ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

SECURE AND COORDINATED BEAMFORMING IN 5G AND BEYOND SYSTEMS USING DEEP NEURAL NETWORKS

Ph.D. THESIS

Utku ÖZMAT

Department of Applied Informatics

Cybersecurity Engineering and Cryptography Programme

MARCH 2024

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

SECURE AND COORDINATED BEAMFORMING IN 5G AND BEYOND SYSTEMS USING DEEP NEURAL NETWORKS

Ph.D. THESIS

Utku ÖZMAT
(707162003)

Department of Applied Informatics

Cybersecurity Engineering and Cryptography Programme

Thesis Advisor: Asst. Prof. Dr. Mehmet Akif YAZICI
Co-Advisor: Asst. Prof. Dr. Mehmet Fatih DEMİRKOL

MARCH 2024

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

5G VE ÖTESİ SİSTEMLERDE DERİN SİNİR AĞLARI KULLANARAK GÜVENLİ VE KOORDİNELİ HÜZMELEME

DOKTORA TEZİ

Utku ÖZMAT
(707162003)

Bilişim Uygulamaları Anabilim Dalı

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

Tez Danışmanı: Dr. Öğr. Üyesi Mehmet Akif YAZICI
Eş Danışman: Dr. Öğr. Üyesi Mehmet Fatih DEMİRKOL

MART 2024

Utku ÖZMAT, a Ph.D. student of ITU Graduate School student ID 707162003 successfully defended the thesis entitled "SECURE AND COORDINATED BEAMFORMING IN 5G AND BEYOND SYSTEMS USING DEEP NEURAL NETWORKS", which he/she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Asst. Prof. Dr. Mehmet Akif YAZICI** Istanbul Technical University	.....
Co-Advisor :	**Asst. Prof. Dr. Mehmet Fatih DEMİRKOL** Haliç University	.....
Jury Members :	**Prof. Dr. Lütfiye DURAK ATA** Istanbul Technical University	.....
	Prof. Dr. Hakan Ali ÇIRPAN Istanbul Technical University	.....
	Assoc. Prof. Dr. Mustafa NAMDAR Kütahya Dumlupınar University	.....
	Asst. Prof. Dr. Semiha TEDİK BAŞARAN Istanbul Technical University	.....
	Asst. Prof. Dr. Arif BAŞGÜMÜŞ Bursa Uludağ University	.....

Date of Submission : **5 January 2024**
Date of Defense : **6 March 2024**

To my beloved wife and adored daughter Göksu,

FOREWORD

First and foremost, my sincere appreciation goes to my primary advisor, Asst. Prof. Dr. Mehmet Akif YAZICI. Their unwavering commitment to academic excellence, insightful guidance, and mentorship have been the cornerstones of my doctoral journey. From the inception of this research to its culmination, their expertise, patience, and encouragement have played a pivotal role in shaping the trajectory of my work.

Equally deserving of my deepest gratitude is my co-advisor, Asst. Prof. Dr. Mehmet Fatih DEMİRKOL. Their collaborative spirit, career insights, and constructive feedback have been instrumental in refining the nuances of my research. The synergy between my advisors has created a dynamic and enriching academic environment, propelling me to explore new horizons and reach intellectual heights that would not have been possible without their combined expertise.

To the esteemed members of the thesis progress committee, your constructive critiques, insightful suggestions, and thoughtful guidance have been pivotal at each stage of this academic exploration. Your expertise and commitment to fostering academic excellence have not only refined the scope of this work but have also served as beacons, illuminating the path forward. The intellectual discourse and rigorous discussions during progress evaluations have been instrumental in honing the clarity and depth of the research.

I must also express my gratitude to my colleagues and fellow researchers who have been companions on this intellectual expedition. Your insights, camaraderie, and shared passion for knowledge have been a source of inspiration and have enriched the fabric of this research.

Finally, to my family, your encouragement and understanding during the peaks and valleys of this academic pursuit have been my anchor. Your unwavering support, love, and inspiration have been the driving forces behind the completion of this thesis.

March 2024

Utku ÖZMAT
(Telecommunication Engineer)

TABLE OF CONTENTS

	Page
FOREWORD	**ix**
TABLE OF CONTENTS	**xi**
ABBREVIATIONS	**xiii**
SYMBOLS	**xv**
LIST OF TABLES	**xvii**
LIST OF FIGURES	**xix**
SUMMARY	**xxiii**
ÖZET	**xxvii**
1. INTRODUCTION	**1**
1.1 Problem Statement	2
1.2 Aim and Objectives	2
1.3 Outline	4
2. TECHNICAL BACKGROUND AND RELATED WORK	**5**
2.1 5G and Beyond Networks	5
2.2 Massive MIMO and CoMP Techniques	9
2.2.1 Massive MIMO systems	9
2.2.2 Comparison of SISO, MIMO and massive MIMO systems	12
2.2.3 Coordinated multi-point transmission	17
2.3 Physical Layer Security	21
2.4 Deep Learning Methods in Mobile Networks	24
2.5 Related Work	27
3. BEAM MANAGEMENT IN 5G AND BEYOND NETWORKS	**31**
3.1 The Motivation Behind 5G NR Beam Management	31
3.2 Elements of Beam Management	33
3.2.1 Beam sweeping	33
3.2.2 Beam measurement and determination	35
3.2.3 Beam reporting	36
3.2.4 Beam recovery	36
3.2.5 Beam switching	37
3.3 Beam Management Procedures	37
3.3.1 Procedure 1: SSB-based beam sweeping	37
3.3.2 Procedure 2: CSI-RS based Tx-end beam refinement	41
3.3.3 Procedure 3: CSI-RS based Rx-end beam refinement	43
4. DEEP LEARNING-BASED SECURE BEAM MANAGEMENT	**45**
4.1 Secure Initial Access and Beam Selection using Deep Learning	47
4.1.1 Channel model and antenna configuration	48
4.1.2 Secure beam selection algorithm	54
4.1.3 DNN model for single-cell transmission	54
4.1.3.1 Data generation	55
4.1.3.2 DNN architecture	57
4.2 Secure Multi-Point Coordinated Beamforming using Deep Learning	60
4.2.1 Channel model and antenna configuration	62
4.2.2 Multi-point secure beam selection algorithm	63
4.2.3 DNN model for multi-point transmission	63
4.2.3.1 Data generation	64
4.2.3.2 DNN architecture	65
5. RESULTS AND DISCUSSION	**67**
5.1 Simulation Environment for Single-Cell Transmission Scenario	68
5.1.1 Terrain model	70
5.1.2 The statistical channel model	71
5.1.3 Prediction performance of DNN	73
5.1.4 The achievable RSRP levels	76

5.1.5 The achievable P_{SD} and P_{SSD} probabilities 77
5.2 Simulation Environment for Multi-Point Transmission Scenario 79
5.2.1 Terrain model 79
5.2.2 The statistical channel model 80
5.2.3 Prediction performance of DNN 82
5.2.4 The achievable RSRP levels 83
5.2.5 The achievable P_{SD} and P_{SSD} probabilities 85
5.3 Examining Security in Single-Cell vs. Multi-Point Transmission 88
6. CONCLUSIONS AND FUTURE WORKS **91**
6.1 Suggestions for Future Works 93
REFERENCES **95**
CURRICULUM VITAE **105**

ABBREVIATIONS

1G : First generation
2G : Second generation
3CLS : Communication, computing, control, localization, and sensing
3G : Third generation
3GPP : 3rd Generation Partnership Project
4G : Forth generation
5G : Fifth generation
6G : Sixth generation
Adam : Adaptive moment estimation
AE : Auto-encoder
AoA : Angle of arrival
AWGN : Additive white Gaussian noise
BS : Base station
CB : Coordinated beamforming
CNN : Convolutional neural network
CoMP : Coordinated multi-point
CRAS : Connected robotics and autonomous systems
CS : Coordinated scheduling
CSI : Channel state information
CSI-RS : Channel state information-reference signal
DL : Deep learning
DMRS : Demodulation reference signal
DNN : Deep neural network
DPS : Dynamic point selection
ECOC : Error-correcting output codes
eMBB : Enhanced mobile broadband
eNB : eNodeB
FPGA : Field-programmable gate array
FR : Frequency range
gNB : gNodeB
GPS : Global positioning system
GSM : Global system for mobile communications
IoT : Internet of things
JR : Joint reception
JT : Joint transmission
KNN : K-nearest neighbors algorithm
KPI : Key performance indicator
LED : Light-emitting diode
LTE : Long-term evolution
MAC : Medium access control

MBRLLC : Mobile Broadband Reliable Low Latency Communication
ML : Machine learning
MLP : Multilayer perceptron
mMIMO : Massive multiple-input-multiple-output
mMTC : Massive machine-type communications
mmWave : Millimeter wave
MIB : Master information block
MIMO : Multiple-input-multiple-output
MPS : Multi-Purpose Services
MU-MIMO : Multi-user multiple-input-multiple-output
mURLLC : Massive ultra-reliable and low-latency communication
NR : New radio
NZP : Non-zero-power
OFDM : Orthogonal frequency division multiplexing
PBCH : Physical broadcast channel
PDCCH : Physical downlink control channel
PDP : Power delay profile
PHY : Physical layer
PLS : Physical layer security
PRACH : Physical random access channel
PSS : Primary synchronization signal
RA : Random access
RACH : Random access channel
RF : Radio frequency
RSRP : Reference signal received power
Rx : Receive
SIB : System information block
SINR : Signal-to-interference-plus-noise ratio
SISO : Single-input single-output
SNR : Signal-to-noise ratio
SRS : Sounding reference signal
SSD : Secure and successful detection
SSB : Synchronization signal blocks
SS : Synchronization signal
SSS : Secondary synchronization signal
SU-MIMO : Single-user multiple-input-multiple-output
SVM : Support vector machine
TRP : Transmit/receive point
TP : Transmission point
Tx : Transmit
UE : User equipment
umMIMO : Ultra massive multiple-input-multiple-output
URA : Uniform rectangular array
URLLC : Ultra-reliable and low-latency communication
VLC : Visible light communication
XR : Extended reality

SYMBOLS

α_l	: Complex channel gain at l-th path
β	: Security threshold
ϑ, φ	: Elevation and azimuth angles of the signal
γ_u	: Aggregated channel parameters
$\mathbf{A}$	: Steering matrix
$\mathbf{a_v}$, $\mathbf{a_h}$	: Steering vectors in vertical and horizontal axes
$\mathbf{b}$	: Best beam pair indices
$\mathbf{C}$	: Capacity
$\mathbf{f_{i,j}}$	: Beamformed signal
$\mathbf{G_T}$,$\mathbf{G_R}$	: Antenna gains of transmit and receive beams
$\mathbf{H}$	: Channel
$\mathbf{i,j}$	: Transmitter and receiver beam indices
$\mathbf{K}$	: Number of classes
$\mathbf{K_T}$, $\mathbf{K_R}$	: Number of beams at transmitter and receiver
$\mathbf{l}$	: Path
$\mathbf{L_p}$	: Total number of paths
$\mathbf{L_{CE}}$	: Cross-entropy loss
$\mathbf{M}$	: Receiving antenna elements
$\mathbf{M_v}$, $\mathbf{M_h}$	: Receiving antenna elements in vertical and horizontal axes
$\mathbf{N}$	: Transmitting antenna elements
$\mathbf{N_v}$, $\mathbf{N_h}$	: Transmitting antenna elements in vertical and horizontal axes
$\mathbf{n}$	: Additive noise power
$\mathbf{P_{i,j}}$	: Measured signal strength
$\mathbf{P_L}$	: Path loss
$\mathbf{P_{SD}}$	: Probability of successful detection
$\mathbf{P_{SSD}}$	: Probability of secure and successful detection
$\mathbf{P_T}$	: Transmit power
$\mathbf{T}$	: Number of samples
$\mathbf{u}$	: Receiver
$\mathbf{w_j}$	: Weight for class j
$\mathbf{y_{ij}}$	: Output for sample i for class j
$\mathbf{z_{ij}}$	: Indicator that the i-th sample belongs to the j-th class

LIST OF TABLES

Page

Table 2.1 : Requirements and KPIs of 5G, B5G and 6G. **9**
Table 3.1 : The maximum number of SSBs for frequencies in 5G NR. **35**
Table 4.1 : Experimental results of the different model hyperparameters. **58**
Table 5.1 : Simulation parameters for the single-cell transmission scenario. **70**
Table 5.2 : Classification metrics comparison of the proposed DNN with other learning schemes when $K = 1$ in the terrain model. **75**
Table 5.3 : Simulation parameters for the multi-point transmission scenario. **80**

LIST OF FIGURES

Page

Figure 2.1 : 5G usage scenarios of International Mobile Telecommunications (IMT)-2020 ..... **6**
Figure 2.2 : The difference between classical communication systems and MIMO. **11**
Figure 2.3 : Systematic representation of SISO systems. **13**
Figure 2.4 : Systematic representation of SU-MIMO systems. **14**
Figure 2.5 : Systematic representation of MU-MIMO systems. **16**
Figure 2.6 : Systematic representation of mMIMO systems. **17**
Figure 2.7 : CoMP transmission scheme with two geographically isolated TPs. . **18**
Figure 2.8 : The downlink CoMP schemes: coordinated scheduling and beamforming (CS/CB)..... **19**
Figure 2.9 : The downlink CoMP schemes: joint transmission (JT) and dynamic point selection (DPS)..... **20**
Figure 2.10 : Illustration of main security threats at the physical layer. **22**
Figure 2.11 : Illustration of specific communication scenarios where PLS can supplement cryptographic approaches. **23**
Figure 2.12 : The relation between deep learning, machine learning, and artificial intelligence. **25**
Figure 2.13 : Classification of the potential applications of DL in mobile and wireless networks. **27**
Figure 3.1 : UE attach timing diagram. **34**
Figure 3.2 : SSBs and beam mapping. **35**
Figure 3.3 : Procedure 1 end-to-end processing steps. **38**
Figure 3.4 : SS burst generation. **39**
Figure 3.5 : SSB beam sweeping in downlink. **39**
Figure 3.6 : Procedure 1 spatial scene simulation. **40**
Figure 3.7 : CSI-RS based transmit-end beam refinement. **41**
Figure 3.8 : Procedure 2 end-to-end processing steps. **42**
Figure 3.9 : Procedure 2 spatial scene simulation. **42**
Figure 4.1 : mMIMO beam patterns of Tx-Rx antennas. **49**
Figure 4.2 : Illustration of a mMIMO spatial perspective with Tx-Rx beams and scatterers..... **50**
Figure 4.3 : The potential eavesdropper positions in a single-cell scenario. **51**
Figure 4.4 : User locations in a real cellular network served by a single cell. **55**
Figure 4.5 : The data generation step of the DNN model through an exhaustive search..... **56**
Figure 4.6 : The training step of the DNN model and its architecture. **59**
Figure 4.7 : The testing step of the DNN model with an unseen testing data. **60**

Figure 4.8 : The potential eavesdropper positions in a multi-point transmission scenario. **61**
Figure 4.9 : User locations in a real cellular network served by two cells. **63**
Figure 4.10 : The DNN architecture to predict beam pairs in multi-point transmission. **65**
Figure 5.1 : The best Tx beams with security constraints for each user. Each color belongs to a different Tx beam. **69**
Figure 5.2 : The best Tx beams without security constraints for each user. Each color belongs to a different Tx beam. **69**
Figure 5.3 : Comparison of prediction performance for the terrain model with security constraints in a single-cell scenario. **72**
Figure 5.4 : Comparison of prediction performance for the terrain model without security constraints in a single-cell scenario. **72**
Figure 5.5 : Comparison of prediction performance for the statistical model with security constraints in the single-cell scenario. **73**
Figure 5.6 : Comparison of prediction performance for the statistical model without security constraints in the single-cell scenario. **74**
Figure 5.7 : The training and validation curves of the proposed DNN subject to accuracy and loss when $K = 1$. **75**
Figure 5.8 : Achievable RSRP values under varying conditions of security constraints (s.c.), along with the RSRP levels accomplished by the proposed DNN employing the Top-K beam pairs in the single-cell terrain model. **75**
Figure 5.9 : Achievable RSRP values under varying conditions of security constraints (s.c.), along with the RSRP levels accomplished by the proposed DNN employing the Top-K beam pairs in the single-cell statistical model. **76**
Figure 5.10 : Achievable probabilities for P_{SD} and P_{SSD} under different security constraints, and the corresponding probabilities achieved by the proposed method using Top-K beam pairs in the terrain model in a single-cell scenario. **77**
Figure 5.11 : Achievable probabilities for P_{SD} and P_{SSD} under different security constraints, and the corresponding probabilities achieved by the proposed method using Top-K beam pairs in the statistical model in a single-cell scenario. **78**
Figure 5.12 : Users distribution based on the serving TP. **79**
Figure 5.13 : Comparison of prediction performance for the terrain model with security constraints in the multi-point scenario. **81**
Figure 5.14 : Comparison of prediction performance for the terrain model without security constraints in the multi-point scenario. **82**
Figure 5.15 : Comparison of prediction performance for the statistical model with security constraints in the multi-point scenario. **83**
Figure 5.16 : Comparison of prediction performance for the statistical model without security constraints in the multi-point scenario. **84**

Figure 5.17 : Achievable RSRP values under varying conditions of security constraints (s.c.), along with the RSRP levels attained by the proposed DNN employing the Top-K beam pairs in the multi-point terrain model. **85**
Figure 5.18 : Achievable RSRP values under varying conditions of security constraints (s.c.), along with the RSRP levels attained by the proposed DNN employing the Top-K beam pairs in the multi-point statistical model. **86**
Figure 5.19 : The achievable P_{SD} and P_{SSD} probabilities with and without security constraints (s.c.), and the P_{SD} and P_{SSD} probabilities the proposed method achieves using the Top-K beam pairs for the terrain model in the multi-point scenario. **87**
Figure 5.20 : The achievable P_{SD} and P_{SSD} probabilities with and without security constraints (s.c.), and the P_{SD} and P_{SSD} probabilities the proposed method achieves using the Top-K beam pairs for the statistical model in the multi-point scenario. **87**
Figure 5.21 : The achievable P_{SD} and P_{SSD} probabilities with and without DPS-CoMP for the terrain model. **88**
Figure 5.22 : The achievable P_{SD} and P_{SSD} probabilities with and without DPS-CoMP for the statistical model. **89**

SECURE AND COORDINATED BEAMFORMING IN 5G AND BEYOND SYSTEMS USING DEEP NEURAL NETWORKS

SUMMARY

Beam management stands as a crucial element within the fifth generation (5G) new radio (NR), pivotal for shaping an efficient initial access and tracking process. It functions to consistently identify the optimal beam pair between the user equipment (UE) and the gNodeB (gNB), significantly contributing to overall system efficiency.

