63, no. 2, pp. 1–12, 2020.

[53] H. M. Furqan, M. S. J. Solaija, J. M. Hamamreh, and H. Arslan, "Intelligent physical layer security approach for V2X communication," *arXiv preprint arXiv:1905.05075*, 2019.

[54] C. Li, C.-P. Li, K. Hosseini, S. B. Lee, J. Jiang, W. Chen, G. Horn, T. Ji, J. E. Smee, and J. Li, "5G-based systems design for tactile Internet," *Proceedings of the IEEE*, vol. 107, no. 2, pp. 307–324, 2018.

[55] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2018.

[56] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[57] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015.

[58] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 6–11, 2019.

[59] M. S. J. Solaija, H. M. Furqan, Z. E. Ankaralı, and H. Arslan, "Cyclic Prefix (CP) Jamming Against Eavesdropping Relays in OFDM Systems," *arXiv preprint arXiv:2110.09130*, 2021.

[60] M. S. J. Solaija, S. E. Zegrar, and H. Arslan, "Delay-doppler based key generation using otfs," *IEEE Wireless Communications Letters*, 2023.

[61] M. S. J. Solaija, H. Salman, and H. Arslan, "Towards a unified framework for physical layer security in 5G and beyond networks," *IEEE Open Journal of Vehicular Technology*, vol. 3, pp. 321–343, 2022.

[62] V. H. Mac Donald, "Advanced mobile phone service: The cellular concept," *The Bell System Technical Journal*, vol. 58, no. 1, pp. 15–41, 1979.

[63] P. Godlewski, M. Maqbool, M. Coupechoux, and J.-M. Kélif, "Analytical evaluation of various frequency reuse schemes in cellular OFDMA networks," in *Proceedings of the 3rd International Conference on Performance Evaluation Methodologies and Tools*, 2008, pp. 1–10.

[64] C. Kosta, B. Hunt, A. U. Quddus, and R. Tafazolli, "On interference avoidance through inter-cell interference coordination (ICIC) based on OFDMA mobile systems," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 973–995, 2012.

[65] C. Xiong, “Enhanced ICIC for LTE-A HetNet ,” *ZTE Technologies*, vol. 14, no. 1, pp. 7–9, 2012.

[66] 3rd Generation Partnership Project (3GPP), “Coordinated Multi-point Operation for LTE Physical Layer Aspects (Rel-11) ,” Technical Report 36.819, ver 11.2.0, Sept. 2013.

[67] ——, “Coordinated Multi-point Operation for LTE with Non-ideal Backhaul (Rel-12) ,” Technical Report 36.874, ver 12.0.0, Dec. 2013.

[68] A. Roessler, J. Schlienz, S. Merkel, and M. Kottkamp, “LTE-Advanced (3GPP Rel. 12) Technology Introduction White Paper,” *Rohde & Schwarz*, 2015.

[69] 3rd Generation Partnership Project (3GPP), “Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall Description; Stage 2 (Rel-16) ,” Technical Specification 36.300, ver 16.1.0, Mar. 2020.

[70] ——, “Study on further enhancements to Coordinated Multi-Point (CoMP) Operation for LTE (Rel-14) ,” Technical Report 36.741, ver 14.0.0, Mar. 2017.

[71] ——, “Study on New Radio Access Technology: Radio Access Architecture and Interfaces (Rel-14) ,” Technical Report 38.801, ver 14.0.0, Mar. 2017.

[72] ——, “Study on CU-DU lower layer split for NR (Rel-15) ,” Technical Report 38.816, ver 15.0.0, Dec. 2017.

[73] G. R. MacCartney and T. S. Rappaport, “Millimeter-wave base station diversity for 5G coordinated multipoint (CoMP) applications,” *IEEE Transactions on Wireless Communications*, vol. 18, no. 7, pp. 3395–3410, 2019.

[74] 3rd Generation Partnership Project (3GPP), “Enhancements on MIMO for NR,” Work Item Description RP-182863, Dec. 2018.

[75] ——, “NR-based Access to Unlicensed Spectrum,” Work Item Description RP-191575, Jun. 2019.

[76] ——, “Study on NR-based access to unlicensed spectrum (Rel-16) ,” Technical Report 38.889, ver 16.0.0, Dec. 2018.

[77] N. Men and O. Bonaventure, “MPTCP: Opening the way for convergence in the 5G era - White Paper,” *Tessares*, 2019.

[78] F. Tariq, M. R. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, “A speculative study on 6G,” *IEEE Wireless Communications*, vol. 27, no. 4, pp. 118–125, 2020.

[79] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, “What should 6G be?” *Nature Electronics*, vol. 3, no. 1, pp. 20–29, 2020.

[80] H.-S. Park, Y. Lee, T.-J. Kim, B.-C. Kim, and J.-Y. Lee, “Handover mechanism in NR for ultra-reliable low-latency communications,” *IEEE Network*, vol. 32, no. 2, pp. 41–47, 2018.

[81] Olivier Bonaventure and SungHoon Seo, *Multipath TCP Deployments*, accessed Aug. 9, 2020. [Online]. Available: https://www.ietfjournal.org/multipath-tcp-deployments/

[82] 3rd Generation Partnership Project (3GPP), "Release 15 Description; Summary of Rel-15 Work Items (Rel-15) ," Technical Report 21.915 , ver 15.0.0, Sep. 2019.

[83] J. Rao and S. Vrzic, "Packet duplication for URLLC in 5G dual connectivity architecture," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2018, pp. 1–6.

[84] F. Mezghani, P. Kortoçi, N. Mitton, and M. Di Francesco, "A multi-tier communication scheme for drone-assisted disaster recovery scenarios," in *IEEE Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2019, pp. 1–6.

[85] F. Qamar, K. B. Dimyati, M. N. Hindia, K. A. B. Noordin, and A. M. Al-Samman, "A comprehensive review on coordinated multi-point operation for LTE-A," *Computer Networks*, vol. 123, pp. 19–37, 2017.

[86] K.-C. Chen, T. Zhang, R. D. Gitlin, and G. Fettweis, "Ultra-low latency mobile networking," *IEEE Network*, vol. 33, no. 2, pp. 181–187, 2018.

[87] M. A. Habibi, M. Nasimi, B. Han, and H. D. Schotten, "A comprehensive survey of RAN architectures toward 5G mobile communication system," *IEEE Access*, vol. 7, pp. 70 371–70 421, 2019.

[88] 3rd Generation Partnership Project (3GPP), "Integration of Satellite Access in 5G," Work Item Description SP-180326, Jun. 2018.

[89] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, 2019.

[90] M. S. J. Solaija, H. Salman, H. Arslan, and B. Ozbakis, "Multi-AP Coordination: Recap and Additional Considerations," document IEEE 802.11-20/1713r2 Oct. 2020.

[91] T. Erpek, A. Abdelhadi, and T. C. Clancy, "An optimal application-aware resource block scheduling in LTE," in *IEEE International Conference on Computing, Networking and Communications (ICNC)*, 2015, pp. 275–279.

[92] Z. Xiong, M. Zhang, H. Helmers, M. Baker, P. Godin, and D. Li, "Centralized dynamic point blanking in LTE-advanced network for inter-cell interference mitigation," in *IEEE 81st Vehicular Technology Conference (VTC Spring)*, 2015, pp. 1–5.

[93] O. D. Ramos-Cantor and M. Pesavento, "Decentralized coordinated scheduling with muting in LTE-Advanced networks," in *IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2017, pp. 1–5.

[94] O. D. Ramos-Cantor, J. Belschner, G. Hegde, and M. Pesavento, "Centralized coordinated scheduling in LTE-Advanced networks," *EURASIP*

Journal on Wireless communications and Networking, vol. 2017, no. 1, pp. 1–14, 2017.

[95] R. Agrawal, A. Bedekar, S. Kalyanasundaram, N. Arulselvan, T. Kolding, and H. Kroener, "Centralized and decentralized coordinated scheduling with muting," in *IEEE 79th Vehicular Technology Conference (VTC Spring)*, 2014, pp. 1–5.

[96] K. Shen and W. Yu, "Distributed pricing-based user association for downlink heterogeneous cellular networks," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1100–1113, 2014.

[97] Q. Ye, B. Rong, Y. Chen, M. Al-Shalash, C. Caramanis, and J. G. Andrews, "User association for load balancing in heterogeneous cellular networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2706–2716, 2013.

[98] K. Alexandris, C.-Y. Chang, and N. Nikaein, "Utility-based opportunistic scheduling under multi-connectivity with limited backhaul capacity," *IEEE Networking Letters*, vol. 1, no. 2, pp. 80–83, 2019.

[99] E. Bjornson, E. A. Jorswieck, M. Debbah, and B. Ottersten, "Multiobjective signal processing optimization: The way to balance conflicting metrics in 5G systems," *IEEE Signal Processing Magazine*, vol. 31, no. 6, pp. 14–23, 2014.

[100] 3rd Generation Partnership Project (3GPP), "System architecture for the 5G System (5GS); Stage 2 (Rel-16) ," Technical Specification 23.501, ver 16.5.1, Aug. 2020.

[101] Y. Fang, B. Sun, N. Li, D. Yang, and Z. Han, "Channel Access Category," document IEEE 802.11-20/0468r0 Mar. 2020.

[102] X. Su, L. Li, and P. Zhang, "Interference alignment based hybrid cooperative transmission strategy with limited backhaul," *IET Communications*, vol. 13, no. 1, pp. 45–53, 2018.

[103] S. Bassoy, H. Farooq, M. A. Imran, and A. Imran, "Coordinated multipoint clustering schemes: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 743–764, 2017.

[104] 3rd Generation Partnership Project (3GPP), "Study on Self-Organizing Networks (SON) for enhanced Coordinated Multi-Point (eCoMP) (Rel-15) ," Technical Report 36.742, ver 15.0.0, Jun. 2017.

[105] ——, "Study on physical layer enhancements for NR ultra-reliable and low latency case (URLLC) (Rel-16) ," Technical Report 38.824, ver 1.0.0, Nov. 2018.

[106] ——, "Study on new radio (NR) access technology; Physical layer aspects ," Technical Report 38.802, ver 2.0.0, March. 2013.

[107] T. Jacobsen, R. Abreu, G. Berardinelli, K. Pedersen, P. Mogensen, I. Z. Kovács, and T. K. Madsen, "System Level Analysis of Uplink Grant-free Transmission for URLLC," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2017, pp. 1–6.

[108] D. Jiang, H. Wang, E. Malkamaki, and E. Tuomaala, "Principle and Performance of Semi-persistent Scheduling for VoIP in LTE System," in *Proc. IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCom)*, 2007, pp. 2861–2864.

[109] H. Shariatmadari, Z. Li, M. A. Uusitalo, S. Iraji, and R. Jäntti, "Link Adaptation Design for Ultra-reliable Communications," in *IEEE International Conference on Communications (ICC)*, 2016, pp. 1–5.

[110] J. J. Nielsen, R. Liu, and P. Popovski, "Ultra-reliable low latency communication using interface diversity," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 1322–1334, 2018.

[111] P. Popovski, J. J. Nielsen, C. Stefanovic, E. de Carvalho, E. Strom, K. F. Trillingsgaard, A.-S. Bana, D. M. Kim, R. Kotaba, J. Park *et al.*, "Wireless access for ultra-reliable low-latency communication: Principles and building blocks," *IEEE Netw.*, vol. 32, no. 2, pp. 16–23, 2018.

[112] G. Mountaser *et al.*, "Cloud-RAN in Support of URLLC," in *IEEE Globecom Workshops (GC Wkshps)*, Singapore, Dec. 2017, pp. 1–6.

[113] A. Karimi, K. I. Pedersen, N. H. Mahmood, J. Steiner, and P. Mogensen, "Centralized Joint Cell Selection and Scheduling for Improved URLLC Performance," in *IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2018, pp. 1–6.

[114] C. She, C. Liu, T. Q. Quek, C. Yang, and Y. Li, "UAV-assisted uplink transmission for ultra-reliable and low-latency communications," in *Proc. IEEE International Conference on Communications Workshops (ICC Wkshps)*, 2018, pp. 1–6.

[115] P. J. Melsa, R. C. Younce, and C. E. Rohrs, "Impulse response shortening for discrete multitone transceivers," *IEEE Transactions on Communications*, vol. 44, no. 12, pp. 1662–1672, 1996.

[116] M. Yusuf and H. Arslan, "Secure multi-user transmission using CoMP directional modulation," in *Proc. IEEE 82nd Vehicular Technology Conference (VTC)*, 2015, pp. 1–2.

[117] M. Xu, X. Tao, F. Yang, and H. Wu, "Enhancing secured coverage with CoMP transmission in heterogeneous cellular networks," *IEEE Communications Letters*, vol. 20, no. 11, pp. 2272–2275, 2016.

[118] J. Yao, C. Zhong, Z. Liu, and J. Xu, "3D trajectory optimization for secure UAV communication with CoMP reception," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[119] J. M. Cioffi, "A multicarrier primer," *ANSI T1E1*, vol. 4, pp. 91–157, 1991.

[120] R. K. Martin, M. Ding, B. L. Evans, and C. R. Johnson, "Efficient channel shortening equalizer design," *EURASIP Journal on Advances in Signal Processing*, vol. 2003, no. 13, pp. 1–12, 2003.

[121] Amy Nordum, Kristen Clark and IEEE Spectrum Staff, *Everything You Need to Know About 5G*, accessed Aug. 3, 2020.

[Online]. Available: https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g

[122] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 74–80, 2004.

[123] S. Pahuja and P. Jindal, "Cooperative communication in physical layer security: Technologies and challenges," *Wireless Personal Communications*, vol. 108, no. 2, pp. 811–837, 2019.

[124] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2734–2771, 2018.

[125] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, 2012.

[126] R. Zhao, X. Tan, D.-H. Chen, Y.-C. He, and Z. Ding, "Secrecy performance of untrusted relay systems with a full-duplex jamming destination," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 11 511–11 524, 2018.

[127] S. J. Goldberg, Y. C. Shah, and A. Reznik, "Method and apparatus for performing JRNSO in FDD, TDD and MIMO communications," Mar. 19 2013, US Patent 8,401,196.

[128] X. Wu *et al.*, "A secret key generation method based on CSI in OFDM-FDD system," in *Globecom Workshops (GC Wkshps)*. IEEE, 2013, pp. 1297–1302.

[129] H. Taha and E. Alsusa, "Secret key exchange using private random precoding in MIMO FDD and TDD systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 4823–4833, 2016.

[130] O. Gungor, F. Chen, and C. E. Koksal, "Secret key generation from mobility," in *Globecom Workshops (GC Wkshps)*. IEEE, 2011, pp. 874–878.

[131] A. Badawy *et al.*, "Secret key generation based on AoA estimation for low SNR conditions," in *81st Vehicular Technology Conference (VTC Spring)*. IEEE, 2015, pp. 1–7.

[132] K. Lin, Z. Ji, Y. Zhang, G. Chen, P. L. Yeoh, and Z. He, "Secret key generation based on 3D spatial angles for UAV communications," in *Wireless Communications and Networking Conference (WCNC)*. IEEE, 2021, pp. 1–6.