In machine learning-assisted beam management research, deep neural networks (DNNs) emerge as a preferred solution, showcasing their autonomy in recognizing critical features in the dynamic 5G context. DNNs excel in capturing nonlinear relationships between input parameters and optimal beam configurations, making them robust tools for addressing beam management complexities. Deep learning algorithms extend their utility to coordinated multi-point (CoMP) scenarios, dynamically scheduling data transmissions and selecting users based on real-time considerations. Additionally, ML integration in physical layer security enhances network security by identifying and mitigating potential threats.

The beam management process involves utilizing synchronization signal blocks (SSB), transmit/receive point (TRP) beam sweeping, and UE beam sweeping to establish an effective beam pair link, maximizing spectral efficiency. However, the exhaustive search across potential beam pairs becomes challenging with the increasing number of antenna elements in massive multiple-input-multiple-output (MIMO), leading to heightened latency and energy consumption. This emphasizes the urgent need for a streamlined and secure access approach in rapidly deploying 5G networks.

To eliminate the need for this repetitive exhaustive searches and reduce communication overhead, a DNN-based scheme is proposed. The beam selection problem is treated as a classification task, with the optimal Tx-Rx beam pair index as the target output and user positions as input to the DNN model. Leveraging this information that unrelated to specific frequency bands or channels, the trained DNN model suggests a collection of K favorable beam pair indices. Rather than conducting a thorough search across all possible beam pairs, the signalling overhead due to beam sweeping is minimized by exploring only within the a chosen set of K beam pairs. It's worth noting that, the additional time required or the time overhead during beam sweeping also increases with a higher number of beams. Hence, the key motivation behind incorporating deep learning into beam selection process is enhance the beam search/sweeping process, focusing on minimizing latency, reducing energy consumption, and strengthening communication security.

In this thesis, we introduce two transmission models. The first model outlines a DNN-based secure initial access and beam selection procedure within a single

serving cell framework. The SSB beam sweeping process is automated using a DNN, demonstrating the alignment of the proposed DNN with existing standards. Notably, our approach prioritizes the selection of a beam pair, aiming to maximize the RSRP for the UE while also guaranteeing that the RSRP observed by potential eavesdroppers stays below a specified threshold. The inherent properties of mMIMO and beamforming contribute to achieving a precise level of protection against eavesdropping attacks, eliminating the need for additional security mechanisms such as injecting artificial noise, generating secure keys, employing directional modulation, and others.

The second model addresses the beam selection challenge in networks employing mMIMO and CoMP for secure radio coverage. In this scenario, we introduce a DNN-driven CoMP beamforming approach aimed at predicting the indices of the most secure beam pairs among multiple coordinated TPs and the UE. This model aligns with the same motivation as the single-cell scenario, emphasizing the importance of communication security.

The proposed method relies solely on utilizing location information without dependence on channel parameters or estimation procedures. Additionally, no supplementary security mechanisms at the physical layer are employed, and there is no requirement for alterations to current standards.

Our approach is practical and aligns seamlessly with 5G NR signaling, requiring no adjustments to the standard. However, variations in system parameters introduce unique scenarios, necessitating retraining of the DNN for adaptation.

To delineate and evaluate our proposed DL-based method, we utilize two scenarios. In the initial scenario, referred to as the terrain model, data is acquired from a network planning software. This software calculates RSRP values based on specified parameters from various operational cells and authentic 3D terrain data. For a comprehensive understanding of our proposed method's effectiveness, we introduce a second scenario, the statistical model. This scenario involves the use of synthetically generated data employing a statistical channel model, incorporating system variables in 5G NR outlined in standards. This framework provides a robust and solid evaluation of our proposed method.

Based on the defined scenarios and channel models, simulations are conducted in the MATLAB environment. Firstly, the prediction performance of the DNN is evaluated by comparing it with some benchmark ML models, and the training and validation performance of the DNN are examined. Then, achievable RSRP levels are simulated for baseline and secure beam selection algorithms to observe variations at the maximum achievable RSRP level, considering it as the trade-off for fortifying communication security whenever deemed feasible. Next, the secure and successful detection probabilities are examined to measure the security improvement made to the existing networks. Finally, single-cell and multi-point transmission models are compared in terms of security and communication availability.

The numerical results illustrate that the proposed DNN-based beam selection algorithm significantly improves the secure coverage probability for both single-cell and multi-point transmission models. Moreover, employing a DNN to reduce the search

space, whether aiming to provide the best or most secure beam pair, results in a substantial reduction in both the time and energy consumed during the beam selection process. This reduction is crucial, especially for delay-sensitive services in 5G and beyond networks.

5G VE ÖTESİ SİSTEMLERDE DERİN SİNİR AĞLARI KULLANARAK GÜVENLİ VE KOORDİNELİ HÜZMELEME

ÖZET

Beşinci nesil (5G) ve ötesi mobil haberleşme sistemlerinde hüzme yönetimi oldukça kritik bir öneme sahiptir. 5G'deki dalga şekli, hüzmeler aracıyla gönderilen bir dalga şeklidir. Tüm kanallar (merkeze doğru gönderim ve kontrol/veri kanalları) ve tüm sinyaller (aşağı ve yukarı yönlü senkronizasyon sinyalleri) hüzmeleme yapısına göre tasarlanmıştır. Hüzmeleme ile kapsama tek ve geniş bir radyo dalgası yerine, çok daha fazla sayıda ve enerjinin konsantre edildiği radyo dalgaları ile sağlanmaktadır. Sayısal, analog veya hibrit şeklinde türleri olan hüzmeleme işlemi, kullanıcılara daha yüksek güçte sinyal iletilebilmesini, girişimin azaltılmasını ve bağlantı yoğunluğunun artırılabilmesini sağlamaktadır. Çok sayıda anten elemanının aynı frekans ve zaman kaynağında çalışması prensibine dayanan masif çoklu giriş çoklu çıkış (mMIMO) teknolojisi ile birlikte hüzmeleme, 5G'nin öne çıkan özelliklerinden biridir. Hüzme yönetiminin ana bileşenleri, hüzme tarama, hüzme ölçümü, belirlenmesi ve raporlanması, hüzme kurtarma ve hüzme değişimi şeklinde sıralanmaktadır. Bu süreç, kullanıcı ekipmanı (UE) ve servis veren baz istasyonu (gNodeB) arasındaki iletişim sürdükçe devam etmektedir ve alıcı-verici arasındaki en uygun hüzme çiftini belirleyerek genel olarak haberleşmenin sürekliliği ve verimliliği için ihtiyaç duyulan en önemli fiziksel katman unsurlarından biridir.

Öte yandan, son zamanlarda makine öğrenimi (ML), özellikle derin öğrenme (DL), mobil ve kablosuz ağlara yönelik çok çeşitli araştırma alanlarında öne çıkan bir teknik haline gelmiştir. DL yöntemlerinin potansiyel alanları arasında mobilite analizi, kullanıcı konumlandırılması, kablosuz sensör ağları, ağ kontrolü, ağ güvenliği, sinyal işleme, ağ düzeyinde ve uygulama düzeyinde mobil veri analizi yer almaktadır. Tez çalışmasında da sunulduğu üzere, DL algoritmalarının hüzme yönetimi süreçlerinde kullanılması da literatürde yer bulmaktadır. Bu alandaki yapılan çalışmalarda, açısal ve zaman alanlarında doğrusal olmayan özelliklerin çıkarılmasındaki üstünlüğü ile yüksek doğrulukta hüzme çifti tahmini yapılabildiği gösterilmiştir. Ek olarak, hüzme takibindeki yükü en aza indirmek için öngörülü hüzme değişimi de gerçekleştirilebilmektedir. Bu yüzden, derin sinir ağları (DNN) giriş parametreleri ile optimum hüzme konfigürasyonları arasındaki doğrusal olmayan ilişkileri yakalama konusunda başarılı olduklarından, hüzme yönetiminin doğasından gelen karmaşıklıkla başa çıkmak için tercih edilen araçlar olarak öne çıkmaktadır. Ayrıca, DL algoritmaları koordineli çoklu nokta (CoMP) iletimi senaryolarında da kullanılmaktadır. Burada veri iletiminin dinamik olarak planlanması ve gerçek zamanlı olarak kullanıcı veya iletim noktalarının (TP) seçimi işlemleri otonom olarak yapılabilmektedir. Ek olarak, fiziksel katman güvenliğinde ML entegrasyonu, potansiyel tehditleri önceden tanımlayarak ve önleyerek ağ güvenliğini artırmaktır.

Hüzme yönetimi süreci içerisinde spektral verimliliği maksimize etmek ve etkili bir hüzme çifti üzerinden haberleşme sağlayabilmek için senkronizasyon sinyal bloklarının (SSB) kullanımı, iletim/alım noktası (TRP) ve UE tarafında hüzme taraması işlemleri yer almaktadır. Böylece tüm olası hüzme çiftlerinin taranmaktadır. Ancak, mMIMO ile birlikte artan anten elemanlarıyla bu işlemlerin yapılması artan gecikme ve enerji tüketimine yol açmaktadır. Bu yüzden, hızla artan 5G kurulumları ve servislerin ihtiyaç duydukların gecikme ve güvenlik gereksinimleri doğrultusunda bu problemin çözümü acil bir ihtiyaç olarak vurgulanmaktadır.

Tez çalışmasında, yukarıda bahsedilen tekrarlayan kapsamlı hüzme çifti taramalarına gerek duymamak ve sinyalleşme yükünü azaltmak için bir DNN tabanlı şema önerilmektedir. Hüzme seçimi problemi önerilen DNN algoritması içerisinde bir sınıflandırma problemi olarak görülmüştür ve UE koordinatları giriş bilgisi olarak, optimum verici (Tx)-alıcı (Rx) hüzme çifti indeksi ise çıkış bilgisi olarak kullanılmıştır. DNN modelinin eğitiminden sonra, K adet uygun hüzme çifti indeksini önermektedir. Tüm olası hüzme çiftleri arasında kapsamlı bir arama yapmak yerine, sadece önerilen K adet hüzme çifti içerisinde bir arama yapılarak, hüzme taraması esnasındaki sinyalleşme yükü azaltılmaktadır. 5G ve ötesi ağlarda anten dizin sayıları (dolayısıyla hüzme sayıları) artacağından hüzme taraması süresi de yükselmektedir. Bu nedenle, derin öğrenme algoritmalarının hüzme yönetimi süreçlerine entegre edilmesindeki ana motivasyon, gecikme, enerji tüketimi ve iletişim güvenliği açısından hüzme arama sürecini iyileştirmektir.

Tez çalışmasında, hüzme seçimine dair iki senaryo önerilmektedir. İlk senaryoda servis veren tek hücrenin yer aldığı bir haberleşme sisteminde DNN tabanlı ilk erişim ve hüzme hizalaması prosedürü ele alınmaktadır. SSB hüzme taraması süreci, DNN yapısı kullanılarak otonom bir şekilde gerçekleştirilmektedir ve önerilen DNN yapısının mevcuttaki standartlar ile uyumluluğunu gösterilmektedir. Özellikle, önerilen yaklaşım UE için RSRP'yi maksimize etmekle kalmamakta, aynı zamanda potansiyel gizli dinleyiciler tarafından gözlemlenen RSRP'nin de belirli bir eşiği aşmamasını sağlamayı amaçlayan güvenli bir hüzme çiftinin seçiminin sağlamaktadır. mMIMO ve hüzmeleme tekniklerinin kendiliğinden gelen özellikler kullanılarak, yapay gürültü enjeksiyonu, güvenli anahtar üretimi, yönlü modülasyon vb. gibi ek güvenlik mekanizmalarına ihtiyaç duymadan gizli dinleme saldırılarına karşı belirli bir güvenlik düzeyine ulaşılmasına katkıda bulunulmaktadır.

İkinci senaryo ise mMIMO ve CoMP birlikte kullanarak güvenli radyo kapsamı için ağlarda optimum hüzme ve TP seçimi sorununa odaklanılmaktadır. Bu senaryoda, birden fazla koordineli TP ve UE arasında en güvenli hüzme çifti indislerini tahmin etmeyi amaçlayan DNN tabanlı bir CoMP hüzmeleme şeması önerilmektedir. Bu çoklu-noktadan iletim senaryosu da tek hücreli senaryo ile aynı motivasyona sahip olup, iletişim güvenliğinin artırılması ve hüzme seçimi esnasında yaşanan gecikmenin ve enerji tüketiminin azaltılması amaçlanmaktadır.

Her iki senaryodada önerilen güvenli hüzme seçimi yönetimi yalnızca kullanıcıların konum bilgilerine dayanmaktadır ve diğer başka herhangi bir kanal parametresine ve kanal kestirim prosedürene bağlı değildir. Güvenlik açısından bakıldığında literatürdeki ana kullanım amaçlarına ek olarak mMIMO ve CoMP teknolojilerinden güvenli haberleşme için de yararlanılabileceği gösterilmiştir. Böylelikle herhangi

bir ek fiziksel katman güvenliği yöntemi kullanılmadığından mevcut haberleşme standartlarında herhangi bir değişiklik yapma ihtiyacı da oluşmamaktadır.

Tezde sunulan yöntem pratikte uygulanabilir olup, 5G NR sinyalizasyonu ile uyumlu olarak çalışabilmektedir. Fakat, sistem parametrelerinde (frekans, kullanılan hüzme sayısı, anten dizin sayıları, anten açıları, güvenlik eşik değeri vb.) yapılacak herhangi bir değişiklik kendi senaryosunu yaratacağından DNN'in bu yeni değişikliklere uyum sağlayabilmesi için yeniden eğitilmesi gerekmektedir.

Önerilen DL tabanli yöntemi açıklayıp değerlendirebilmek için iki kanal modeli kullanılmıştır. İlk model karasal model olarak adlandırılmakta ve kullanıcı verileri bir ağ planlama yazılımından alınmaktadır. Bu yazılım, İstanbul/Büyükçekmece bölgesinde yer alan gerçek hücresel ağa ait üç boyutlu arazi verilerini kullanarak önceden belirlenen olası kullanıcı konumlarıdaki RSRP değerlerini hesaplamaktadır. Önerilen yöntemin etkinliğini ispatlamak amacıyla spesifik bir saha konfigürasyona ait birinci modele ek olarak genelleştirilmiş bir model daha sunulmaktadır. Bu ikinci model istatistiksel kanal modeli olarak adlandırılmakta olup, standartlarda belirlenen 5G NR sistem değişkenlerine göre kurgulanmış bir kanal modelinde üretilen sentetik verileri içermektedir. Böylece önerilen yöntemin, sadece belli özellikte bir kanala değil, sistem değişkenlerinin konfigüre edilebildiği ve rastlantısallık içeren kapsamlı bir ağ ortamı üzerinde denemesini de sunulmaktadır.

Tanımlanan senaryo ve kanal modellerine göre, benzetimler MATLAB ortamında gerçekleştirilmiştir. Her iki senaryo ve model için de herbirinde 96 nöron barındıran ve dört gizli katmandan oluşan bir DNN mimarisi kullanılmıştır. Giriş katmanında üç boyutlu kullanıcı konum bilgisi, çıkış katmanında ise hüzme çifti indeksleri kullanılmıştır. DL modeli olarak ise bu tarz sınıflandırma görevlerindeki ispat edilen başarısından dolayı çok katmanlı algılayıcı (MLP) modeli seçilmiştir. Sonuçlara geçilmeden önce tasarlanan DNN mimarisi üzerinde çeşitli kontroller yapılarak aşırı öğrenme problemine sahip olmadığı doğrulanmıştır. Performans analizi bölümünde çeşitli metrikler ele alınarak sistemin başarısı gösterilmiştir. İlk olarak, DNN modelinin tahmin performansı referans olarak alınan ML modelleri ile karşılaştırılarak değerlendirilmiştir. DNN'in ele alınan diğer iki ML algoritmasından daha üstün performans sergilediği gösterilmiştir. Ardından, en yüksek RSRP ve güvenli hüzme seçim algoritmaları için elde edilebilir maksimum RSRP seviyeleri çıkartılmıştır. Buradaki amaç, en yüksek RSRP'yi veren hüzme çifti ile bunu bir güvenlik kısıtı altında veren hüzme çifti arasındaki erişilebilir maksimum RSRP cinsinden karşılaştırmasını yapmaktadır. Böylelikle güvenli haberleşme için haberleşmenin başarısına zarar vermeden RSRP değerinden ne kadar bir ödünleşim yapıldığı gösterilmiştir. Sonraki adımda ise, güvenli ve başarılı kestirim olasılıkları üzerinden bir değerlendirme sunulmuştur. Burada da önerilen güvenli hüzme seçimi yönteminin mevcut ağlarda istatistiki olarak ne kadar bir güvenlik sağladığına dair benzetimlere yer verilmiştir. Son olarak, tek hücre ve çoklu-nokta iletim modelleri arasında güvenlik ve iletişimin erişilebilirliği açısından karşılaştırmalar gösterilmiştir.

Sayısal sonuçlar, önerilen DNN tabanlı hüzme seçim algoritmasının hem tek hücreli hem de çoklu-nokta iletim senaryoları için güvenli kapsama olasılığını önemli ölçüde iyileştirdiğini göstermektedir. Ayrıca, gerek en yüksek sinyal seviyesini veren gerekse en yüksek güvenliği sağlayan hüzme çiftinin seçimi görevlerinde, önerilen DNN

modelinin, hüzme seçim süreci sırasında tüketilen zaman ve enerjide önemli bir azalma sağladığı gözlemlenmiştir. Bu azalma, özellikle 5G ve ötesi ağlardaki gecikmeye duyarlı servisler için hayati önem taşımaktadır.