[133] B. Liu, A. Hu, and G. Li, "Secret key generation scheme based on the channel covariance matrix eigenvalues in FDD systems," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1493–1496, 2019.

[134] G. Li, A. Hu, C. Sun, and J. Zhang, "Constructing reciprocal channel coefficients for secret key generation in FDD systems," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2487–2490, 2018.

[135] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138 406–138 446, 2020.

[136] J. Hu, J. Shi, S. Ma, and Z. Li, "Secrecy analysis for orthogonal time frequency space scheme based uplink LEO satellite communication," *IEEE Wireless Communications Letters*, vol. 10, no. 8, pp. 1623–1627, 2021.

[137] Z. Tie, J. Shi, Z. Li, S. Li, and W. Liang, "Security performance analysis for an OTFS-based joint unicast-multicast streaming system," *IEEE Transactions on Communications*, vol. 70, no. 10, pp. 6764–6777, 2022.

[138] J. Sun, Z. Wang, and Q. Huang, "Secure precoded orthogonal time frequency space modulation," in *13th International Conference on Wireless Communications and Signal Processing (WCSP)*. IEEE, 2021, pp. 1–5.

[139] W. Liang, X. Liu, J. Shi, L. Li, and J. Hu, "Underlying security transmission design for orthogonal time frequency space (OTFS) modulation," *Sensors*, vol. 22, no. 20, p. 7919, 2022.

[140] M. Shakiba-Herfeh, A. Chorti, and H. V. Poor, "Physical layer security: Authentication, integrity, and confidentiality," in *Physical Layer Security*. Springer, 2021, pp. 129–150.

[141] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[142] L. Wang and A. M. Wyglinski, "Detection of man-in-the-middle attacks using physical layer wireless security techniques," *Wireless Communications and Mobile Computing*, vol. 16, no. 4, pp. 408–426, 2016.

[143] P. Hao, X. Wang, and A. Behnad, "Relay authentication by exploiting I/Q imbalance in amplify-and-forward system," in *Global Communications Conference (GLOBECOM)*. IEEE, 2014, pp. 613–618.

[144] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2418–2434, 2010.

[145] N. Xie and S. Zhang, "Blind authentication at the physical layer under time-varying fading channels," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1465–1479, 2018.

[146] G. Chen and W. Dong, "Jamcloak: Reactive jamming attack over cross-technology communication links," in *26th International Conference on Network Protocols (ICNP)*. IEEE, 2018, pp. 34–43.

[147] L. Hao, T. Li, and Q. Ling, "A highly efficient secure communication interface: collision-free frequency hopping (CFFH)," in *Workshop on Signal Processing Applications for Public Security and Forensics*. IEEE, 2007, pp. 1–4.

[148] X. Cheng and B. Huang, "A center-based secure and stable clustering algorithm for VANETs on highways," *Wireless Communications and Mobile Computing*, vol. 2019, 2019.

[149] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[150] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *27th USENIX Security Symposium*, 2018, pp. 15–32.

[151] M. Stanislav and T. Beardsley, "Hacking IoT: A case study on baby monitor exposures and vulnerabilities," *Rapid7 Report*, 2015.

[152] R. F. Schaefer, H. Boche, and H. V. Poor, "Secure communication under channel uncertainty and adversarial attacks," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1796–1813, 2015.

[153] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[154] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2016.

[155] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China communications*, vol. 14, no. 12, pp. 1–14, 2017.

[156] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: Modeling and validation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2091–2106, 2016.

[157] O. Gungor, F. Chen, and C. E. Koksal, "Secret key generation via localization and mobility," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 6, pp. 2214–2230, 2014.

[158] L. Mucchi, S. Caputo, P. Marcocci, G. Chisci, L. Ronga, and E. Panayirci, "Security and reliability performance of noise-loop modulation: Theoretical analysis and experimentation," *IEEE Transactions on Vehicular Technology*, 2022.

[159] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, 2014.

[160] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2022.

[161] W. Li, D. Mclernon, J. Lei, M. Ghogho, S. A. R. Zaidi, and H. Hui, "Cryptographic primitives and design frameworks of physical layer encryption for wireless communications," *IEEE Access*, vol. 7, pp. 63 660–63 673, 2019.

[162] R. Ma, L. Dai, Z. Wang, and J. Wang, "Secure communication in TDS-OFDM system using constellation rotation and noise insertion," *IEEE*

Transactions on Consumer Electronics, vol. 56, no. 3, pp. 1328–1332, 2010.

[163] D. Park, J. Ahn, C. Choe, S. Woo, S. Ahn, and J. Choi, "A Noise-Shaped Signaling Method for Vehicle-to-Everything Security," *IEEE Access*, vol. 9, pp. 75 385–75 397, 2021.

[164] B. Chen, C. Zhu, W. Li, J. Wei, V. C. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.

[165] D. Xu, P. Ren, Q. Du, L. Sun, and Y. Wang, "Physical layer security improvement by constellation selection and artificial interference," in *Wireless Communications and Networking Conference (WCNC)*. IEEE, 2017, pp. 1–6.

[166] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, pp. 25 863–25 875, 2017.

[167] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "New physical layer key generation dimensions: Subcarrier indices/positions-based key generation," *IEEE Communications Letters*, vol. 25, no. 1, pp. 59–63, 2020.

[168] J. M. Hamamreh, Z. E. Ankarali, and H. Arslan, "CP-less OFDM with alignment signals for enhancing spectral efficiency, reducing latency, and improving PHY security of 5G services," *IEEE Access*, vol. 6, pp. 63 649–63 663, 2018.

[169] B. He, Y. She, and V. K. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9577–9581, 2017.

[170] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2599–2612, 2012.

[171] X. Li, H.-N. Dai, M. K. Shukla, D. Li, H. Xu, and M. Imran, "Friendly-jamming schemes to secure ultra-reliable and low-latency communications in 5G and beyond communications," *Computer Standards & Interfaces*, vol. 78, p. 103540, 2021.

[172] M. Yang, B. Zhang, Y. Huang, N. Yang, D. Guo, and B. Gao, "Secure multiuser communications in wireless sensor networks with TAS and cooperative jamming," *Sensors*, vol. 16, no. 11, p. 1908, 2016.

[173] L. Peng, A. Hu, J. Zhang, Y. Jiang, J. Yu, and Y. Yan, "Design of a hybrid RF fingerprint extraction and device classification scheme," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 349–360, 2018.

[174] W. Li, N. Wang, L. Jiao, and K. Zeng, "Physical Layer Spoofing Attack Detection in MmWave Massive MIMO 5G Networks," *IEEE Access*, vol. 9, pp. 60 419–60 432, 2021.

[175] X. Li, K. Huang, S. Wang, and X. Xu, "A physical layer authentication mechanism for IoT devices," *China Communications*, 2021.

[176] Y. An, S. Zhang, and Z. Ji, "A Tag-Based PHY-Layer Authentication Scheme Without Key Distribution," *IEEE Access*, vol. 9, pp. 85 947–85 955, 2021.

[177] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2009.

[178] Q. Wang, H. Zhang, Q. Lyu, X. Wang, and J. Bao, "A Novel Physical Channel Characteristics-based Channel Hopping Scheme for Jamming-resistant in Wireless Communication," *International Journal of Network Security*, vol. 20, no. 3, pp. 439–446, 2018.

[179] G. Noubir, "On connectivity in ad hoc networks under jamming using directional antennas and mobility," in *International Conference on Wired/Wireless Internet Communications*. Springer, 2004, pp. 186–200.

[180] H. Yang, Z. Xiong, J. Zhao, D. Niyato, Q. Wu, H. V. Poor, and M. Tornatore, "Intelligent reflecting surface assisted anti-jamming communications: A fast reinforcement learning approach," *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 1963–1974, 2020.

[181] M. K. Ozdemir and H. Arslan, "Channel estimation for wireless OFDM systems," *IEEE Communications Surveys & Tutorials*, vol. 9, no. 2, pp. 18–48, 2007.

[182] A. B. Kihero, A. Tusha, and H. Arslan, "Wireless Channel and Interference," in *Wireless Communication Signals: A Laboratory-based Approach*. Wiley Online Library, 2021, pp. 267–323.

[183] D. Marabissi, L. Mucchi, and A. Stomaci, "IoT Nodes Authentication and ID Spoofing Detection Based on Joint Use of Physical Layer Security and Machine Learning," *Future Internet*, vol. 14, no. 2, p. 61, 2022.

[184] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, 2015.

[185] H. Khodakarami and F. Lahouti, "Link adaptation for physical layer security over wireless fading channels," *IET Communications*, vol. 6, no. 3, pp. 353–362, 2012.

[186] Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Security and Communication Networks*, vol. 8, no. 2, pp. 332–341, 2015.

[187] L. Y. Paul, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, 2008.

[188] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[189] S. Kundu, D. A. Pados, and S. N. Batalama, "Hybrid-ARQ as a communications security measure," in *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2014, pp. 5681–5685.

[190] J. M. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond," *IEEE Communications Letters*, vol. 21, no. 5, pp. 1191–1194, 2017.

[191] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[192] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571–2579, 2008.

[193] M. K. Samimi, G. R. MacCartney, S. Sun, and T. S. Rappaport, "28 GHz millimeter-wave ultrawideband small-scale fading models in wireless channels," in *83rd Vehicular Technology Conference (VTC Spring)*. IEEE, 2016, pp. 1–6.

[194] E. N. Papasotiriou, A.-A. A. Boulogeorgos, K. Haneda, M. F. de Guzman, and A. Alexiou, "An experimentally validated fading model for THz wireless systems," *Scientific Reports*, vol. 11, no. 1, pp. 1–14, 2021.

[195] Y. Xing, T. S. Rappaport, and A. Ghosh, "Millimeter wave and sub-THz indoor radio propagation channel measurements, models, and comparisons in an office environment," *IEEE Communications Letters*, vol. 25, no. 10, pp. 3151–3155, 2021.

[196] G. D. Durgin, T. S. Rappaport, and D. A. De Wolf, "New analytical models and probability density functions for fading in wireless communications," *IEEE Transactions on Communications*, vol. 50, no. 6, pp. 1005–1015, 2002.

[197] J. D. V. Sánchez, D. P. M. Osorio, F. J. López-Martínez, M. C. P. Paredes, and L. F. Urquiza-Aguiar, "On the secrecy performance over N-wave with diffuse power fading channel," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15 137–15 148, 2020.

[198] J. M. Romero-Jerez, F. J. Lopez-Martinez, J. F. Paris, and A. J. Goldsmith, "The fluctuating two-ray fading model: Statistical characterization and performance analysis," *IEEE Transactions on Wireless Communications*, vol. 16, no. 7, pp. 4420–4432, 2017.

[199] W. Zeng, J. Zhang, S. Chen, K. P. Peppas, and B. Ai, "Physical layer security over fluctuating two-ray fading channels," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8949–8953, 2018.

[200] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy Capacity Analysis Over $\kappa-\mu$ Fading Channels: Theory and Applications," *IEEE Transactions on Communications*, vol. 64, no. 7, pp. 3011–3024, 2016.

[201] S. Iwata, T. Ohtsuki, and P.-Y. Kam, "Secure outage probability over $\kappa-\mu$ fading channels," in *International Conference on Communications (ICC)*. IEEE, 2017, pp. 1–6.

[202] J. M. Moualeu and W. Hamouda, "On the secrecy performance analysis of SIMO systems over $\kappa-\mu$ fading channels," *IEEE Communications Letters*, vol. 21, no. 11, pp. 2544–2547, 2017.

[203] J. D. V. Sánchez, D. P. M. Osorio, F. J. López-Martínez, M. C. P. Paredes, and L. F. Urquiza-Aguiar, "Information-Theoretic Security of MIMO Networks Under $\kappa - \mu$ Shadowed Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 6302–6318, 2021.

[204] J. M. Moualeu, D. B. da Costa, W. Hamouda, U. S. Dias, and R. A. de Souza, "Physical layer security over $\alpha - \kappa - \mu$ and $\alpha - \eta - \mu$ fading channels," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 1025–1029, 2018.

[205] T. R. R. Marins, A. A. Dos Anjos, V. M. R. Peñarrocha, L. Rubio, J. Reig, R. A. A. de Souza, and M. D. Yacoub, "Fading evaluation in the mm-Wave band," *IEEE Transactions on Communications*, vol. 67, no. 12, pp. 8725–8738, 2019.

[206] A. Mathur, Y. Ai, M. R. Bhatnagar, M. Cheffena, and T. Ohtsuki, "On physical layer security of $\alpha - \eta - \kappa - \mu$ fading channels," *IEEE Communications Letters*, vol. 22, no. 10, pp. 2168–2171, 2018.

[207] P. Yadav, S. Kumar, and R. Kumar, "A comprehensive survey of physical layer security over fading channels: Classifications, applications, and challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 9, p. e4270, 2021.

[208] H. Arslan, "RF Impairments," in *Wireless Communication Signals: A Laboratory-based Approach*. Wiley Online Library, 2021, pp. 99–120.

[209] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 92–98, 2019.

[210] P. Hao and X. Wang, "Performance enhanced wireless device authentication using multiple weighted device-specific characteristics," in *China Summit and International Conference on Signal and Information Processing (ChinaSIP)*. IEEE, 2015, pp. 438–442.

[211] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 152–158, 2016.

[212] L. Zhao, X. Zhang, J. Chen, and L. Zhou, "Physical layer security in the age of artificial intelligence and edge computing," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 174–180, 2020.

[213] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Transactions on Communications*, vol. 62, no. 5, pp. 1658–1667, 2014.

[214] M. Karabacak, B. Peköz, G. Mumcu, and H. Arslan, "Arraymetrics: Authentication through chaotic antenna array geometries," *IEEE Communications Letters*, vol. 25, no. 6, pp. 1801–1804, 2021.

[215] L. Afeef, H. M. Furqan, and H. Arslan, "Physical Layer Authentication Scheme in Beamspace MIMO Systems," *IEEE Communications Letters*, 2022.

[216] A. Badawy, T. Elfouly, T. Khattab, A. Mohamed, and M. Guizani, "Unleashing the secure potential of the wireless physical layer: Secret key generation methods," *Physical Communication*, vol. 19, pp. 1–10, 2016.

[217] C. Perkins, L. Lei, M. Kuhlman, T.-H. Lee, G. Gateau, S. Bergbreiter, and P. Abshire, "Distance sensing for mini-robots: RSSI vs. TDOA," in *International Symposium of Circuits and Systems (ISCAS)*. IEEE, 2011, pp. 1984–1987.

[218] A. Badawy, T. Khattab, T. ElFouly, A. Mohamed, and D. Trinchero, "Secret key generation based on channel and distance measurements," in *6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. IEEE, 2014, pp. 136–142.

[219] R. L. Rivest, "Cryptography," in *Handbook of Theoretical Computer Science, Volume A*, J. Van Leeuwen and J. Leeuwen, Eds. Elsevier, 1990, ch. 13, pp. 718–755.