İlerleyen çalışmalarda, hüzme seçimi sonrasında, hem Tx hem de Rx tarafında hüzme iyileştirmesi ve hüzme değişimi prosedürlerinin optimize edilebileceği bir DNN şeması tasarımı ele alınabilir. Böylelikle kablosuz haberleşme sistemlerindeki geriye kalan hüzme yönetimi süreçlerinde de bir iyileştirme yapılabilir ve çeşitli açılardan (güvenlik, spektral ve enerji verimliliği) katkılar sağlanabilir.

Ayrıca, çoklu-nokta iletimi senaryoları için de geliştirmeler yapılabilir. Benzer şekilde CoMP ağlarında oluşabilecek herhangi bir bağlantı ya da servis kalitesi kaybı esnasında hüzme değişimi ya da hüzme kurtarma süreçlerinin DNN yapıları kullanılarak iyileştirilmesi de araştırmaya açık bir diğer konudur.

1. INTRODUCTION

In fifth generation (5G) systems, the integration of massive multiple-input-multiple-output (mMIMO) and coordinated multi-point (CoMP) transmission plays a crucial role in maximizing overall network performance, spectral efficiency, and coverage. When coupled with deep learning techniques, these technologies gain the capability to dynamically adapt and optimize, enhancing the overall efficiency of the network. Additionally, security is of paramount importance, encompassing not only cryptographic measures but also addressing physical layer vulnerabilities where eavesdropper attacks compromise communication confidentiality through unauthorized interception.

The use of mMIMO technology involves concentrating energy toward intended directions with high gains through its numerous antennas, employing spatial multiplexing. This leads to faster data rates, increased network capacity, and improved signal quality [1]. Consequently, it is essential to establish an efficient procedure for identifying an appropriate transmission point (TP) and searching for a suitable beam pair among all the beams between the transmitter (Tx) and the receiver (Rx). Given the highly dynamic and dense nature of 5G and beyond systems, this process can pose challenges, necessitating the development of fast, energy-efficient, and secure beamforming schemes [2].

On another front, CoMP transmission is a technique that enables multiple base stations (BSs) to collaborate and collectively serve a user or a cluster. Through coordinated transmissions, these BSs can offer improved coverage and higher data rates, particularly at cell edges [3]. CoMP can be applied in various ways, such as joint transmission (JT), where a UE concurrently receives transmissions from multiple BSs, or dynamic point selection (DPS), where the optimal BS is selected for transmission based on the user's location and channel conditions.

1.1 Problem Statement

The beam management's initial access phase, known as procedure P-1, is formally outlined in standard TR 38.802 [4] by the 3rd generation partnership project (3GPP). This involves using synchronization signal blocks (SSB) broadcasted as a transmit burst, along with beam sweeping at both transmit/receive and UE ends, to create a link between beam pairs. To optimize spectral efficiency between the Tx and Rx, it is crucial to identify the best beam pair based on the reference signal received power (RSRP). To achieve this, a thorough exploration is carried out across all potential combinations of Tx and Rx beam pairs. The expanding quantity of antenna elements, leading to a rise in the number of beams with mMIMO, amplifies the complexity of the initial access procedure, particularly in relation to latency and energy consumption [5]. The widespread adoption of 5G networks demands a swift, energy-efficient, and secure initial access.

Furthermore, the integration of mMIMO and CoMP transmission within 5G networks facilitates effective resource allocation and interference control. These technologies collectively empower 5G networks to attain not only elevated data rates and expanded coverage but also heightened security. However, the utilization of CoMP with mMIMO poses greater challenges compared to traditional cellular networks because coordination involves not only overseeing transmissions from pre-determined cells but also selecting a combination of beams from each point.

1.2 Aim and Objectives

In this thesis, we present two transmission models. The first model introduces a deep neural netwok (DNN)-based approach for secure initial access and beam selection in the presence of a single serving cell. In this model, the SSB beam sweeping procedure is automated using a DNN, serving as a proof of concept to showcase the compatibility of the proposed DNN with existing standards. Unlike conventional methods, which prioritize the beam pair with the highest signal strength, our method entails choosing a beam pair. This selection is not only based on maximizing the signal strength for the UE but also strives to ensure that the RSRP observed by potential eavesdroppers remains below a specified threshold. Protection to safeguard from eavesdropping

attacks is achieved through the inherent characteristics of mMIMO and beamforming, eliminating the need for additional security measures such as injecting artificial noise, generating secure keys, employing directional modulation, and others [6].

The second model addresses the beam selection challenge in networks utilizing mMIMO and DPS-CoMP for secure radio coverage. In this context, we propose a DNN-based CoMP beamforming algorithm for forecasting the indices of the most secure beam pair between multiple coordinated TPs and the UE. This model aligns with the same motivation as the single-cell scenario, emphasizing the need for secure communication in multi-point transmission configurations.

In the single-cell transmission scenario, we introduce a system for autonomous beam management, utilizing DNNs, developed to forecast the indices of the most secure beam pair between the BS and the UE in the initial access procedure. The inherent properties of mMIMO and beamforming offer a precise level of protection against eavesdropping attacks without the need for additional security mechanisms. Our proposed scheme aligns with 5G NR signaling without necessitating modifications to the standard. It relies solely on the users' positions as input, excluding the necessity for channel information parameters.

In the context of multi-point transmission scenario, our focus extends to addressing the beam selection challenge within networks employing massive multiple-input-multiple-output (mMIMO) and dynamic point selection (DPS) in CoMP configurations to ensure secure radio coverage. We propose a novel CoMP beamforming scheme based on DNN to predict the most secure beam pair indices between multiple coordinated TPs and the UE.

Our proposed beam management system aims to optimize the beam search/sweeping process, focusing on reducing latency and energy consumption by narrowing down the search space. Prioritizing communication security, we assess the system's performance in two scenarios. The first involves real data from a radio network planning software, calculating RSRP values based on parameters from existing cells and actual 3D terrain information. The second scenario is artificial, generated using a statistical channel model with 5G NR system variables defined in 3GPP procedure P-1. In both

scenarios, we conduct two experiments: one maximizing RSRP and the other, while also maximizing RSRP, adheres to security constraints.

To minimize beam search overhead, the DNN focuses on the K best beam pairs rather than an exhaustive search. We evaluate the prediction accuracy and the achieved RSRP level by the best beam pair within these $Top-K$ pairs. Our contribution introduces a novel DNN-based secure initial access and beam alignment procedure, the first of its kind in the literature. The main contributions of the thesis can be outlined as follows:

- The proposed method includes a substantial reduction in beam search latency and energy consumption compared to the standard P-1 procedure.
- During the initial access and beam alignment procedure for a single-cell scenario, we prioritize selecting the pair with the highest RSRP ensuring secure communications when possible. This approach extends to CoMP transmission, allowing the prediction of the most secure beam pair indices between multiple coordinated TPs and the UE.
- Beyond its primary function, CoMP is leveraged to enhance data security by safeguarding against eavesdroppers.

1.3 Outline

Chapter 1 commences with an introduction, setting the context for the thesis and presenting the addressed problem. Clear aims and objectives are outlined. Chapter 2 encompasses background knowledge, covering essential concepts in telecommunication and computer science relevant to the study. It also reviews papers from previous years related to the study. In Chapter 3, detailed procedures for beam management in 5G NR are provided. Chapter 4 outlines the methodology employed in this thesis and explains the intricate DNN-based secure beamforming scheme. Chapter 5 presents and analyzes the research results for justification. Chapter 6 concludes the results and underscores the research gap for further exploration.

2. TECHNICAL BACKGROUND AND RELATED WORK

In this chapter, the wireless communication concepts, which constitute the basis of our research, will be analyzed and explained. Subsequently, a summary of the related works in this area will be provided.

2.1 5G and Beyond Networks

The surge in mobile subscribers worldwide, coupled with the proliferation of data-intensive applications on user terminals, underscores the imperative for wireless services characterized by full connectivity, reliability, and high data rates [7]. Approximately every decade witnesses the emergence of a new generation of mobile networks [8]. The first generation, commonly referred to as 1G (though not officially named as such), made its debut in the 1980s, operating in an analog format and exclusively supporting voice calls. Subsequent to this, three transformative updates unfolded, denoted as the second, third, and fourth generation networks—2G, 3G, and 4G, respectively [9]. The 2G era, embodied by the global system for mobile communications (GSM) signified a pivotal shift from analog to digital signaling in the 1990s. This transition laid the groundwork for an expanded array of services beyond voice calls as part of its evolutionary trajectory, incorporating text messaging and rudimentary internet services. With the dawn of the new century, 3G emerged forth accelerated internet access and the advent of video calling. Launched in the 2010s and persisting today, the 4G era brought about notably faster data rates, enabling services such as high-definition video streaming and the ability to accommodate a substantial number of subscribers in a single cell. In 2019, the deployment of 5G networks began, initially positioned as the catalyst for the applications demanding higher data bandwidth and reasonable latency. [10]. With each evolutionary leap in wireless generations, the demand for additional services propelled the need for faster data rates, necessitating a transition to channels with increased bandwidth [11].

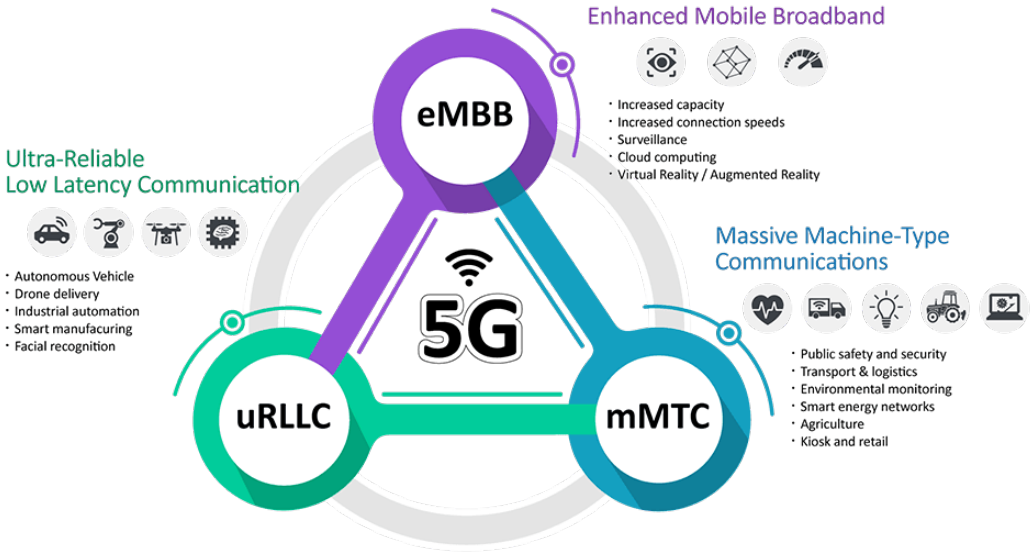


Figure 2.1 : 5G usage scenarios of International Mobile Telecommunications (IMT)-2020

Building on the performance enhancement strategies initiated in 3G and continued through 4G, 5G inherits a trajectory of deploying more hardware and utilizing additional spectrum to achieve performance gains. Similar to its predecessors, 5G is expected to undergo continuous evolution. The initial deployment approach, in many instances, centers on the 3GPP NR standard for dense areas, utilizing the band between 2 and 6 GHz. Alternate strategies involve utilizing lower frequency ranges in the millimeter-wave (mmWave) band, employing mMIMO technologies, beamforming and small cell densification.

Within the framework of 5G, three distinct service options are made available: enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC), and massive machine-type communication (mMTC) as illustrated in Figure 2.1. Each targets improved data rate, reduced transmission latency, and enhanced connectivity performance, respectively [12]. However, it is important to note that achieving these targets simultaneously is a challenge, and a compromise between them must be sought. Currently, key performance indicators (KPIs) for 5G include a peak data rate on the order of 1 Gb/s, end-to-end transmission delay of 5 ms, and processing delay of 100 ns. The next evolution, termed beyond 5G (B5G), is

envisioned to significantly enhance these KPIs, targeting a peak data rate of 100 Gb/s, end-to-end transmission delay of 1 ms, and processing delay of 50 ns [10].

Looking ahead, the objective of the sixth generation (6G) network is to revolutionize wireless evolution by shifting from merely having "connected things" to fostering "connected intelligence" [13]. 6G aims to seamlessly integrate applications covering a range of autonomous driving to extended reality (XR). Crucially, 6G should incorporate sustainability into mobile network developments and eliminate the existing digital disparity by ensuring universal access to digital information, addressing a gap where 5G fell short. The fundamental requirements for 6G networks include achieving fast data rates, exceptional reliability, and minimal latency for a variety of devices practically simultaneously. The essential prerequisites for 6G networks can be outlined as follows [13]–[15]:

- **Exponential Data Rates:** 6G is envisioned to demand Incredibly fast data transmission rates, reaching the order of 1 Tb/s, reflecting the ever-growing appetite for data-intensive applications.
- **Minimal Latency:** To support critical verticals, 6G necessitates very low end-to-end transmission latency, aiming for duration of less than 1 ms, ensuring rapid and responsive communication.
- **Utilization of Higher Frequency Bands:** Channel capacity theory guides the utilization of higher frequency spectrum with wider bandwidth channels. This entails a shift to frequencies beyond 6 GHz, extending to ranges above 86 GHz, and even exploring unconventional communication methods such as visible light communication (VLC).
- **Energy Efficiency:** The pursuit of high data rates in 6G mandates a thorough consideration of energy efficiency, focusing on minimizing the energy expended per transmitted bit.
- **Ubiquitous 3D Network:** The vision for 6G entails a pervasive, three-dimensional, and continuously accessible broadband global network. Achieving wide coverage involves the integration of terrestrial cellular networks with non-terrestrial

networks, encompassing satellite and aerial systems, as well as underwater communication links.

- **Connected Intelligence with Machine Learning:** Due to the intricate characteristics of the network, the realization of a ubiquitous 3D network requires 6G to manifest in the form of connected intelligence, incorporating machine learning capabilities to manage the network's complexity effectively.
- **Evolution of Service Classes:** Beyond the existing eMBB, URLLC, and mMTC services, 6G anticipates the emergence of new service classes, reflecting the evolving demands and complexities of future communication needs.

As anticipated, there are varying perspectives among research groups regarding the number and nature of service classes expected in 6G [9,10,12,13,16]. These service classes involve a balance of factors such as achievable distance, speed, latency, power consumption, among others. Broadly, there is a convergence of ideas, envisioning some services as human-centric and others as machine-centric. According to [17], four fundamental services are proposed:

1. Mobile Broadband Reliable Low Latency Communication (MBRLLC): MBRLLC is crafted to fulfill demanding criteria for speed, dependability, and response time, while also addressing energy efficiency and low-rate reliability latency in mobile settings. This service category encompasses applications such as XR, autonomous vehicles, drones, as well as traditional eMBB and URLLC services.
2. Massive URLLC (mURLLC): mURLLC integrates ultra-high reliability with extensive connectivity and scalability in URLLC. This category encompasses applications like the Internet of Things (IoT), sensing, robotics, and blockchain.
3. Human-Centric Services: These services revolve around collecting data to enrich the quality of the human physical experience.
4. Multi-Purpose 3CLS and Energy Services (MPS): The term 3CLS denotes the merging of communication, computing, control, localization, and sensing. These services strive to attain elevated control stability, minimal computing latency,

Table 2.1 : Requirements and KPIs of 5G, B5G and 6G.

Requirement/KPI	5G	B5G	6G
Application types	eMBB, URLLC, mMTC	Reliable eMBB, URLLC, mMTC, hybrid	MBRLLC, mURLLC, Human-centric services, MPS
Device type	Smartphones, sensors, drones	Same w/ 5G + XR equipment	Same w/ B5G + robotics, telemedicine
Data rate	1 Gb/s	100 Gb/s	1 Tb/s
End-to-end delay	5 ms	1 ms	<1 ms
Processing delay	100 ns	50 ns	10 ns
Reliability	99.999%	99.9999%	99.99999%
Power efficiency	–	–	1 pJ/b
Spectral efficiency	30 b/s/Hz	30 b/s/Hz	100 b/s/Hz
Jitter	–	–	1 μ sn
Location precision	20 cm (2D)	20 cm (2D)	1 cm (3D)

precise localization, accurate sensing and mapping, low latency, and reliable communication—all while adhering to specified energy guidelines for information transfer. Applications include connected robotics and autonomous systems, telemedicine, environmental imaging or mapping, and specific instances of XR services.

A thorough analysis of Table 2.1 reveals a more intricate examination of the requirements and KPIs for 6G, along with a comparative assessment against the attainments of 5G and B5G [10,18,19].

2.2 Massive MIMO and CoMP Techniques

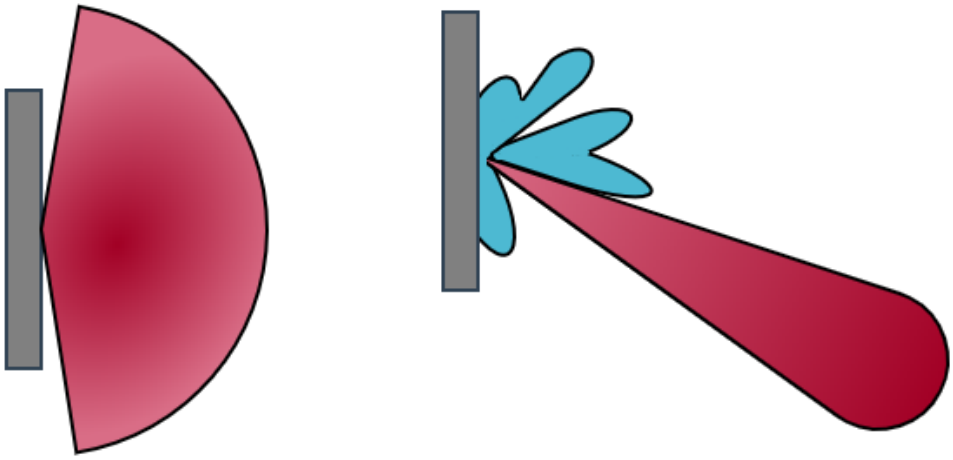
2.2.1 Massive MIMO systems

mMIMO technology is a crucial element in 5G wireless systems and beyond. Its significance lies in its ability to provide high spectral efficiency to numerous users simultaneously through straightforward signal processing. mMIMO emerges as a promising technique for attaining high spectral and energy efficiency in wireless systems [20]. In mMIMO, a large antenna array at the BS serves a comparatively fewer number of users (few tens), resulting in substantial processing gain and improved

performance compared to conventional MIMO systems [21]. Despite the advantages it offers, the practical implementation of mMIMO encounters hurdles. This is due to the fact that each transmit antenna at the BS and multi-antenna users requires dedicated signal processing resources like radio frequency (RF) chains, power amplifiers, and additional circuitry. Consequently, this results in heightened power usage and increased architectural intricacy. Moreover, it becomes essential to ensure reliable signal detection of spatially multiplexed information streams at the receiving end. This is particularly crucial due to inter-channel interference, which involves the interference between multiple streams transmitted from the antennas of the same user or BS. This consideration is vital for achieving URLLC. [22].

While the concept of MIMO dates back to the 1990s, initially termed as spatial division multiple access [23], its practical implementation in wireless networks was not financially viable at that time. This was primarily due to the use of a limited number of antennas, which resulted in negligible data throughput gains. The landscape changed with the introduction of MIMO in 4G and mMIMO in 5G, where 5G base stations in various countries now deploy 64 fully digital transceiver RF chains, each equipped with multiple MIMO antennas. Looking ahead to 6G, it is anticipated that antenna structures with higher counts than mMIMO, commonly referred to as ultra-massive MIMO (umMIMO), will be employed. Additionally, MIMO applications in the VLC domain, utilizing light-emitting diode (LED) arrays and multiple photodetectors, have also been explored [24,25].

The MIMO transmitter plays a crucial role in beamforming, a concept that can be illustrated effectively through Figure 2.2 [23]. This figure compares the signals emitted by a traditional base station (Figure 2.2(a)) with the beamformed signal produced by a MIMO antenna array (Figure 2.2(b)), where the array comprises M antennas. Unlike the conventional base station, which emits a single, broadly distributed signal (common in 2G and 3G), the antenna array can focus the signal in a specific direction, directed towards a user. Beamforming and beam steering involve adjusting the amplitude and phase shift of the signal at each antenna element, accomplished in analog, digital, or hybrid manners [26]. When M antennas are employed, users experience a signal strength that is M times greater than what they would observe with just one antenna.



(a) The classical BS radiates one signal uniformly into its coverage area.

(b) A MIMO BS radiates multiple signals (indicated by different colors) that are focused at their respective receivers.

Figure 2.2 : The difference between classical communication systems and MIMO.

However, a limitation is that signal strength in any direction other than the beam's direction is nearly zero. Despite this drawback, each antenna can be controlled individually, enabling the simultaneous service of K users (where $K \leq M$). Each user perceives the signal strength of M/K, generated by what is referred to as an antenna subarray. It's important to note that the gain and beam width are influenced by the subarray's size, making scenarios where $M >> K$ the preferred operating mode in MIMO for maintaining high received signal strength. To sustain this condition as the number of users (K) increases, M should be increased accordingly. As M increases, MIMO transitions to mMIMO and eventually umMIMO. For scenarios with an even higher user count, multiple transceivers (each with multiple antennas) are introduced, forming transceiver chains. For instance, umMIMO scenarios envision the possibility of 1,024 transceivers, each with 1,024 antennas, allowing for 1 THz transmissions [27].

mMIMO and umMIMO have garnered considerable interest for 5G and 6G, respectively, due to several compelling reasons [23]:

- Advances in integrated circuit and packaging technologies have reached a stage where the cost of constructing antenna arrays is no longer prohibitive.

- The evolution of information theory has progressed to a point where the selection of the appropriate operating regime is no longer a significant concern.
- The signal-processing complexity required for the construction and control of MIMO systems has become manageable, even within a small form factor.
- The inclusion of a large number of antennas provides unprecedented spatial resolution, enhancing robustness against small-scale fading and the capability to suppress interference effectively.

2.2.2 Comparison of SISO, MIMO and massive MIMO systems

Single-input single-output (SISO) systems employ a single radiating element at both the Tx and Rx ends. In contrast, MIMO systems utilize multiple elements at both ends. Compared to SISO systems, MIMO systems exhibit significantly enhanced system throughput and reliability. The multiplexing gain, diversity gain, and array gain of MIMO antenna systems are notably higher than those of SISO antenna systems [20,28].

The diversity gain in MIMO is influenced by the number of channels between the Tx and Rx ends, which can be increased by incorporating more channels. On the other hand, achieving maximum multiplexing gain in a MIMO system is possible with fewer antennas at the Tx and Rx ends. Therefore, there is an inherent trade-off between these two gains, making it challenging to optimize them simultaneously [28].

In mMIMO systems, a greater number of radiating elements are employed compared to conventional MIMO systems [29]. The system's performance can be evaluated across four scenarios: SISO antenna system, single-user MIMO (SU-MIMO) antenna system, multi-user MIMO (MU-MIMO) system, and mMIMO system. The communication model involves N_t transmitting antennas at the transmitter end and M_r receiving antennas for each K_u user at the receiver end.

1. **SISO System [$N_t = 1$, $M_r = 1$ and $K_u = 1$]:**
   A SISO system consists of a single element in each transmitter and receiver module, communicating through a single channel as depicted in Figure 2.3. In the SISO

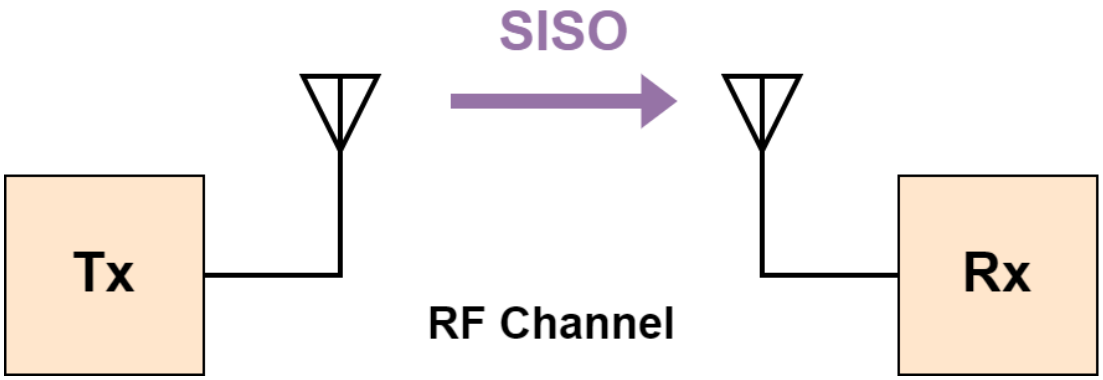


Figure 2.3 : Systematic representation of SISO systems.

configuration, both the Tx and Rx possess only one antenna each. The received signal, denoted as y is expressed as

$$y = Hx + n, \tag{2.1}$$

where H represents the channel matrix. x is the transmitting vector and n is the noise vector which is additive white Gaussian noise (AWGN). The noise follows a complex normal distribution function denoted as $CN(0,\sigma)$, where the mean is zero, and the standard deviation is σ. In the case of a SISO system, the channel matrix H is a scalar, one-dimensional entity, so the received signal y can be expressed as SISO channel capacity (bits/s/Hz) as per the formulation provided in [30].

$$C_{SISO} = \log_2(1+\gamma) = \left(1 + h^2 \frac{P_t}{\sigma_n^2}\right). \tag{2.2}$$

In here, the channel coefficient is denoted by h, transmitted power by P_t, noise power by σ_n^2, and the signal-to-noise ratio (SNR) by γ. Consequently, improving the channel capacity of a SISO system involves elevating the SNR.

2. **SU-MIMO System [$N_t > 1$, $M_r > 1$ and $K_u = 1$]:**
   A single-user MIMO (SU-MIMO) system consists of multiple elements in both the transmitter and receiver modules. Communication occurs through multiple parallel channels, each dedicated to a single user, as illustrated in Figure 2.4.

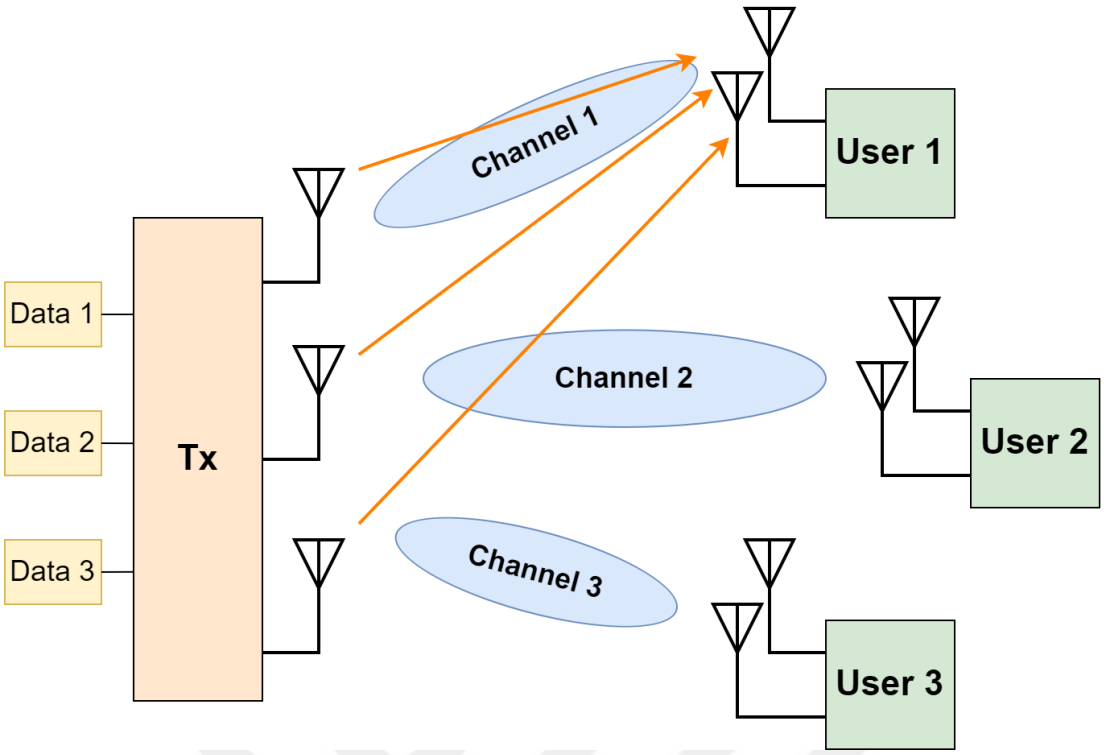


Figure 2.4 : Systematic representation of SU-MIMO systems.

In a MIMO antenna system, both spectral efficiency and data rate experience a significant increase, and this enhancement occurs without impacting the SNR or bandwidth. This improvement is attributed to the presence of multiple antennas at both the Tx and Rx sides. The augmented channel capacity of a MIMO system arises from spatial multiplexing, achieved through the simultaneous transmission of multiple channels from various radiating elements [31]. However, this added channel capacity comes with trade-offs in terms of physical space (especially in mobile handsets), deployment costs associated with multiple radiating elements, and increased signal processing complexity [32]. In a SU-MIMO system, only one user is served during a single transmission time interval among K potential users. The received signal vector in this context can be described as

$$y_m = \sqrt{\rho} H_{mn} x_n + n_m, \tag{2.3}$$

where x_n is transmit signal vector ($x_n \in C^{N_t \times 1}$), n_m is the noise vector ($n_m \in C^{M_r \times 1}$), and n is the transmitting antennas ($n = 1, \cdots, N_t$), m is the receiving antennas

($m = 1, \cdots, M_r$). H_{mn} is the channel matrix, ρ is the normalized transmit power, and the total power of the system is unity ($E\|x_n\|^2 = 1$). The channel capacity (bits/s/Hz) of a SU-MIMO system can be expressed as

$$C_{SU-MIMO} = \log_2 \left| I + \frac{\rho}{N_t} HH^* \right|, \tag{2.4}$$

where I represents the identity matrix and the channel capacity of SU-MIMO system is bounded by

$$\log_2 (1 + \rho M_r) \leq C_{SU-MIMO}, \tag{2.5}$$

$$\log_2 (1 + \rho M_r) \leq \min (N_t, M_r) \log_2 \left(1 + \frac{\rho \max (N_t, M_r)}{N_t} \right). \tag{2.6}$$

3. **MU-MIMO System [$N_t > 1$, $M_r > 1$, $M_{K_u} = 1$ and $K_u = 1$]:**
   A MU-MIMO system incorporates multiple components in both the transmitter and receiver modules, facilitating communication through several channels assigned to individual users, as depicted in Figure 2.5.

   MU-MIMO presents numerous advantages over the SU-MIMO system. These include: (i) achieving multi-user diversity in the spatial domain by efficiently distributing total resources among multiple users with spatially correlated channels [33]; (ii) enabling MU-MIMO transmitting antennas to simultaneously send signals to numerous users, allowing the use of a single antenna at the user end to reduce system costs; (iii) exhibiting a relatively lower sensitivity to propagation issues [34]. The received signal vector ($y_k \in C^{K_u \times 1}$) of a MU-MIMO system can be formulated as

$$y_k = \sqrt{\rho} H_{k,n} x_n + n_k, \tag{2.7}$$

where $H_{k,n}$ represents the channel matrix ($H_{k,n} \in C^{K_u \times N_t}$), x_n is the transmit signal vector ($x_n \in C^{N_t \times 1}$), and n_k is the noise vector ($n_k \in C^{K_u \times 1}$) of the MU-MIMO system. The capacity of a MU-MIMO system can be expressed as

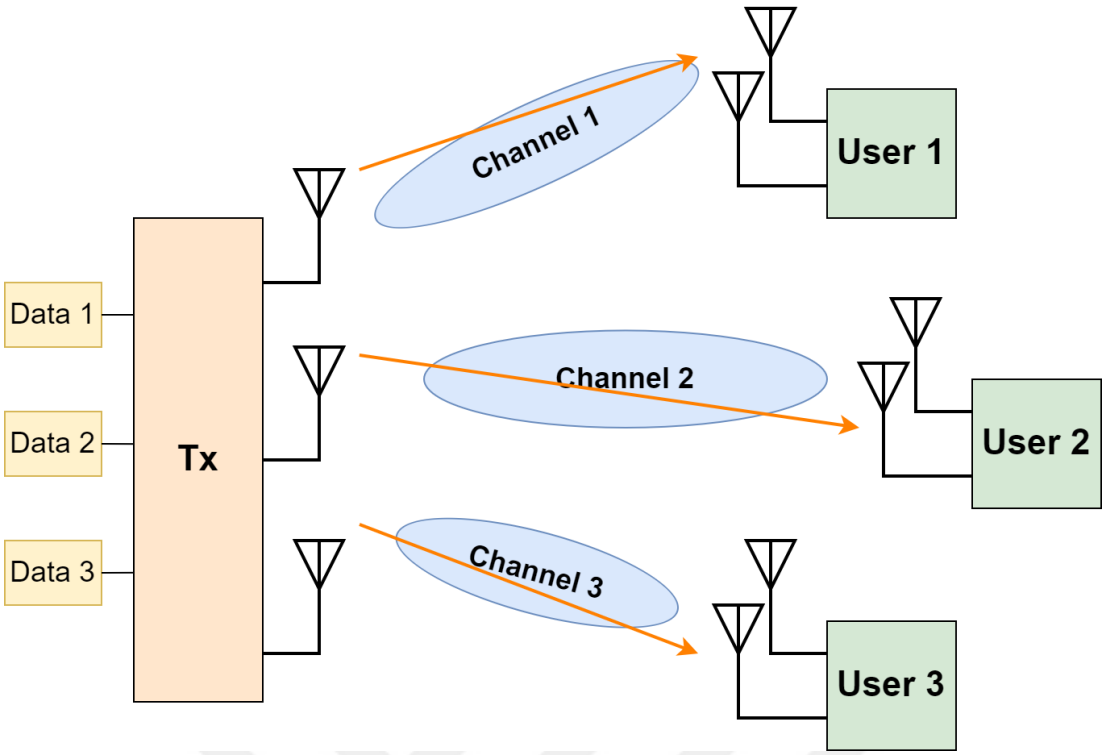


Figure 2.5 : Systematic representation of MU-MIMO systems.

$$C_{MU-MIMO} = \max \log_2 |I + \rho HPH^*| . \tag{2.8}$$

Here, P is a diagonal power matrix ($P = p_1,\ p_2,\ \cdots,\ p_k$) with power allocation. In recent times, diverse MU-MIMO antenna systems have been developed owing to their enhanced system performance concerning capacity and reliability [33].

4. **Massive MIMO System [$N_t \gg M_r$ and $N_t \to \infty$ or $M_r \gg N_t$ and $M_r \to \infty$]:**
   The mMIMO system shares similarities with MU-MIMO, but it distinguishes itself by having an exceptionally large number of radiation elements in either the transmitter or receiver module, as depicted in Figure 2.6.