[220] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 48–54, 2019.

[221] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[222] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[223] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Physical layer security designs for 5G and beyond," in *Flexible and Cognitive Radio Access Technologies for 5G and Beyond*, H. Arslan and E. Basar, Eds. IET, 2020, ch. 18, pp. 545–587.

[224] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2016.

[225] Z. Rezki and M.-S. Alouini, "On the finite-SNR diversity-multiplexing tradeoff of zero-forcing transmit scheme under secrecy constraint," in *International Conference on Communications Workshops (ICC)*. IEEE, 2011, pp. 1–5.

[226] M. Pei, L. Wang, and D. Ma, "Linear MMSE transceiver optimization for general MIMO wiretap channels with QoS constraints," in *International Conference on Communications in China (ICCC)*. IEEE, 2013, pp. 259–263.

[227] L. Zhang, Y. Cai, B. Champagne, and M. Zhao, "Tomlinson-Harashima precoding design in MIMO wiretap channels based on the MMSE criterion," in *International Conference on Communication Workshop (ICCW)*. IEEE, 2015, pp. 470–474.

[228] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "MIMO Gaussian broadcast channels with confidential and common messages," in *International Symposium on Information Theory*. IEEE, 2010, pp. 2578–2582.

[229] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *41st Annual Conference on Information Sciences and Systems*. IEEE, 2007, pp. 905–910.

[230] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *International Symposium on Information Theory*. IEEE, 2007, pp. 2471–2475.

[231] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Communications Letters*, vol. 17, no. 7, pp. 1483–1486, 2013.

[232] T. Xiong, W. Lou, J. Zhang, and H. Tan, "MIO: Enhancing wireless communications security through physical layer multiple inter-symbol obfuscation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1678–1691, 2015.

[233] S. Althunibat, V. Sucasas, and J. Rodriguez, "A physical-layer security scheme by phase-based adaptive modulation," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 9931–9942, 2017.

[234] S. E. Zegrar, H. M. Furqan, and H. Arslan, "Flexible physical layer security for joint data and pilots in future wireless networks," *IEEE Transactions on Communications*, vol. 70, no. 4, pp. 2635–2647, 2022.

[235] M. Yusuf and H. Arslan, "Controlled inter-carrier interference for physical layer security in OFDM systems," in *84th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2016, pp. 1–5.

[236] N. Van Huynh, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Jam Me If You Can: Defeating Jammer With Deep Dueling Neural Network Architecture and Ambient Backscattering Augmented Communication," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 11, pp. 2603–2620, 2019.

[237] P. Zhang, J. Liu, Y. Shen, H. Li, and X. Jiang, "Lightweight tag-based PHY-layer authentication for IoT devices in smart cities," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3977–3990, 2019.

[238] K. R. Liu, A. K. Sadek, W. Su, and A. Kwasinski, *Cooperative communications and networking*. Cambridge university press, 2009.

[239] L. Xiao, X. Wan, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1676–1687, 2017.

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

[241] M. Di Renzo, A. Zappone, M. Debbah, M.-S. Alouini, C. Yuen, J. De Rosny, and S. Tretyakov, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2450–2525, 2020.

[242] M. Alayasra and H. Arslan, "IRS-Enabled Beam-Space Channel," *IEEE Transactions on Wireless Communications*, 2021.

[243] A. Almohamad, A. M. Tahir, A. Al-Kababji, H. M. Furqan, T. Khattab, M. O. Hasna, and H. Arslan, "Smart and secure wireless communications via reflecting intelligent surfaces: A short survey," *IEEE Open Journal of the Communications Society*, 2020.

[244] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[245] J. Qiao and M.-S. Alouini, "Secure transmission for intelligent reflecting surface-assisted mmWave and terahertz systems," *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1743–1747, 2020.

[246] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Communications Letters*, vol. 9, no. 6, pp. 778–782, 2020.

[247] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, K. Adhikari, X. Li, M. Quiroz-Castellanos, and R. Kharel, "Reconfigurable intelligent surfaces-enabled vehicular networks: A physical layer security perspective," *arXiv preprint arXiv:2004.11288*, 2020.

[248] M. H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, "Reconfigurable intelligent surfaces-aided physical layer security enhancement in D2D underlay communications," *IEEE Communications Letters*, vol. 25, no. 5, pp. 1443–1447, 2020.

[249] U. Altun and E. Basar, "Ris enabled secure communication with covert constraint," in *55th Asilomar Conference on Signals, Systems, and Computers*. IEEE, 2021, pp. 685–689.

[250] B. Kim, T. Erpek, Y. E. Sagduyu, and S. Ulukus, "Covert communications via adversarial machine learning and reconfigurable intelligent surfaces," *arXiv preprint arXiv:2112.11414*, 2021.

[251] H. Du, J. Kang, D. Niyato, J. Zhang, D. I. Kim *et al.*, "Reconfigurable Intelligent Surface-Aided Joint Radar and Covert Communications: Fundamentals, Optimization, and Challenges," *arXiv preprint arXiv:2203.02704*, 2022.

[252] J. Hu, X. Shi, S. Yan, Y. Chen, T. Zhao, and F. Shu, "Hybrid relay-reflecting intelligent surface-aided covert communications," *arXiv preprint arXiv:2203.12223*, 2022.

[253] G. Li, L. Hu, P. Staat, H. Elders-Boll, C. Zenger, C. Paar, and A. Hu, "Reconfigurable Intelligent Surface for Physical Layer Key Generation: Constructive or Destructive?" *arXiv preprint arXiv:2112.10043*, 2021.

[254] M. H. Yılmaz, E. Güvenkaya, H. M. Furqan, S. Köse, and H. Arslan, "Cognitive security of wireless communication systems in the physical layer," *Wireless Communications and Mobile Computing*, vol. 2017, 2017.

[255] B. Wang and N. Z. Gong, "Stealing hyperparameters in machine learning," in *Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 36–52.

[256] 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 Transactions on Communications*, vol. 68, no. 6, pp. 3834–3862, 2020.

[257] H. Türkmen, M. S. J. Solaija, A. Tusha, and H. Arslan, "Wireless sensing - enabler of future wireless technologies," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 29, no. 1, pp. 1–17, 2021.

[258] D. E. Lawrence, "Low probability of intercept antenna array beamforming," *IEEE Transactions on Antennas and Propagation*, vol. 58, no. 9, pp. 2858–2865, 2010.

[259] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 1004–1015.

[260] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 428–445, 2012.

[261] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M. Di Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1546–1577, 2021.

[262] Y. Zhang, J. Zhang, M. Di Renzo, H. Xiao, and B. Ai, "Reconfigurable Intelligent Surfaces with Outdated Channel State Information: Centralized vs. Distributed Deployments," *IEEE Transactions on Communications*, 2022.

[263] S. Abeywickrama, R. Zhang, Q. Wu, and C. Yuen, "Intelligent reflecting surface: Practical phase shift model and beamforming optimization," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5849–5863, 2020.

[264] Y. Zhang, J. Zhang, M. Di Renzo, H. Xiao, and B. Ai, "Performance analysis of RIS-aided systems with practical phase shift and amplitude response," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4501–4511, 2021.

[265] I. Trigui, W. Ajib, W.-P. Zhu, and M. Di Renzo, "Performance evaluation and diversity analysis of RIS-assisted communications over generalized fading channels in the presence of phase noise," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 593–607, 2022.

[266] E. Björnson and L. Sanguinetti, "Rayleigh fading modeling and channel hardening for reconfigurable intelligent surfaces," *IEEE Wireless Communications Letters*, vol. 10, no. 4, pp. 830–834, 2020.