   In a mMIMO system, the spectral efficiency experiences a tremendous boost due to the presence of a vast number of antennas [20,29]. Under the initial condition where the number of transmitting antennas N_t is significantly larger than the number of receiving antennas M_r and tends towards infinity ($N_t \gg M_r$ and $N_t \to \infty$), the channel capacity of the mMIMO system can be expressed as

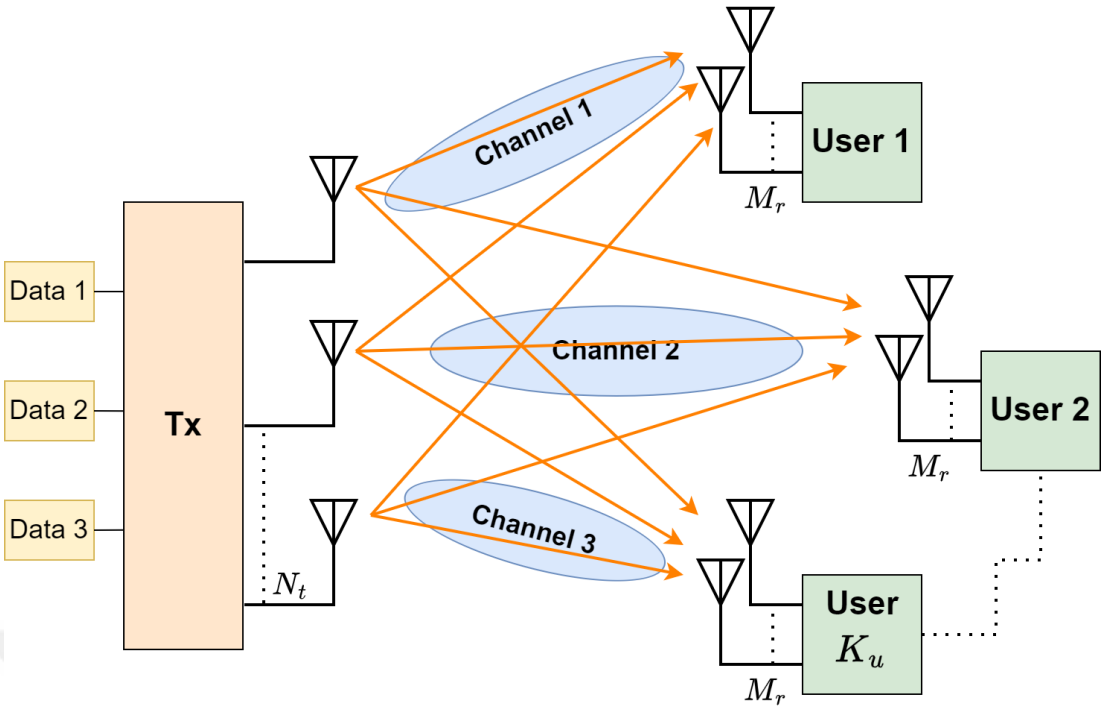


Figure 2.6 : Systematic representation of mMIMO systems.

$$C_{mMIMO} \approx M_r \log_2 (1+\rho). \tag{2.9}$$

Under the second condition, where the number of receiving antennas M_r is significantly larger than the number of receiving antennas N_t and tends towards infinity ($M_r \gg N_t$ and $M_r \to \infty$), the channel capacity becomes

$$C_{mMIMO} \approx N_t \log_2 \left(1+\frac{\rho M_r}{N_t}\right). \tag{2.10}$$

These two equations reveal that the channel capacity of a mMIMO system exhibits a linear increase with the growing number of antennas at both the Tx and Rx ends.

2.2.3 Coordinated multi-point transmission

CoMP transmission is a strategy enabling multiple BSs to collaborate and jointly cater to a user or a cluster. Through synchronized transmissions, these BSs enhance coverage and elevate data rates, particularly at cell peripheries [3]. The transmitting BS, referred to as the TP in CoMP systems. A CoMP network enhances signal quality

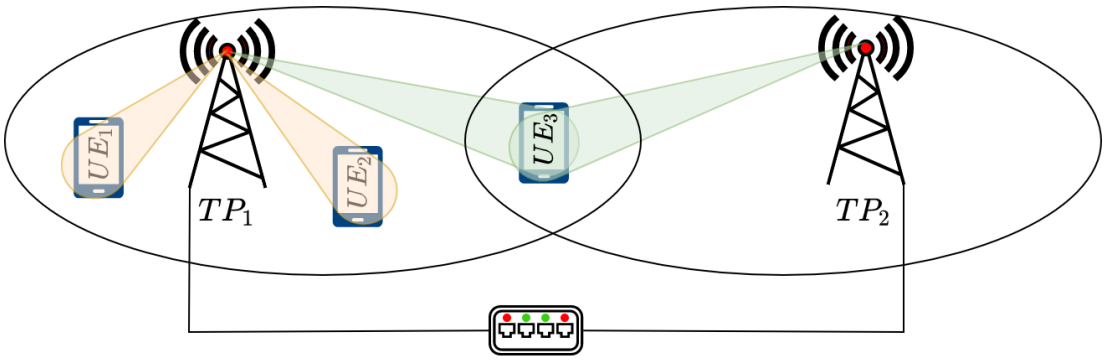


Figure 2.7 : CoMP transmission scheme with two geographically isolated TPs.

for users by coordinating TPs, thereby mitigating interference and improving the user signal-to-interference and noise ratio (SINR). CoMP schemes have found application in 4G and 5G technologies, particularly in scenarios where neighboring cells use the same frequency bands without code and/or time division. The reuse of frequency bands poses challenges, especially for cell-edge users experiencing potential interference. To address insufficient SINR at cell edges, TPs can coordinate their transmissions to minimize interference, or multiple TPs can transmit to a user. In the latter case, TP signals can either be identical to provide a strong signal to the user or carry different components (in terms of time, code, etc.). Strict synchronization is crucial, especially if TPs are geographically isolated, as depicted in Figure 2.7.

CoMP in the downlink direction involves coordinated scheduling and beamforming (CS/CB), joint transmission (JT) and dynamic point selection (DPS), while CoMP in the uplink includes coordinated scheduling (CS) and joint reception (JR) techniques [35]. In downlink CS/CB, one of the coordinated cells is selected as the transmission cell for communication with the user, reducing interference at the cell edge. Dynamic decisions on user scheduling and beamforming occur after coordination among all CoMP set points, with each UE's data transmitted exclusively by its designated transmission cell [36]. In JT-CoMP, multiple TPs simultaneously transmit data to the UE. In the DPS approach, UE data is accessible at several BSs within the coordinating set. However, only one BS transmits data at any given time. The TP can be altered from subframe to subframe to optimize transmission for a UE with fluctuating channel conditions. This situation is particularly probable at a cell edge, where the

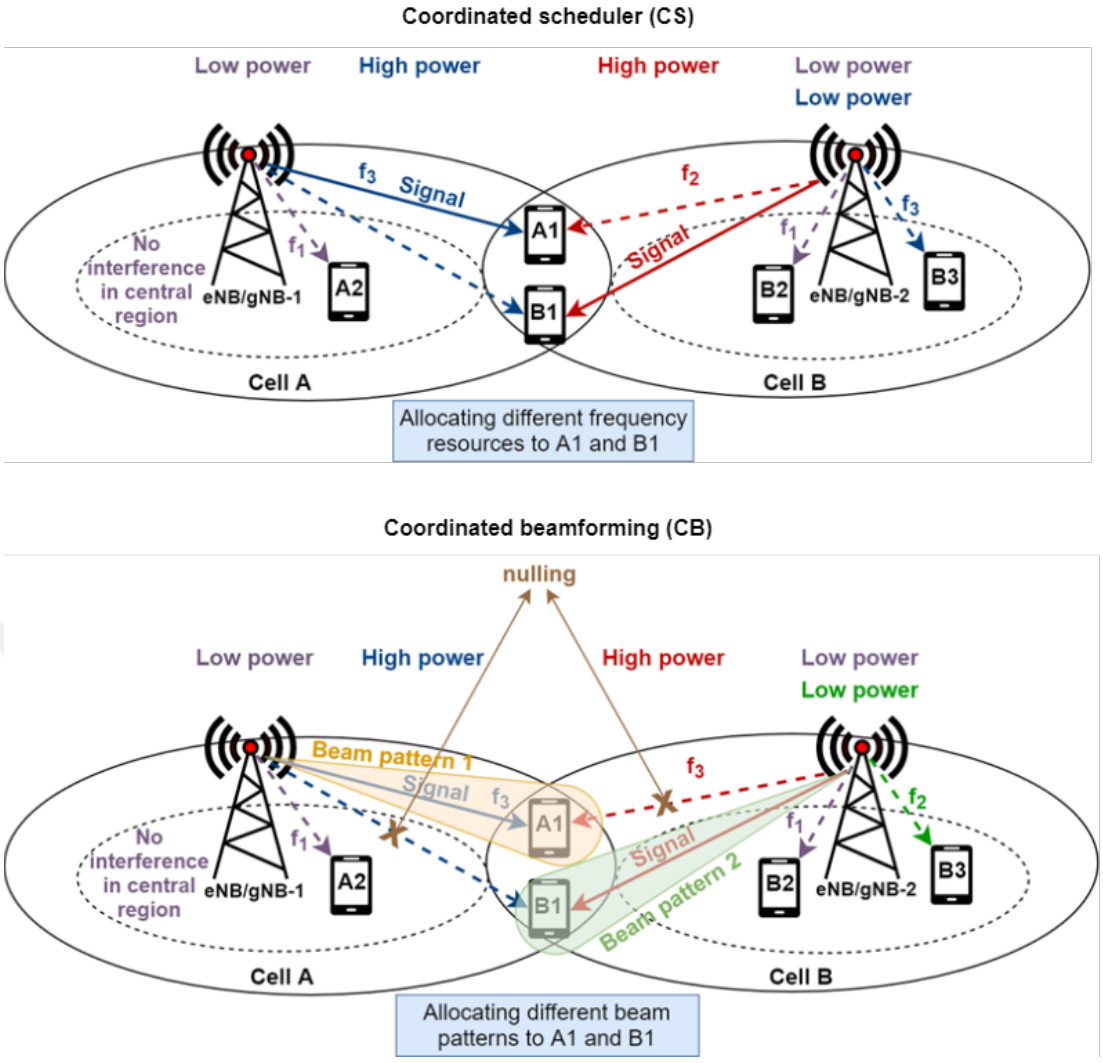


Figure 2.8 : The downlink CoMP schemes: coordinated scheduling and beamforming (CS/CB).

serving BS benefits from favorable long-term channel characteristics, but short-term characteristics may favor other collaborating BSs. A depiction of these downlink CoMP schemes is given in Figures 2.8 and 2.9.

Uplink CS involves identifying the coordinated cell cluster that serves a specific UE. The objective is to maximize cell throughput while maintaining an acceptable level of scheduling complexity and backhaul overhead. In uplink JR, the UE transmits to multiple TPs simultaneously, with cooperative processing of the data [37].

CoMP scenarios are also defined in 3GPP Release 11 and Release 12 [38,39] for 4G networks. CoMP is anticipated to be a pivotal element in the widespread deployment

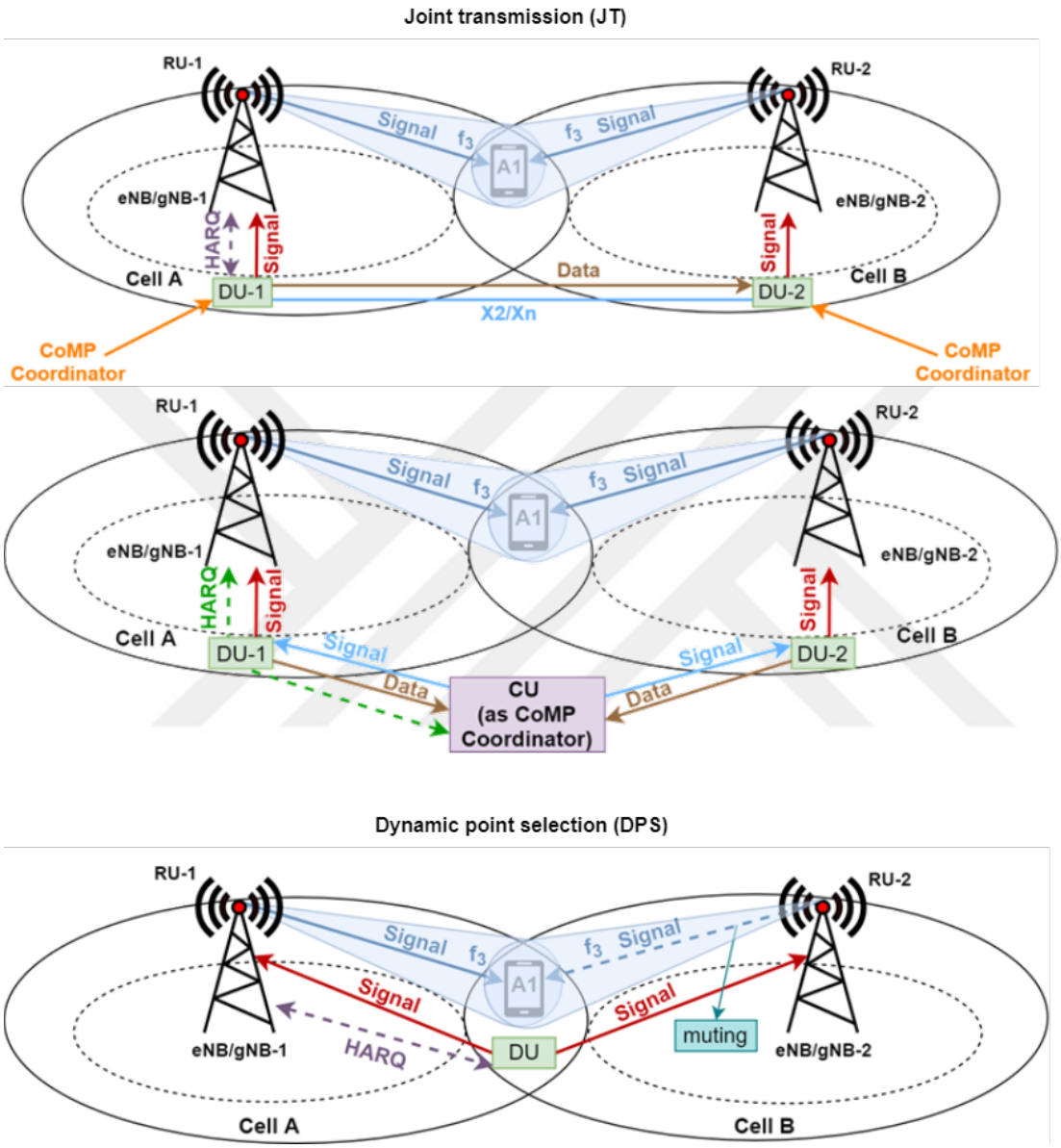


Figure 2.9 : The downlink CoMP schemes: joint transmission (JT) and dynamic point selection (DPS).

of 5G, given the denser nature of 5G networks. Interference avoidance techniques like CoMP are critical due to the increased network density in 5G, and the new architectures, such as Centralized-RAN (C-RAN), control/data plane split, low latency backhaul, etc., are expected to facilitate CoMP deployment.

The distinctive aspect of 5G and subsequent networks lies in the variety of services they offer, catering to diverse user needs. Yet, the demands for these services often conflict, highlighting the importance of a coordinated and adaptable network architecture. While CoMP systems were initially introduced to enhance cell edge performance in 4G, their collaborative nature can now be harnessed to meet the varied requirements and enable technologies for 5G and beyond networks [40].

2.3 Physical Layer Security

As depicted in Figure 2.10, wireless systems face three primary types of attacks. In *eavesdropping* [41], a malicious node or attacker attempts to intercept the ongoing transmission between the legitimate transmitter (Alice) and receiver (Bob). It's important to note that eavesdropping goes beyond extracting transmitted data between legitimate nodes; it can also encompass capturing additional information such as user behavior or network usage patterns. Typically, eavesdropping attacks are passive in nature, exerting no direct impact on the system. Consequently, detecting the presence of an eavesdropper within the system becomes a more challenging task [42]. Conversely, a *jammer* [43] aims to disrupt legitimate wireless transmissions by transmitting noise-like signals on the same time–frequency resources, degrading the perceived link quality at the legitimate transceivers. The *spoofer* [44] represents the most sophisticated attack, intending to deceive legitimate nodes into believing it is also a legitimate device. Once the spoofer infiltrates the network, it can send misleading messages to the legitimate receiver.

Traditional security measures for communication networks predominantly depend on cryptographic techniques [38]. However, alongside established security methods, there is a growing interest in novel security approaches grounded in the principles of information theory. These approaches center on leveraging the secrecy capacity of the wireless channel to enhance data security.

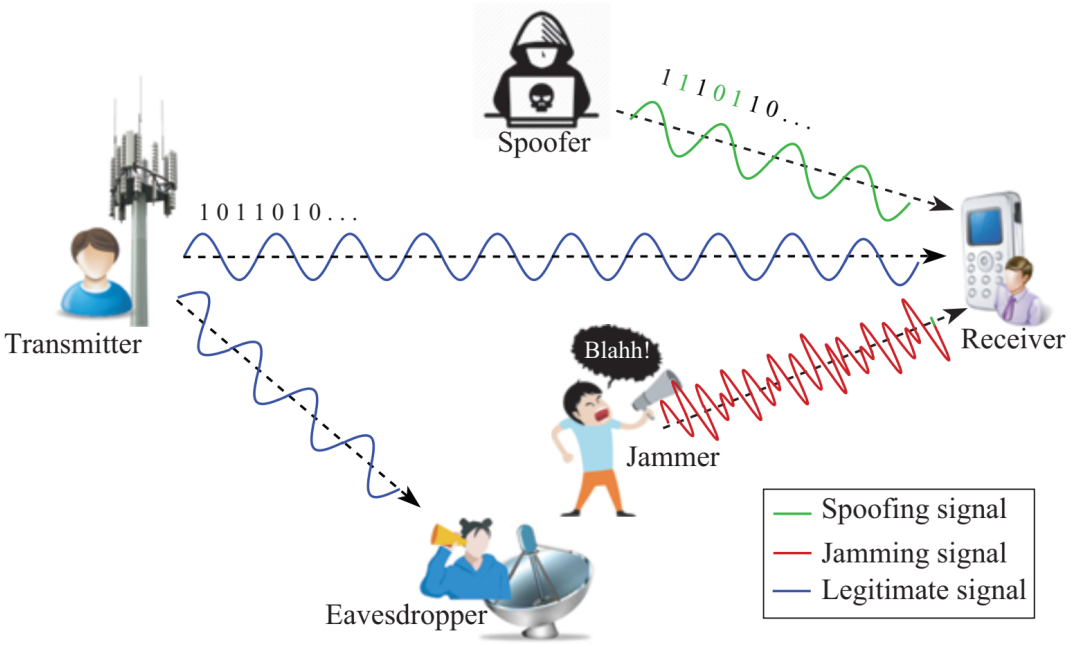


Figure 2.10 : Illustration of main security threats at the physical layer.