[267] S. Sun and H. Yan, "Small-scale spatial-temporal correlation and degrees of freedom for reconfigurable intelligent surfaces," *IEEE Wireless Communications Letters*, vol. 10, no. 12, pp. 2698–2702, 2021.

[268] R. Liu, Q. Wu, M. Di Renzo, and Y. Yuan, "A path to smart radio environments: An industrial viewpoint on reconfigurable intelligent surfaces," *IEEE Wireless Communications*, 2022.

[269] S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-wave cellular wireless networks: Potentials and challenges," *Proceedings of the IEEE*, vol. 102, no. 3, pp. 366–385, 2014.

[270] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Physical layer security in large-scale millimeter wave ad hoc networks," in *Global Communications Conference (GLOBECOM)*. IEEE, 2016, pp. 1–6.

[271] V. Petrov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Exploiting multipath terahertz communications for physical layer security in beyond 5G networks," in *Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2019, pp. 865–872.

[272] K. Sengupta, X. Lu, S. Venkatesh, and B. Tang, "Physically secure sub-THz wireless links," in *International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2020, pp. 1–7.

[273] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. M. Assi, and H. Haas, "Physical layer security for visible light communication systems: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1887–1908, 2020.

[274] Y. Liang, H. V. Poor, and S. Shamai, "Physical layer security in broadcast networks," *Security and Communication Networks*, vol. 2, no. 3, pp. 227–238, 2009.

[275] A. Mostafa and L. Lampe, "Enhancing the security of VLC links: Physical-layer approaches," in *Summer Topicals Meeting Series (SUM)*. IEEE, 2015, pp. 39–40.

[276] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu, and H. Haas, "Physical-layer security in 6G networks," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1901–1914, 2021.

[277] F. Rinaldi, H.-L. Maattanen, J. Torsner, S. Pizzi, S. Andreev, A. Iera, Y. Koucheryavy, and G. Araniti, "Non-terrestrial networks in 5G & beyond: A survey," *IEEE Access*, vol. 8, pp. 165 178–165 200, 2020.

[278] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 33–52, 2019.

[279] X. Zhang, B. Zhang, and D. Guo, "Physical layer secure transmission based on fast dual polarization hopping in fixed satellite communication," *IEEE Access*, vol. 5, pp. 11 782–11 790, 2017.

[280] G. Giambene, S. Kota, and P. Pillai, "Satellite-5G integration: A network perspective," *IEEE Network*, vol. 32, no. 5, pp. 25–31, 2018.

[281] K. Guo, K. An, B. Zhang, Y. Huang, and D. Guo, "Physical layer security for hybrid satellite terrestrial relay networks with joint relay selection and user scheduling," *IEEE Access*, vol. 6, pp. 55 815–55 827, 2018.

[282] V. Bankey and P. K. Upadhyay, "Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2488–2501, 2019.

[283] G. J. Sutton, J. Zeng, R. P. Liu, W. Ni, D. N. Nguyen, B. A. Jayawickrama, X. Huang, M. Abolhasan, Z. Zhang, E. Dutkiewicz *et al.*, "Enabling technologies for ultra-reliable and low latency communications: From PHY and MAC layer perspectives," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2488–2524, 2019.

[284] H. Ren, C. Pan, Y. Deng, M. Elkashlan, and A. Nallanathan, "Resource allocation for secure URLLC in mission-critical IoT scenarios," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5793–5807, 2020.

[285] W. Yang, R. F. Schaefer, and H. V. Poor, "Secrecy-reliability tradeoff for semi-deterministic wiretap channels at finite blocklength," in *International Symposium on Information Theory (ISIT)*. IEEE, 2017, pp. 2133–2137.

[286] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[287] 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, 2018.

[288] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[289] D. Marabissi, L. Mucchi, and S. Morosi, "User-cell association for security and energy efficiency in ultra-dense heterogeneous networks," *Sensors*, vol. 21, no. 2, p. 508, 2021.

[290] X. He, R. Jin, and H. Dai, "Physical-layer assisted secure offloading in mobile-edge computing," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 4054–4066, 2020.

[291] R.-F. Liao, H. Wen, J. Wu, F. Pan, A. Xu, H. Song, F. Xie, Y. Jiang, and M. Cao, "Security enhancement for mobile edge computing through physical layer authentication," *IEEE Access*, vol. 7, pp. 116 390–116 401, 2019.

[292] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2018.

[293] V. Marojevic, "C-V2X security requirements and procedures: Survey and research directions," *arXiv preprint arXiv:1807.09338*, 2018.

[294] B. M. ElHalawany, A. A. A. El-Banna, and K. Wu, "Physical-layer security and privacy for vehicle-to-everything," *IEEE Communications Magazine*, vol. 57, no. 10, pp. 84–90, 2019.

[295] X. Luo, Y. Liu, H.-H. Chen, and Q. Guo, "Physical layer security in intelligently connected vehicle networks," *IEEE Network*, vol. 34, no. 5, pp. 232–239, 2020.

[296] Y. E. Sagduyu, T. Erpek, and Y. Shi, "Adversarial machine learning for 5G communications security," in *Game Theory and Machine Learning for Cyber Security*. Wiley Online Library, 2021, pp. 270–288.

[297] N. Papernot, P. McDaniel, X. Wu, S. Jha, and A. Swami, "Distillation as a defense to adversarial perturbations against deep neural networks," in *Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 582–597.

[298] X. Cao and N. Z. Gong, "Mitigating evasion attacks to deep neural networks via region-based classification," in *Proceedings of the 33rd Annual Computer Security Applications Conference*, 2017, pp. 278–287.

[299] W. Guo, "Explainable artificial intelligence for 6G: Improving trust between human and machine," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 39–45, 2020.

[300] D. Doran, S. Schulz, and T. R. Besold, "What does explainable AI really mean? A new conceptualization of perspectives," *arXiv preprint arXiv:1710.00794*, 2017.

[301] G. Thamilarasu and R. Sridhar, "Exploring cross-layer techniques for security: Challenges and opportunities in wireless networks," in *Military Communications Conference (MILCOM)*. IEEE, 2007, pp. 1–6.

[302] J. M. Hamamreh, M. Yusuf, T. Baykas, and H. Arslan, "Cross MAC/PHY layer security design using ARQ with MRC and adaptive modulation," in *Wireless Communications and Networking Conference (WCNC)*. IEEE, 2016, pp. 1–7.

[303] L. Zhou, D. Wu, B. Zheng, and M. Guizani, "Joint physical-application layer security for wireless multimedia delivery," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 66–72, 2014.

[304] S. Bassoy, M. Jaber, M. A. Imran, and P. Xiao, "Load aware self-organising user-centric dynamic CoMP clustering for 5G networks," *IEEE Access*, vol. 4, pp. 2895–2906, 2016.

[305] S. Bassoy, M. A. Imran, S. Yang, and R. Tafazolli, "A load-aware clustering model for coordinated transmission in future wireless networks," *IEEE Access*, vol. 7, pp. 92 693–92 708, 2019.

[306] 3rd Generation Partnership Project (3GPP), "Technical Specification Group Radio Access Network; Study on channel model for frequencies from 0.5 to 100 GHz (Rel-16)," Technical Report 38.901, ver 16.1.0, Dec. 2019.

[307] P. Marsch and G. Fettweis, "Static clustering for cooperative multi-point (CoMP) in mobile communications," in *Proc. IEEE International Conference on Communications (ICC)*, 2011, pp. 1–6.

[308] S. S. Ali and N. Saxena, "A novel static clustering approach for comp," in *IEEE 7th International Conference on Computing and Convergence Technology (ICCCT)*, 2012, pp. 757–762.