Physical layer security (PLS) constitutes a set of information-theoretic security techniques designed to ensure confidentiality. The fundamental concept driving PLS is to leverage the inherent attributes of the wireless channel, including factors like noise, fading, interference, dispersion, diversity, and more. This approach aims to enable legitimate users to effectively communicate and decode data, while thwarting malicious users from doing so. With the increasing significance of PLS in the context of 5G and future networks, there is a growing focus in the literature on exploring the possibilities and addressing the challenges associated with achieving robust data security at the physical layer [41]. This involves adapting to the requirements of emerging technologies and considering the potential opportunities presented by PLS.

PLS, introduced by Wyner [45], has emerged as a promising approach to address the escalating secrecy requirements within the framework of information theory. Recent research on PLS is particularly focused on cooperative and heterogeneous cellular networks as a means of overcoming security challenges in 5G network interoperability. With the growing demand for mobile traffic, cost-effective and adaptable solutions are essential for 5G and future networks.

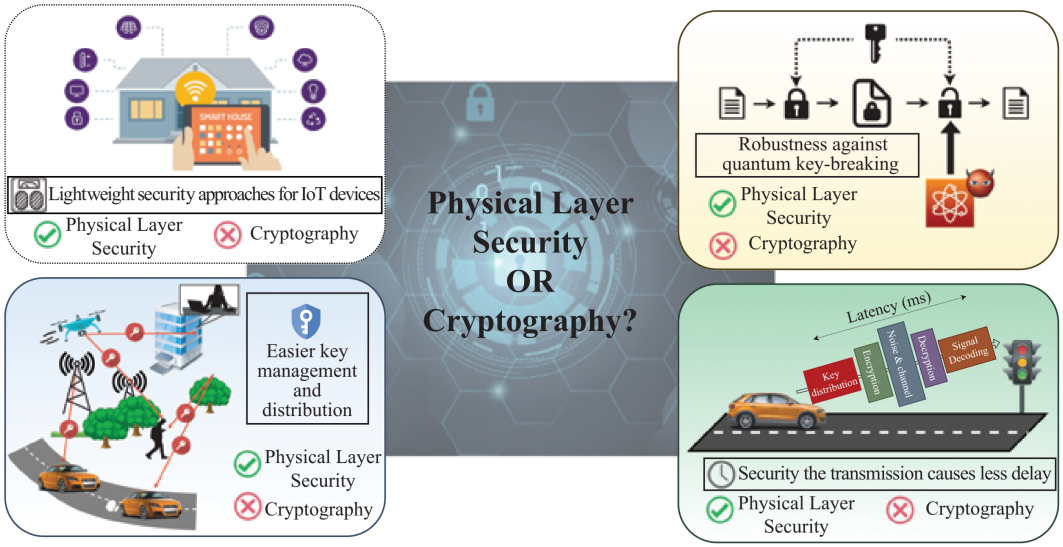


Figure 2.11 : Illustration of specific communication scenarios where PLS can supplement cryptographic approaches.

Contrasting PLS techniques with cryptographic methods for 5G networks reveals key distinctions. Firstly, PLS techniques operate independently of computational complexity, ensuring security regardless of eavesdropping device capabilities. This stands in contrast to cryptographic techniques, which often hinge on computationally intensive tasks like integer factorization, especially in public key schemes. Given the diverse computational capabilities of connected devices in 5G networks, PLS techniques offer a valuable security solution. Secondly, the decentralized structure of most 5G networks, where devices can join or leave at any time, poses challenges for cryptographic key distribution and management. PLS techniques address this issue by facilitating secure data transmission and cryptography key distribution in 5G networks [46]. Consequently, PLS can serve as an additional or supportive layer of protection within the existing security architecture.

Figure 2.11 depicts scenarios posing challenges for cryptography but amenable to PLS approaches [47]. Unlike cryptography, which necessitates a trustworthy third party for key sharing, PLS allows communicating nodes to derive keys from the shared propagation channel, eliminating the need for a trusted third party in key sharing [48]. Additionally, PLS supports asymmetrical security mechanisms, enabling the transfer of complexity to the BS/access point side, making it well-suited for IoT terminals [49].

In comparison to cryptographic methods, PLS offers reduced latency as it eliminates the need for key exchanges. Moreover, depending on the specific technique employed, encryption and decryption processes may not be obligatory [50]. Finally, PLS remains resilient against potential threats from quantum computing as it relies on the physical laws governing wireless propagation characteristics, rather than the computational complexity associated with key breaking.

2.4 Deep Learning Methods in Mobile Networks

Deep learning (DL) is essentially a subset of machine learning (ML) that empowers an algorithm to make predictions, classifications, or decisions based on data without explicit programming. Examples of traditional ML tools include linear regression, the k-nearest neighbors classifier, and Q-learning. In contrast to conventional ML methods, which heavily rely on features defined by domain experts, DL algorithms hierarchically extract knowledge from raw data through multiple layers of nonlinear processing units. This process enables them to make predictions or take actions based on specific target objectives. While neural networks are the most well-known DL models, it's essential to note that only neural networks with a sufficient number of hidden layers (typically more than one) are considered *deep* models. Other architectures with multiple layers, such as deep Gaussian processes [51], neural processes [52], and deep random forests [53], can also be regarded as structures within the realm of DL. The primary advantage of DL over traditional ML lies in automatic feature extraction, eliminating the need for costly handcrafted feature engineering. Figure 2.12 provides a high-level illustration of the relationship between DL, ML, and artificial intelligence (AI). ML approaches can be naturally classified into three categories: supervised learning, unsupervised learning, and reinforcement learning. DL architectures have demonstrated exceptional performance across all these domains [54].

The primary goal of deep neural networks (DNNs) is to approximate intricate functions by combining simple and predefined operations of units (or neurons). The objective function can take various forms, such as mapping between images and their class labels (classification), predicting future stock prices based on historical values (regression),

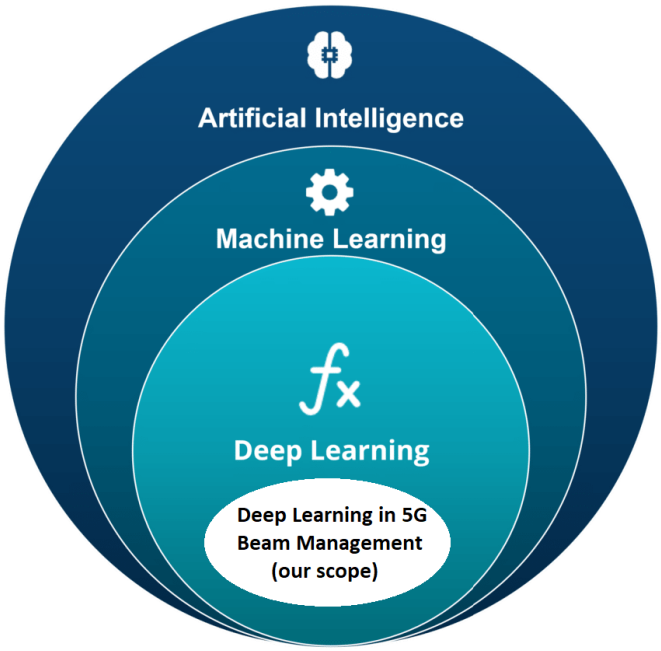


Figure 2.12 : The relation between deep learning, machine learning, and artificial intelligence.

or determining the next optimal chess move based on the current board status (control). These operations typically involve a weighted combination of specific groups of hidden units with a non-linear activation function, determined by the model's structure. These operations, combined with the output units, constitute "layers" in the neural network. The architecture of the neural network resembles the perception process in the brain, where a specific set of units is activated based on the current environment, influencing the output of the neural network model. Various DL models encompass multilayer perceptrons (MLPs), restricted Boltzmann machines (RBMs), auto-encoders (AEs), convolutional neural networks (CNNs), recurrent neural networks (RNNs), generative adversarial network (GAN), and deep reinforcement learning (DRL).

Recently, ML, particularly DL, has gained significant prominence across various research domains related to mobile and wireless networks. The potential applications of DL span diverse areas such as mobility analysis, user localization, wireless sensor networks, network control, network security, signal processing, and the analysis of mobile data at both the network and application levels as given in Figure 2.13 [54]. In here,

- "Deep Learning Driven Network-Level Mobile Data Analysis" concentrates on applications of deep learning built on mobile big data within the network. This includes tasks such as network prediction, traffic classification, and mining Call Detail Records (CDR).
- "Deep Learning Driven App-Level Mobile Data Analysis" shifts the focus to mobile data analytics on edge devices, exploring applications of deep learning in this context.
- "Deep Learning Driven User Mobility Analysis" explores the advantages of using deep neural networks to comprehend the movement patterns of mobile users, whether at the group or individual levels.
- "Deep Learning Driven User Localization" reviews literature employing deep neural networks to localize users in indoor or outdoor environments. This is based on various signals received from mobile devices or wireless channels.
- "Deep Learning Driven Wireless Sensor Networks" discusses significant work on deep learning applications in Wireless Sensor Networks (WSNs). The perspectives covered include centralized vs. decentralized sensing, WSN data analysis, WSN localization, and other applications.
- "Deep Learning Driven Network Control" investigates the utilization of deep reinforcement learning and deep imitation learning in network optimization, routing, scheduling, resource allocation, and radio control.
- "Deep Learning Driven Network Security" presents work leveraging deep learning to enhance network security. This includes infrastructure, software, and privacy-related aspects.
- "Deep Learning Driven Signal Processing" examines physical layer aspects benefiting from deep learning and reviews relevant work on signal processing.
- "Emerging Deep Learning Driven Mobile Network Application" covers other intriguing deep learning applications in mobile networking.

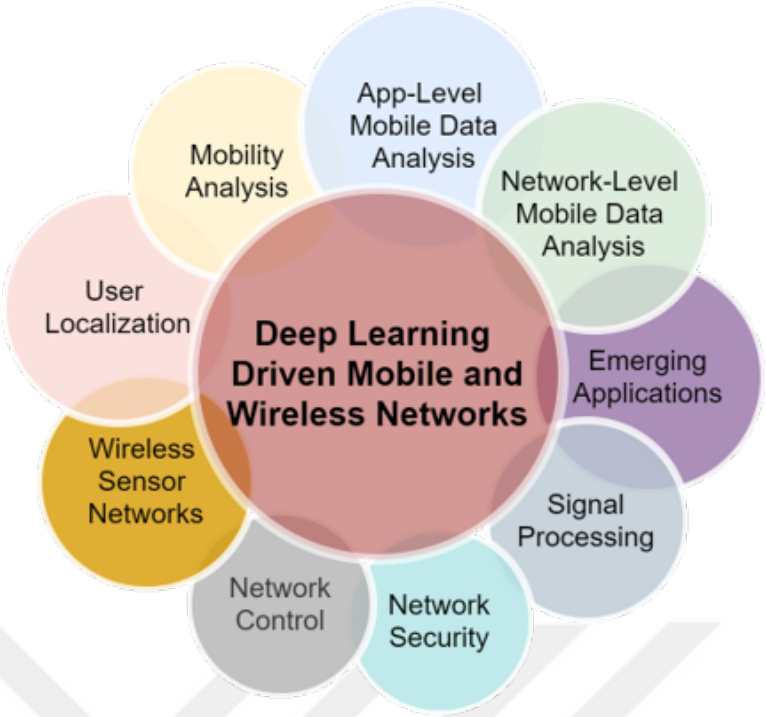


Figure 2.13 : Classification of the potential applications of DL in mobile and wireless networks.

2.5 Related Work

The realm of 5G systems has seen diverse efforts to enhance beam selection and management using learning methods. Geolocations of users are employed in [55] to choose beam indices and the serving gNodeB (gNB) in a 5G-NR mmWave system, leveraging support vector machines. [56] Uses a combination of a vehicle traffic and a ray-tracing simulators to create a dataset within a vehicle-to-infrastructure scenario. Multiple ML algorithms, including a DNN, are then employed to determine the optimal beam pair indices.

Numerous studies treat beam management as a classification problem, leading to the proposal of various DL methods. [57] employs a multi-agent Q-learning algorithm to expedite beam alignment, using different Tx-Rx beam pairs as states and predefined phase rotations as actions. [58] introduces a DL framework, DeepBeam, which uses a waveform dataset for beam management in mmWave networks. Utilizing the directions and angles-of-arrival (AoA) of Tx beams, [58] employs a convolutional neural network to differentiate unique beam patterns, enhancing beam management efficiency. Similarly, [59] presents a DNN, DeepIA, reducing beam sweep time

during initial access by selecting the best spatially oriented beam for a mmWave network based on received signal strength values. [60] proposes a recurrent neural network using RSRP and UE orientation information to predict the best beam index. Furthermore, [61] demonstrates the use of sub-6 GHz channel information to directly predict mmWave beams, a significant development due to low training overhead and increased robustness.

Comparatively, [62] proposes a DNN model predicting the best mmWave beam index using the power delay profile (PDP) of a sub-6 GHz channel, considering both mmWave and sub-6 GHz gNBs. Similarly, [63] and [64] employ sub-6 GHz channel coefficients to predict the best mmWave beams. [65] introduces a neural network architecture to jointly learn site-specific probing beams and beam prediction. [66] highlights the preference for DNNs in beam management due to their capability to autonomously identify crucial features in dynamic 5G NR environments.

Moreover, ML methods find application in beam management procedures post-initial access, particularly after procedure P-1, involving the use of channel state information reference signal (CSI-RS) [4]. [67] and [68] propose ML-based methods for predicting a narrow Tx-end beam, using RSRP, AoA, and timing advance as inputs instead of CSI-RS. Other studies such as [69], [70], and [71] leverage mobility patterns and beam recovery schemes to predict better future beams.

In terms of security, cryptography techniques predominantly operate at higher layers of the data communication stack. PLS has emerged to complement these techniques or alleviate their computational overhead. ML-based PLS schemes, categorized into channel, signal, and coding-based domains, are explored in [42]. [72] proposes a DL-based PLS scheme predicting channel coefficients between legitimate parties, comparing it with zero-forcing based beamforming for mMIMO channels. The trade-off between DL-aided PLS and reliability is analyzed in [73]. Additionally, deep learning algorithms can be utilized in CoMP to orchestrate data transmissions across multiple BSs and dynamically determine which users to serve and how many cells to involve in real-time, as discussed in [74,75]. In our prior works [76,77], we presented a comprehensive analysis, including the maximum probability of successful reception at

the intended receiver while denying reception to the most detrimental eavesdropper, considering varying antenna array sizes, the number of coordinated transmission points, and adaptive transmit power. In a previous study [78], we introduced a secure initial beam selection method based on DL. This approach prioritizes beam pairs by assessing their highest RSRP while taking security considerations into account. Subsequently, in [79], we improved upon our method to address the beam selection problem in networks utilizing mMIMO and DPS-CoMP for secure radio coverage. We introduce a DNN-based CoMP beamforming scheme designed to forecast the most secure beam pair indices between multiple coordinated TPs and the UE.

3. BEAM MANAGEMENT IN 5G AND BEYOND NETWORKS

The 5G design incorporates a crucial element: its capability to function in two distinct frequency spectrum—sub-6 GHz and mmWave. The sub-6 GHz spectrum is decreasing in availability, leading to an increasing prevalence of mmWave frequency bands with wider bandwidths. mmWave, operating above 24 GHz spectrum, is characterized by its short-range nature and high-frequency, offering enhanced capacity [4].

Distinct attributes, including path loss, signal blockage, and fading effects, vary between mmWave and the sub-6 GHz band, posing new complexities for designing systems and impacting end-to-end throughput and user experience quality. Throughput stands out as a critical factor for the success of 5G.

To overcome these challenges, 5G NR standards defined by the 3GPP introduce emerging features in the physical and medium access control layers to establish directional links [4]. Notably, beam management plays a pivotal role, facilitating the acquisition and maintenance of beams. The standards also define novel initial access procedures to ensure the efficacy of directional transmission.

This section delves into various beam management techniques and their integration into the 5G NR network, addressing the intricacies of these features.

3.1 The Motivation Behind 5G NR Beam Management

The UE in 4G long-term evolution (LTE) regularly observes the radio link to assess the channel quality from its primary eNodeB (eNB). This enables the device to assess whether the network can uphold an satisfactory link quality. In case the link quality deteriorates below a predefined threshold, the UE reports a failure in the radio link, triggering a higher-layer re-connection process. This process entails a more time-consuming cell re-selection procedure, leading to an overall reduction in data

rate. The evolution from traditional 4G-LTE networks to 5G involves the introduction of a new globally standardized radio access technology known as NR.

As 5G NR advances into the mmWave spectrum, where hybrid beamforming is commonly used in both BSs and UEs, network management becomes more intricate. However, a highly directional beamforming architecture with a greater number of antenna elements is crucial for achieving higher data rates. Special procedures are necessary for UEs to establish and maintain connections, even in scenarios involving mobility.

mmWave facilitates directional communication with an increased number of antenna elements, providing additional beamforming gain to compensate for propagation loss. Nonetheless, directional links require precise alignment of beams between the gNB and UE. This is accomplished through a series of operations referred to as beam management where UEs and gNBs regularly identify optimal beams to work on at any given time [80].

The 3GPP has established a series of procedures for beam management in [81]–[83] for 5G NR applicable in both modes of operation:

- **Idle mode:** This occurs when the UE is not actively transmitting data. The idle mode procedure is employed when the UE is attempting to connect to a network for the first time upon activation or re-initiating connection after awakening. Beam management in idle mode facilitates establishing directional initial access.
- **Connected mode:** This is when active data exchange is happening between the UE and gNB while the UE moves within the cell. In this mode, the signal can rapidly deteriorate due to mmWave characteristics. Real-time beam management becomes crucial for maintaining a robust link.