[309] K. Kwak, H. Lee, H. W. Je, J. Hong, and S. Choi, "Adaptive and distributed CoMP scheduling in LTE-advanced systems," in *Proc. IEEE 78th Vehicular Technology Conference (VTC Fall)*, 2013, pp. 1–5.

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

[311] A. Al-Hourani, S. Kandeepan, and S. Lardner, "Optimal LAP altitude for maximum coverage," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 569–572, 2014.

[312] A. Al-Hourani, S. Kandeepan, and A. Jamalipour, "Modeling air-to-ground path loss for low altitude platforms in urban environments," in *Proc. IEEE Global Communications Conference (Globecom)*. IEEE, 2014, pp. 2898–2904.

[313] S. Sun, T. S. Rappaport, S. Rangan, T. A. Thomas, A. Ghosh, I. Z. Kovacs, I. Rodriguez, O. Koymen, A. Partyka, and J. Jarvelainen, "Propagation path loss models for 5G urban micro-and macro-cellular scenarios," in *Proc. IEEE 83rd Vehicular Technology Conference (VTC Spring)*, 2016, pp. 1–6.

[314] M. Mozaffari, "Wireless communications and networking with unmanned aerial vehicles: Fundamentals, deployment, and optimization," Ph.D. dissertation, Virginia Polytech. Inst. and State Univ., VA, USA, May 2018. [Online]. Available: https://vtechworks.lib.vt.edu/handle/10919/83921

[315] M.-S. Alouini and M. K. Simon, "Dual diversity over correlated log-normal fading channels," *IEEE Transactions on Communications*, vol. 50, no. 12, pp. 1946–1959, 2002.

[316] M. Speth, S. A. Fechtel, G. Fock, and H. Meyr, "Optimum receiver design for wireless broad-band systems using OFDM - Part I," *IEEE Transactions on Communications*, vol. 47, no. 11, pp. 1668–1677, 1999.

[317] B.-S. Seo, S.-G. Choi, and J.-S. Cha, "Maximum ratio combining for OFDM systems with cochannel interference," *IEEE Transactions on Consumer Electronics*, vol. 52, no. 1, pp. 87–91, 2006.

[318] Z. E. Ankaralı, M. H. Yılmaz, M. Hafez, and H. Arslan, "Channel independent physical layer security," in *IEEE 17th Annual Wireless and Microwave Technology Conference (WAMICON)*, 2016, pp. 1–5.

[319] S. E. Zegrar and H. Arslan, "Effect of prefix/suffix configurations on OTFS systems with rectangular waveforms," *arXiv preprint arXiv:2205.14872*, 2022.

[320] P. Raviteja, K. T. Phan, and Y. Hong, "Embedded pilot-aided channel estimation for OTFS in delay-Doppler channels," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4906–4917, 2019.

[321] F. Liu, Z. Yuan, Q. Guo, Z. Wang, and P. Sun, "Message passing-based structured sparse signal recovery for estimation of OTFS channels with fractional Doppler shifts," *IEEE Transactions on Wireless Communications*, vol. 20, no. 12, pp. 7773–7785, 2021.

[322] European Telecommunications Standards Institute (ETSI), "Intelligent Transport Systems (ITS); Access Layer; Part 1: Channel Models for the 5.9 GHz frequency band)," Technical Report 103 257-1, ver 1.1.1, May 2019.

[323] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017.

[324] X. Cao, P. Yang, M. Alzenad, X. Xi, D. Wu, and H. Yanikomeroglu, "Airborne communication networks: A survey," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 9, pp. 1907–1926, 2018.

[325] W. Mei, Q. Wu, and R. Zhang, "Cellular-connected UAV: Uplink association, power control and interference coordination," *arXiv preprint arXiv:1807.08218*, 2018.

[326] A. Chorti, A. N. Barreto, S. Kopsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6G wireless the role of physical layer security," *arXiv preprint arXiv:2101.01536*, 2021.

[327] 3rd Generation Partnership Project (3GPP), "NR; Physical Channels and Modulation," Technical Specification 38.211, ver 17.1.0, Mar. 2022.

[328] E. Güvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Physical Communication*, vol. 25, pp. 14–25, 2017.

[329] M. Chen, X. Liang, V. Leung, and I. Balasingham, "Multi-hop mesh cooperative structure based data dissemination for wireless sensor networks," in *11th International Conference on Advanced Communication Technology*, vol. 1. IEEE, 2009, pp. 102–106.

[330] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-Allen and Hamilton Inc., Tech. Rep., 2001.

[331] H. Halabian, "Distributed resource allocation optimization in 5G virtualized networks," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 3, pp. 627–642, 2019.

[332] Y. Shi, Y. E. Sagduyu, and T. Erpek, "Reinforcement Learning for Dynamic Resource Optimization in 5G Radio Access Network Slicing," in *IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2020, pp. 1–6.

[333] F. Musumeci, E. De Silva, and M. Tornatore, "Enhancing RAN throughput by optimized CoMP controller placement in optical metro networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 11, pp. 2561–2569, 2018.

[334] A. Marotta, D. Cassioli, C. Antonelli, K. Kondepu, and L. Valcarenghi, "Network solutions for CoMP coordinated scheduling," *IEEE Access*, vol. 7, pp. 176 624–176 633, 2019.

[335] E. Khorov, I. Levitsky, and I. F. Akyildiz, "Current Status and Directions of IEEE 802.11 be, the Future Wi-Fi 7," *IEEE Access*, vol. 8, pp. 88 664–88 688, 2020.

[336] S. Kim, D. Lim, I. Jang, J. Kim, and J. Choi, "Collaborative WLAN Sensing - Follow Ups," document IEEE 802.11-21/0145r5 Mar. 2021.

[337] G. Interdonato, E. Björnson, H. Q. Ngo, P. Frenger, and E. G. Larsson, "Ubiquitous cell-free massive MIMO communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 197, 2019.

[338] J. Zhang, S. Chen, Y. Lin, J. Zheng, B. Ai, and L. Hanzo, "Cell-free massive MIMO: A new next-generation paradigm," *IEEE Access*, vol. 7, pp. 99 878–99 888, 2019.

[339] C. Pan, H. Ren, K. Wang, W. Xu, M. Elkashlan, A. Nallanathan, and L. Hanzo, "Multicell MIMO communications relying on intelligent reflecting surfaces," *IEEE Transactions on Wireless Communications*, vol. 19, no. 8, pp. 5218–5233, 2020.

[340] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, "Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2283–2314, 2020.

[341] G. Song, W. Wang, D. Chen, and T. Jiang, "KPI/KQI-Driven Coordinated Multipoint in 5G: Measurements, Field Trials, and Technical Solutions," *IEEE Wireless Communications*, vol. 25, no. 5, pp. 23–29, 2018.

[342] Y. Li, E. Pateromichelakis, N. Vucic, J. Luo, W. Xu, and G. Caire, "Radio resource management considerations for 5G millimeter wave backhaul and access networks," *IEEE Communications Magazine*, vol. 55, no. 6, pp. 86–92, 2017.

[343] M. H. Johnson and W. K. Harrison, "A rateless approach to physical-layer security," in *International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–6.

[344] B. Van Nguyen, H. Jung, and K. Kim, "Physical layer security schemes for full-duplex cooperative systems: State of the art and beyond," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 131–137, 2018.

[345] J. Wu and P. Fan, "A survey on high mobility wireless communications: Challenges, opportunities and solutions," *IEEE Access*, vol. 4, pp. 450–476, 2016.

[346] L. Mucchi, L. Ronga, X. Zhou, K. Huang, Y. Chen, and R. Wang, "A new metric for measuring the security of an environment: The secrecy pressure," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3416–3430, 2017.