For 5G use cases like eMBB, URLLC, and mMTC, technical innovations are required, making 5G beam management indispensable.

3.2 Elements of Beam Management

Beam management encompasses a set of procedures at Layer 1 (PHY) [83] and Layer 2 (MAC) [84] aimed at establishing and maintaining an optimal beam pair to ensure effective connectivity. This beam pair comprises a transmit beam and its corresponding receive beam in a given link direction, enabling its use for both downlink and uplink transmission and reception. In cases where effective channel reciprocity exists, such as in time division duplex systems, beam management in one direction can be informed by the results of another direction. For instance, the performance of uplink beam management can be optimized using insights gained from downlink beam management.

Before a UE can engage in communication with the network, it must undergo cell search and selection procedures, attaining initial cell synchronization, and acquiring system information. The initial steps involve acquiring frame synchronization, identifying the cell, and decoding the master information block (MIB) and system information block 1 (SIB-1) [81].

In the context of a multi-antenna system that transmits multiple beams, the initial procedure includes detecting the beams from the gNB. Typically, the UE detects all beams within the search space. Figure 3.1 illustrates the timing diagram for the UE attach procedure, incorporating various facets of beam management [85].

The subsequent sections provide detailed insights into the components of beam management.

3.2.1 Beam sweeping

During the initial access process, the UE employs beam sweeping to select the most suitable beam. The gNB emits beams in all directions in a burst at defined regular intervals. When a UE is synchronizing with the network, it reads the SSB and extracts the following information:

- Primary Synchronization Signal (PSS):

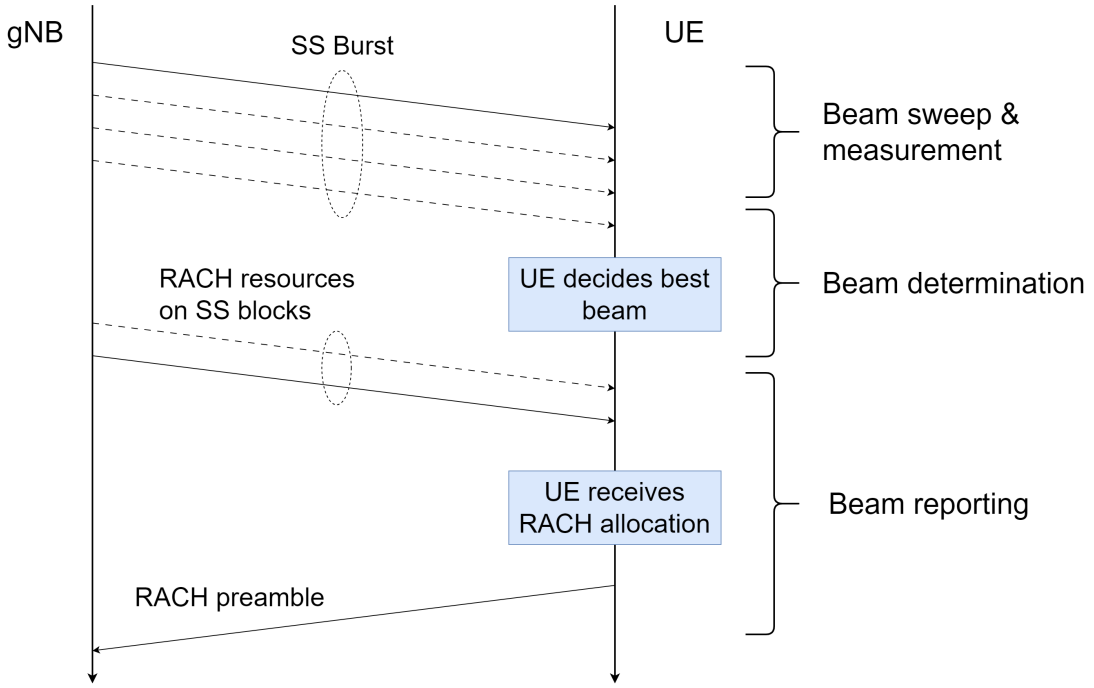


Figure 3.1 : UE attach timing diagram.

  - One out of three potential sequences.
  - Supplies a timing approximation.

- Secondary Synchronization Signal (SSS):
  - One out of 336 potential sequences.
  - Supplies the cell ID (totaling 3 * 336 = 1008).

- Physical Broadcast Channel (PBCH) and Demodulation Reference Signal (DMRS):
  - Incorporates the MIB.
  - Comprises essential information for the subsequent step, which entails decoding SIB-1.

A single SSB extends across four orthogonal frequency division multiplexing (OFDM) symbols in time and 240 subcarriers in frequency (equivalent to 20 resource blocks). Each SSB corresponds to a particular beam, beamformed in a distinct direction. A set of SSBs forms an synchronization signal (SS) burst set within a 5 ms window, and the

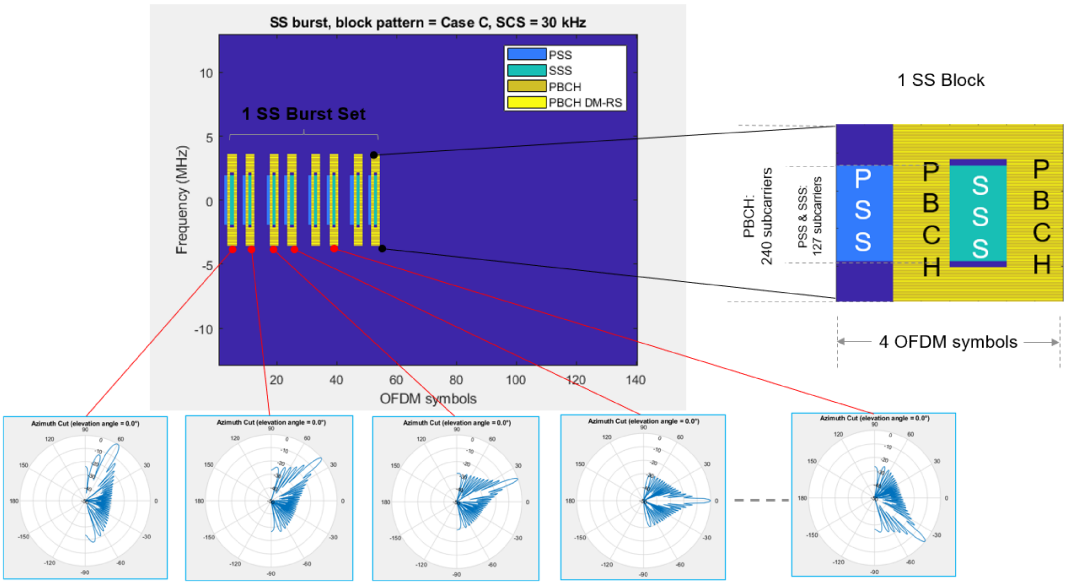


Figure 3.2 : SSBs and beam mapping.

Table 3.1 : The maximum number of SSBs for frequencies in 5G NR.

Frequency range	SSBs per SS burst set
FR-1 - up to 3 GHz	4
FR-1 - 3 to 7.125 GHz	8
FR-2 - mmWave	64

SS burst is periodically repeated every 20 ms. In Figure 3.2, a group of eight SSBs constitutes one SS burst set, aligning with frequency range (FR)-1 [82].

The maximum number of SSBs within an SS burst set is determined by the operating frequency range, as given in Table 3.1 [81].

3.2.2 Beam measurement and determination

The UE evaluates the strength of the beam by gauging the received signal power. During idle mode, this measurement relies on synchronization signals, while in connected mode, it is grounded in the CSI-RS for downlink and the sounding reference signal (SRS) for uplink. Periodically, the UE searches for the optimal beam by adhering to pre-established threshold configurations defined by the gNB, identifying the beam exhibiting the highest RSRP [86].

3.2.3 Beam reporting

The UE communicates the identified best beam to the gNB through a process known as beam reporting. A random access channel (RACH) serves as an uplink channel utilized during initial access or when the mobile device is not synchronized with the network and requires synchronization. During the idle mode, after the UE has selected its beam, there are one or more intervals for the RACH. These intervals have specific time and frequency offsets, and within them, the UE transmits the RACH preamble. The UE transmits the Physical RACH (PRACH) preamble that corresponds to the SSB for which the most suitable beam was determined. There exists a direct correspondence between the received SSB and the transmitted RACH preamble, serving as a means for the UE to report the best beam to the gNB [83,87].

The network sets up the UE to perform particular measurements and relay them at scheduled intervals, a procedure known as measurement reporting. In the connected mode, where the UE is already in communication with the gNB and active data transfer is in progress, it communicates details about the beam by means of a measurement report to the gNB.

3.2.4 Beam recovery

When a beam failure occurs due to unfavorable channel conditions, the beam recovery process is initiated to regain a new beam. The UE continuously monitors the reference signal, detecting a beam failure once the predetermined failure trigger conditions are satisfied.

Upon encountering a beam failure, the UE selects the next optimal beam for transmitting a random access (RA) preamble. If the initial RA attempt proves unsuccessful, the UE transitions to an alternative beam for another RA procedure. The RA preamble is transmitted via the PRACH. Ultimately, the UE receives a downlink resource allocation and an uplink grant through the physical downlink control channel (PDCCH) [81].

To expedite the beam recovery process and ensure the reliability of message delivery, a non-contention-based channel utilizing the PRACH can be employed in 3GPP Release 15. This approach, as opposed to contention-based methods, is utilized for transmitting beam failure recovery requests for the primary cell. In 3GPP Release 16, support for an uplink control channel is additionally introduced to carry beam failure recovery requests for secondary cells in scenarios involving carrier aggregation [88]. Following the completion of the beam failure recovery process, both the gNB and the UE can utilize the newly identified beam(s) for subsequent communication.

3.2.5 Beam switching

Shifting from one beam to another can be referred to as intra-cell mobility or beam-level mobility. Beam switching relies on a trigger condition specific to a beam and the established beam switching algorithm. This operation is applicable when the UE is in connected mode and can be executed through L1/L2 procedures [83,84]. In contrast, handover pertains to inter-cell mobility and constitutes an L3 procedure [89].

3.3 Beam Management Procedures

3GPP TR 38.802 [4] outlines beam management, specifying it into three distinct procedures. This section provides a detailed description of these procedures.

3.3.1 Procedure 1: SSB-based beam sweeping

This procedure concentrates on the initial acquisition based on the SSB for a UE in idle mode. During the initial acquisition, beam sweeping occurs at both the transmit and receive ends to select the optimal beam pair, relying on RSRP measurements. Generally, the chosen beams have a wide scope and may not represent the most efficient beam pair for data transmission and reception [90]. Once connected, the beams undergo further refinement using CSI-RS for downlink and SRS for uplink, a process elaborated in the subsequent procedure.

To initiate Procedure 1, the generation of a synchronization signal burst is necessary. The subsequent step involves beamforming each of the SSBs within the burst, sweeping across both azimuth and elevation directions, and transmitting this

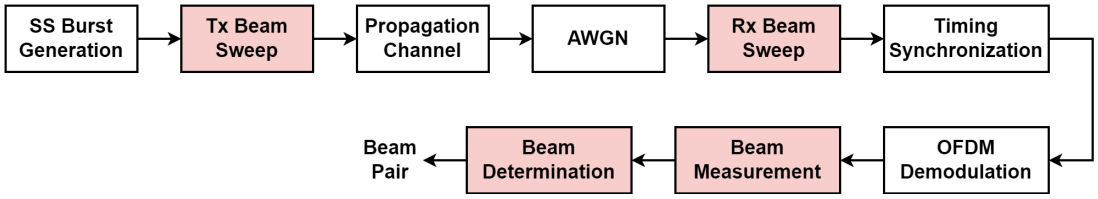


Figure 3.3 : Procedure 1 end-to-end processing steps.

beamformed signal through a spatial scattering channel. On the receiving end, the signal is processed across multiple receive beams.

The RSRP for each transmit-receive beam pair is measured to identify the beam pair link with the highest RSRP. This link denotes the optimum beam pair at both the transmit and receive ends for the simulated spatial scenario. Figure 3.3 illustrates the processing steps, with the beam management-related blocks highlighted in red.

Figure 3.4 provides an illustration of an SS burst [85]. In this depiction, a scattering MIMO channel model is employed, utilizing uniform rectangular arrays (URA) equipped with isotropic antenna elements.

For the implementation of transmit-end beam sweeping, each SSB within the created burst undergoes analog beamforming. The determination of azimuth and elevation directions for various beams relies on the quantity of SSBs in the burst and the defined sweep ranges. Subsequently, each block within the burst is beamformed towards these specified directions. The resulting beamformed burst waveform is then transmitted through the spatially aware scattering channel.

For the process of receive-end beam sweeping, the transmitted burst waveform, which has undergone beamforming, is received sequentially across each individual receive beam. In the Procedure 1, involving N transmit beams and M receive beams, each of the N beams is transmitted M times from the gNB. This ensures that each transmit beam is received by all M receive beams.

An illustrative diagram representing the beam sweeps at both the gNB and UE is provided in Figure 3.5 for the case where $N = M = 4$ in the azimuthal plane. This diagram visually depicts the timeline for the dual sweep, where each interval at the gNB corresponds to a SSB, and each interval at the UE corresponds to the SS burst.

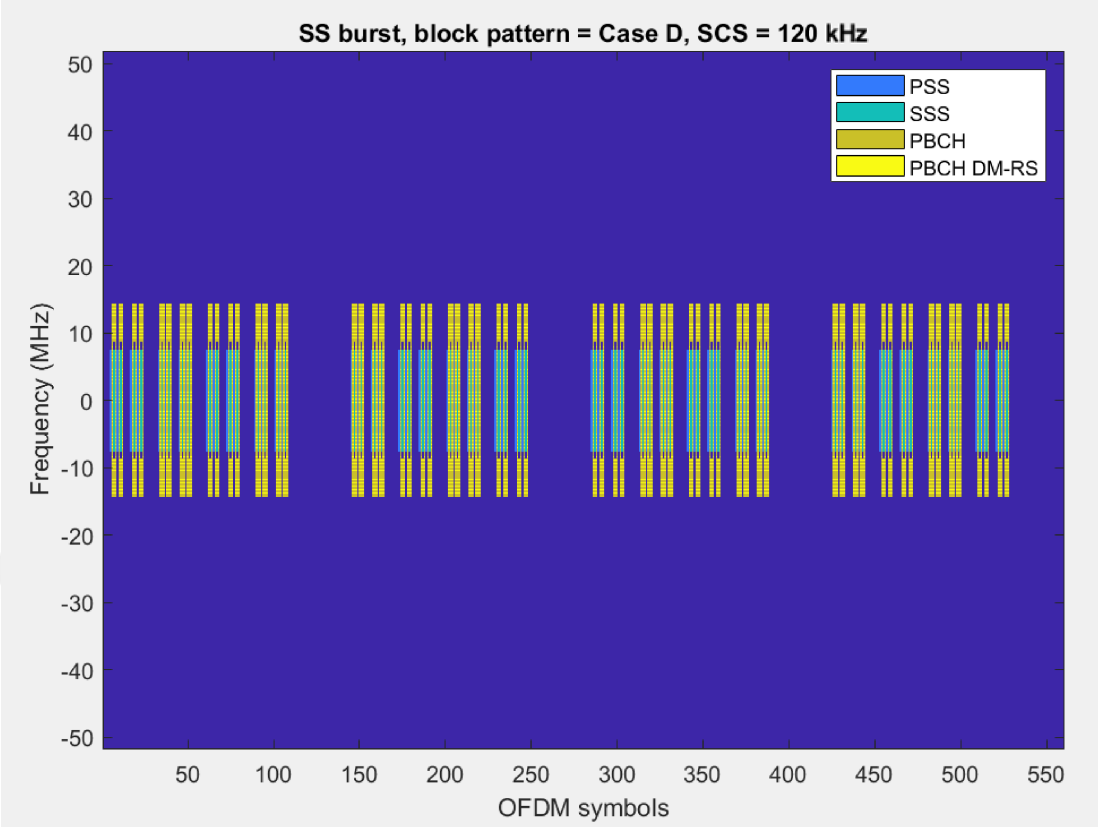


Figure 3.4 : SS burst generation.

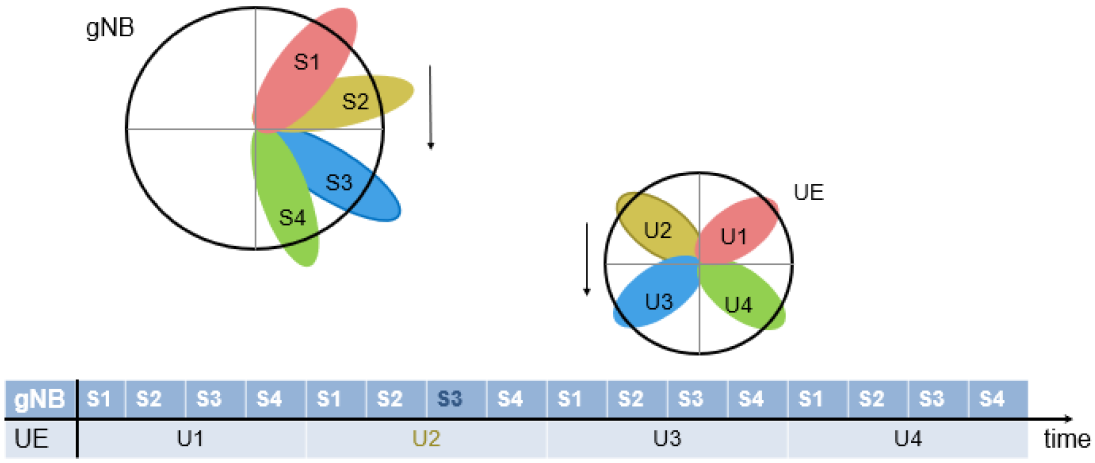


Figure 3.5 : SSB beam sweeping in downlink.