[347] K. S. Ryland, “Software-Defined Radio Implementation of Two Physical Layer Security Techniques,” Ph.D. dissertation, Virginia Tech, 2018.

[348] S. A. Hoseini, F. Bouhafs, and F. den Hartog, “A Practical Implementation of Physical Layer Security in Wireless Networks,” in *19th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2022, pp. 1–4.

[349] F. Bouhafs, M. Mackay, A. Raschellà, Q. Shi, F. den Hartog, J. Saldana, R. Munilla, J. Ruiz-Mas, J. Fernández-Navajas, J. Almodovar *et al.*, “Wi-5: A programming architecture for unlicensed frequency bands,” *IEEE Communications Magazine*, vol. 56, no. 12, pp. 178–185, 2018.

[350] L. Liu, S. Zhang, and R. Zhang, “CoMP in the sky: UAV placement and movement optimization for multi-user communications,” *arXiv preprint arXiv:1802.10371*, 2018.

[351] E. Kalantari, I. Bor-Yaliniz, A. Yongacoglu, and H. Yanikomeroglu, “User association and bandwidth allocation for terrestrial and aerial base stations with backhaul considerations,” in *Proc. IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017, pp. 1–6.

[352] M. Alzenad, A. El-Keyi, and H. Yanikomeroglu, “3-D placement of an unmanned aerial vehicle base station for maximum coverage of users with different QoS requirements,” *IEEE Wireless Communications Letters*, vol. 7, no. 1, pp. 38–41, 2018.

CURRICULUM VITAE

Name Surname : Muhammad Sohaib Jamal Solaija

EDUCATION

B.Sc. : 2014, NUST School of Electrical Engineering and Computer Science (SEECS), Islamabad, Pakistan

M.Sc. : 2014, NUST School of Electrical Engineering and Computer Science (SEECS), Islamabad, Pakistan

PROFESSIONAL EXPERIENCE AND REWARDS

- Awarded the **2nd Prize** at 3rd Universities Patent Competition held by Turkish Patent Office in 2023.
- Awarded multiple performance-based scholarships under TÜBİTAK 2250 program.
- Contributed to WiFi-7 standardization activities as member of the IEEE 802.11be task group.
- Member of the Satellite group under IEEE's Future Networks Technical Community (FNTC) initiative.

PUBLICATIONS, PRESENTATIONS, AND PATENTS ON THE THESIS

- **M. S. J. Solaija**, S. E. Zegrar, and H. Arslan, "Delay-Doppler Based Key Generation Using OTFS," *IEEE Wireless Communications Letters*, May 2023.
- **M. S. J. Solaija**, H. Salman, and H. Arslan, "Towards a Unified Framework for Physical Layer Security in 5G and Beyond Networks," *IEEE Open Journal of Vehicular Technology*, June 2022.
- **M. S. J. Solaija**, H. Salman, A. B. Kihero, M. I. Sağlam and H. Arslan, "Generalized Coordinated Multipoint Framework for 5G and Beyond," *IEEE Access*, vol. 9, pp. 72499-72515, May 2021.
- **M. S. J. Solaija,** H. Salman, K. A. Qaraqe, and H. Arslan, "Spatially Distributed Channel Shortening Aided Physical Layer Security," accepted for presentation in *IEEE International Mediterranean Conference on Communications and Networking (MeditCom),* September 2023.
- **M. S. J. Solaija**, H. M. Furqan, Z. E. Ankarali, and H. Arslan, "Cyclic Prefix (CP) Jamming Against Eavesdropping Relays in OFDM Systems," *IEEE Wireless Communications and Networking Conference (WCNC),* April 2022.
- **M. S. J. Solaija**, S. Dogan, S. Buyukcorak, and H. Arslan, "Hybrid Terrestrial-Aerial Network for Ultra-Reliable Low Latency Communication," *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC),* September 2019.

- "A Delay-Doppler Based Key Generation Method for Secure Wireless Communication" *Turkish Patent Application* 2022/021085.
- "Method for Coordination Group Formation and Scheme Selection in the Presence of Multi-link Devices," *European Patent Application* 20203137.3-1212.
- "Gizli dinleme saldirilarina karşi kablosuz iletişimi korumaya yönelik bir yöntem (A Method for Protecting Wireless Communication Against Eavesdropping Attacks)," *Turkish Patent Application* 2020/22598.
- "Makro-çeşitlilik ile güvenilir kablosuz haberleşme sistemi (A Method of Providing Macro-diversity for Reliable Communication)," *Turkish Patent Application* 2019/21319

OTHER PUBLICATIONS, PRESENTATIONS, AND PATENTS

- H. Türkmen, **M. S. J. Solaija**, A. Tusha, H. Arslan, "Wireless Sensing – Enabler of Future Wireless Technologies", *Turkish Journal of Electrical Engineering & Computer Sciences,* 29(1), 1-17, Jan. 2021.
- H. M. Furqan, **M. S. J. Solaija**, H. Türkmen, H. Arslan, "Wireless Communication, Sensing, and REM: A Security Perspective," *IEEE Open Journal of the Communications Society*, 2(1), 287-321, Jan. 2021.
- A.B. Kihero, **M. S. J. Solaija**, and H. Arslan, "Inter-Numerology Interference for Beyond 5G", *IEEE Access*, vol. 7, pp. 146512-146523, Oct. 2019.
- Y. I. Demir, **M. S. J. Solaija**, and H. Arslan, "On the Performance of Handover Mechanisms for Non-Terrestrial Networks," *IEEE Vehicular Technology Conference (VTC-Spring),* June 2022.
- **M. S. J. Solaija** et al. "Quantum Laboratory Setup for Future Wireless Communication Systems", presented in *Turkish Physical Society – International Physics Conference*, September 2019.
- A. B. Kihero, **M. S. J. Solaija**, A. Yazar, and H. Arslan, "Inter-Numerology Interference Analysis for 5G and Beyond", *IEEE Globecom Workshops*, December 2018.
- "Güvenli kablosuz iletişime yönelik dağitik taşiyici frekans ofseti dengelemesi (Distributed Carrier Frequency Offset Compensation for Secure Wireless Communication)" *Turkish Patent Application* 2021/019472.
- "Kablosuz sistemlerde dinlemeyi önlemek için konstelasyon sembolünün gizlenmesi (Constellation Symbol Obfuscation for Preventing Eavesdropping in Wireless Systems)" *Turkish Patent Application* 2021/019491.
- "Kanal tabanli faz ön denkleştirmesi kullanilarak gizli dinlemenin önlenmesi (Eavesdropping Prevention Using Channel Based Phase Pre Equalization)" *Turkish Patent Application* 2021/019492.
- "Flexible Resource Grid Design for Orthogonal Time Frequency Space (OTFS) Waveform" *Turkish Patent Application* 2021/020126.

COORDINATED MULTI-POINT SYSTEMS FOR FUTURE WIRELESS COMMUNICATION NETWORKS

ORIGINALITY REPORT

12%	8%	7%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dokumen.pub Internet Source	3%
2	kanchiuniv.ac.in Internet Source	2%
3	Hanadi Salman, Hüseyin Arslan. "Physical layer security definition and domains", Institution of Engineering and Technology (IET), 2022 Publication	1%
4	Haji M. Furqan, Muhammad Sohaib J. Solaija, Halise Turkmen, Huseyin Arslan. "Wireless Communication, Sensing, and REM: A Security Perspective", IEEE Open Journal of the Communications Society, 2021 Publication	<1%
5	Submitted to Lebanese International University Student Paper	<1%
6	Submitted to United States Coast Guard Academy	<1%