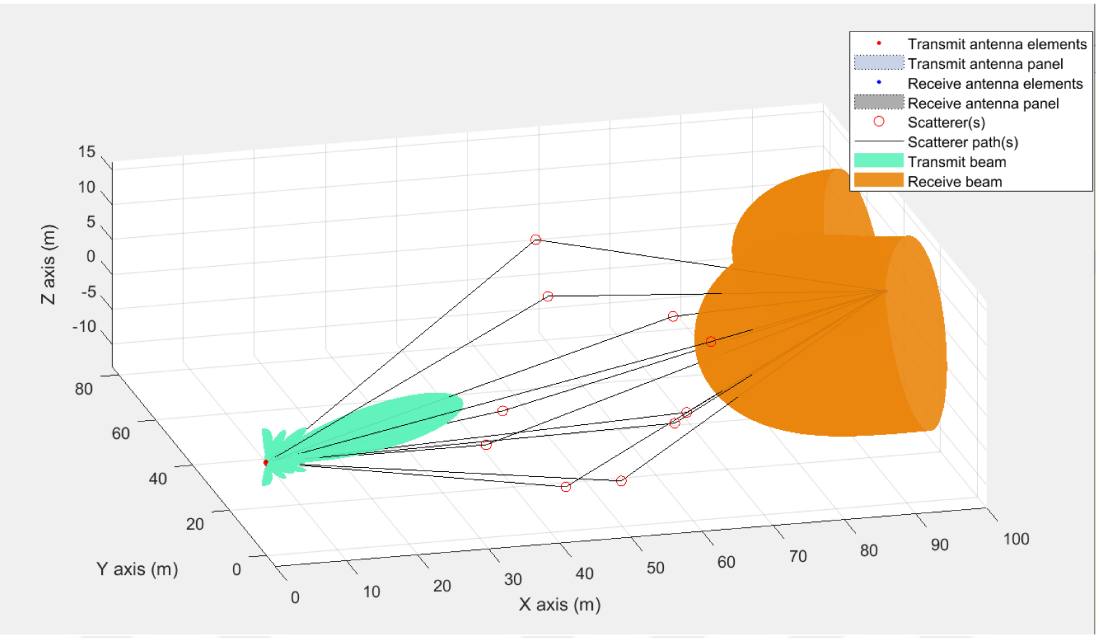


Figure 3.6 : Procedure 1 spatial scene simulation.

In this specific scenario, beams S3 and U2 are highlighted as the notionally selected beam-pair link.

The processing of the transmitted burst at the receiver includes:

- Addition of the scattering channel and additive white Gaussian noise (AWGN)
- Implementation of receive-end beamforming
- Timing correction
- OFDM demodulation
- Extraction of the known SSB grid
- Measurement of the RSRP based on the specified measurement mode (using the SSS or the PBCH-DMRS)

These steps are iteratively performed for each of the receive beams, and the best beam-pair is selected based on the complete set of measurements conducted [91]. Figure 3.6 illustrates a simulation of a 3D spatial scene, showcasing the selected beam identified as part of Procedure 1. The scene incorporates multiple scatterers, and

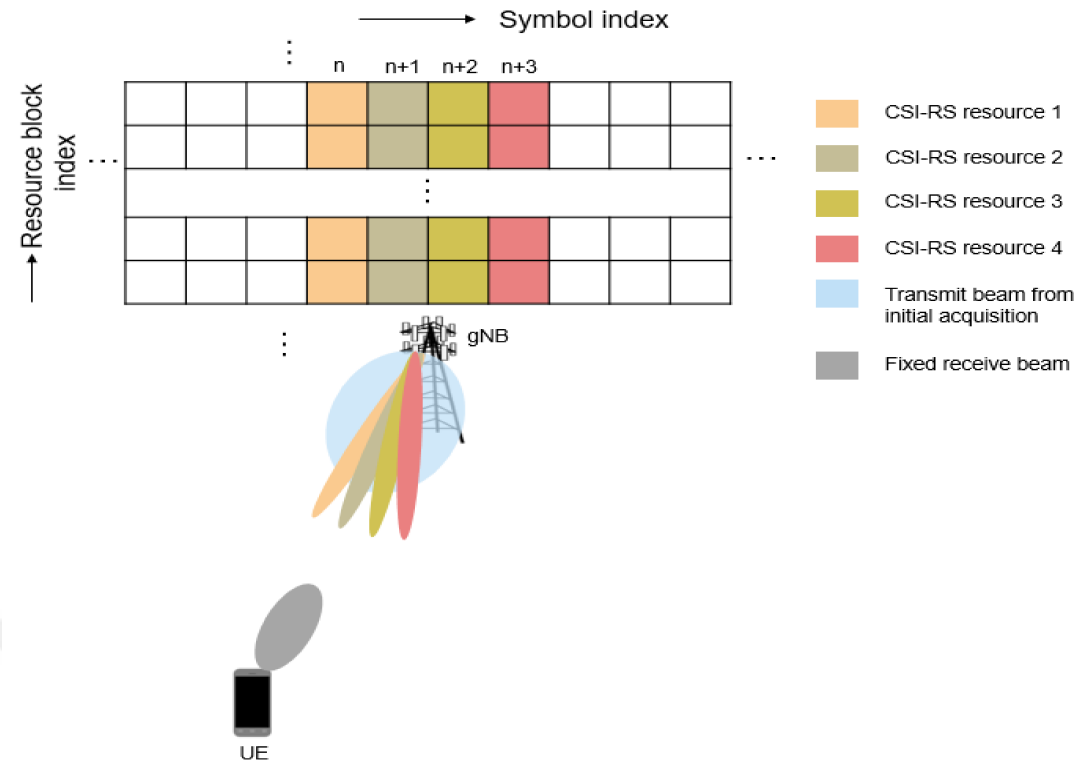


Figure 3.7 : CSI-RS based transmit-end beam refinement.

channel conditions are considered. This depiction provides a more realistic view of the initial acquisition following the completion of Procedure 1.

3.3.2 Procedure 2: CSI-RS based Tx-end beam refinement

Upon establishing the initial beam, achieving a high directivity and gain for unicast data transmission requires a more refined beam compared to the SSB beam. To address this, a set of reference signal resources is configured and transmitted in various directions, utilizing finer beams within the angular range established during the initial acquisition process. Following this, the UE measures all these beams by capturing signals with a fixed receive beam. The optimal transmit beam is ultimately chosen based on the RSRP measurements across all transmit beams.

This procedure focuses on transmit-end beam refinement, involving beam sweeping at the transmit end while maintaining a fixed receive beam. The process relies on non-zero-power (NZP) CSI-RS for downlink transmit-end beam refinement and SRS for uplink transmit-end beam refinement. Procedure 2 is implemented once the initial

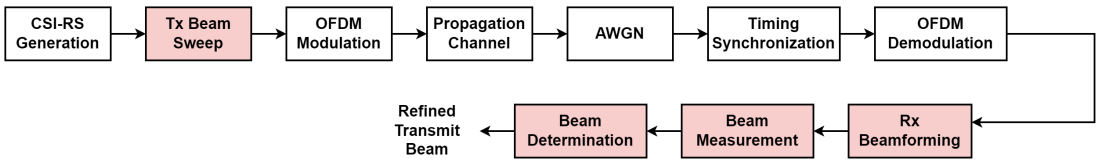


Figure 3.8 : Procedure 2 end-to-end processing steps.

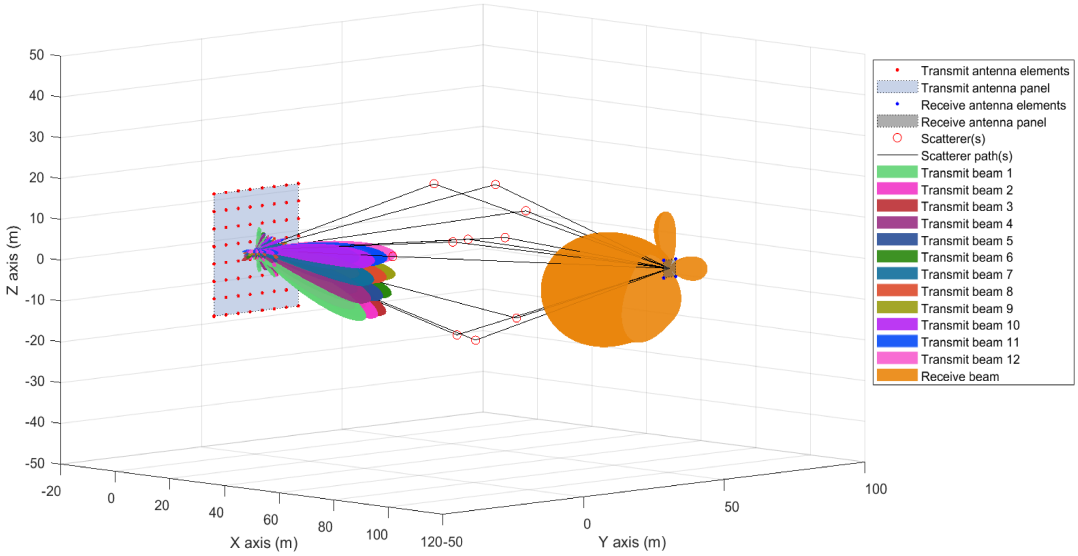


Figure 3.9 : Procedure 2 spatial scene simulation.

connection and beam pair link have been established. It functions as a beam refinement procedure aimed at further enhancing the connection, as illustrated in Figure 3.7.

Employing digital beamforming allows for the using of narrower beams, effectively minimizing interference from multiple users. Initially, the CSI-RS signal undergoes beamforming before being subjected to OFDM modulation. The modulated signal is then transmitted across the scattering channel, introducing AWGN. On the receiving end, timing synchronization and OFDM demodulation occur before implementing receive beamforming. Following this, beam measurement and beam determination take place to derive the refined transmit beam. The components facilitating beam management are emphasized in red in Figure 3.8.

Figure 3.9 illustrates an example of a 3D scattering MIMO scenario. This depiction encompasses Tx and Rx antenna array beam patterns, multiple scatterer positions, and their corresponding paths.

3.3.3 Procedure 3: CSI-RS based Rx-end beam refinement

Procedure 3 focuses on the adjustment of the Rx-end beam, involving beam sweeping at the Rx end based on the current transmit beam. The goal is to pinpoint the optimal receiving beam, which may be either a neighboring beam or a refined beam.

In this process, a set of reference signal resources (NZP CSI-RS for downlink and SRS for uplink) is transmitted using the same transmit beam. The UE or gNB receives the signal using different beams from various directions, covering an angular range. Ultimately, the best Rx beam is selected based on the RSRP measurements across all receiving beams.

4. DEEP LEARNING-BASED SECURE BEAM MANAGEMENT

Beam management is an integral component of 5G NR, playing a vital role in designing an effective initial access and tracking procedure. Its primary function is to consistently identify the optimal beam pair between the UE and the gNB, contributing significantly to the overall efficiency of the system.

The establishment of a beam pair link involves the utilization of SSB transmitted within a transmit burst, along with the execution of transmit/receive point (TRP) beam sweeping and UE beam sweeping. The objective is to create an efficient beam pair link that maximizes spectral efficiency between the transmitter and the receiver, emphasizing the identification of the optimal beam pair based on RSRP. To achieve this, an exhaustive search is conducted across all potential transmit and receive beam pairs. The growing number of antenna elements, and consequently, beams in mMIMO, amplifies the complexity and resource demands of the initial access process, contributing to heightened latency and energy consumption [92]. Given the imperative need for the swift and energy-efficient deployment of 5G networks, a streamlined and secure approach to initial access is crucial. Thus, the development of an efficient procedure for discovering an appropriate TP and searching for a suitable beam pair among all the beams connecting the Tx and the Rx becomes essential [2].

In most research studies centered on ML-assisted beam management, DNNs have emerged as the favored option. In the dynamic context of 5G NR, where optimal beam configurations rely on various factors such as user location and channel conditions, DNNs demonstrate the capability to autonomously recognize and utilize critical features [59,63]. This proficiency substantially diminishes the need for explicit manual feature engineering. Additionally, the connections between input parameters and optimal beam configurations frequently display nonlinear characteristics. As a result, DNNs excel in capturing and comprehending these intricate relationships, serving as a robust tool for tackling the inherent challenges in beam management process

[66]. Additionally, DL algorithms find application in CoMP scenarios, effectively scheduling data transmissions across multiple BSs and dynamically selecting users to serve based on real-time considerations, as explored in [74] and [75]. Moreover, the integration of ML in the realm of physical layer security contributes to network security enhancement, adeptly identifying and mitigating potential threats, as exemplified by research in [72] and [93].

The key motivation behind incorporating DL into beam management is to enhance the beam search/sweeping process by reducing latency and energy consumption while prioritizing communication security. A beam selection method based on DL is introduced, which involves ranking the beam pairs between a transmitter and a legitimate user with the objective of maximizing the signal strength received by the user. Simultaneously, the method ensures that the signal strength observed by the eavesdropper remains below a specified threshold. Rather than conducting an exhaustive search, the beam selection is carried out on a limited set comprising the top beam pairs. This approach results in reduced communication overhead and, consequently, decreased energy consumption.

In this chapter, we propose two transmission models. The first model is a DNN-based secure initial access and beam selection procedure when there is one serving cell. Here, the SSB beam sweeping procedure is automated using a DNN, serving as a proof of concept to demonstrate the compliance of the proposed DNN with existing standards. Additionally, instead of opting for the beam pair solely based on the highest RSRP, our approach entails selecting a beam pair that not only maximizes the RSRP for the UE but also strives to keep the RSRP observed by potential eavesdroppers below a specified threshold. This security measure is achieved through the inherent properties of mMIMO and beamforming, eliminating the need for additional security mechanisms such as injecting an artificial noise, generating secure keys, directional modulation, and others. [6].

The second model focuses on the beam selection problem in networks employing mMIMO and DPS-CoMP for secure radio coverage. In this model, we also propose a DNN-based CoMP beamforming scheme to predict the most secure beam pair indices

between the multiple coordinated TPs and the UE, aligning with the same motivation as in the single-cell scenario.

4.1 Secure Initial Access and Beam Selection using Deep Learning

In this section, the proposed beam selection procedure for secure initial access is described. It is assumed that an eavesdropper is present in the system, and the location of the eavesdropper is unknown to the UE. A threshold value, β, representing the minimum required RSRP level at the receiver side (whether legitimate or eavesdropper) for successful signal decoding, is defined. The intended outcome of the proposed procedure is to maximize the RSRP for the legitimate user while attempting to maintain the RSRP at the eavesdropper below β, if possible. If this objective is accomplished, it is stated that secure and successful communication has taken place.

To circumvent the need for repeatedly conducting an exhaustive search and to reduce communication overhead, a DNN scheme is proposed. The beam selection problem is formulated as a classification task, where the best Tx-Rx beam pair index is the target output, and receiver coordinates serve as input to the DNN algorithm. With out-of-band information, a trained DNN model suggests a set of K favorable beam pairs. Instead of performing an exhaustive search across all beam pairs, the beam sweeping overhead is minimized by searching only within the selected K beam pairs. It should be noted that, as the number of beams increases, the time overhead during beam sweeping also escalates. The current 5G standards for mmWave bands employ 64 beams at both the Tx and Rx ends.

Two distinct scenarios are employed to describe (and subsequently evaluate) the proposed DL-driven procedure. The data for the first scenario, termed *the terrain model*, is derived from a network planning software that calculates RSRP values using parameters from several presently deployed cells and real 3D terrain information. For a more comprehensive understanding of the proposed method's performance, a second scenario, labeled *the statistical model*, utilizes artificially generated data employing a statistical channel model incorporates 5G NR system variables as defined by the 3GPP.

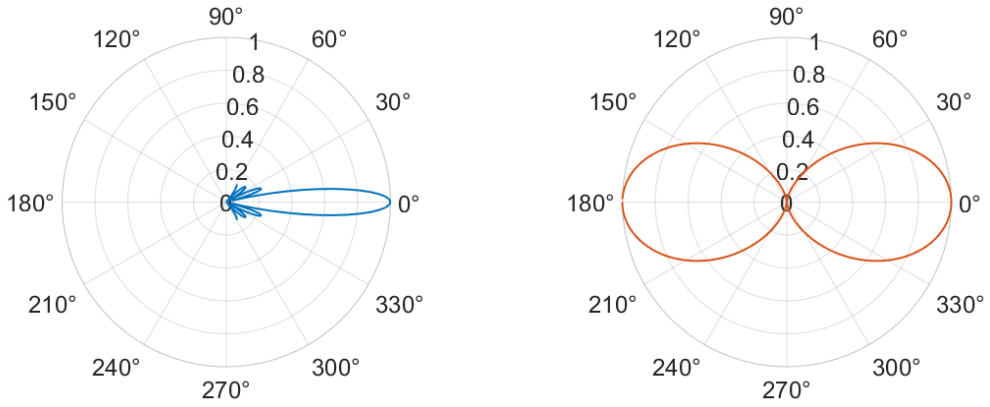
In the terrain model, the realistic radio coverage from a BS in the İstanbul/Büyükçekmece district of Türkiye, operating at 3.5 GHz, is taken into account. The coverage levels are determined using a 3D-map-based simulation tool and are validated through operational data and drive tests conducted by a mobile service provider. A typical urban environment in İstanbul, characterized by high user density and substantial traffic loads, is represented at this site.

Apart from the terrain model derived from radio coverage calculations through a map-based simulation tool at an actual BS site, a more general "statistical model" is also utilized, employing statistically generated multi-path channels to generalize the results. Given that the terrain model in the first scenario is tailored to a distinct environment, the scope of findings is aimed to be broadened by incorporating a second scenario. In this simulated environment, essential parameters from a 5G NR system are introduced. This method enables the examination of result generalizability beyond the constraints of a particular environment, offering insights into the broader implications and applicability of the study.

4.1.1 Channel model and antenna configuration

In this part, channel and antenna configurations are explored, with the introduction of Tx-Rx antenna patterns, steering vectors, and eavesdropper distribution. Following that, we elaborate on the baseline beam selection process during the initial access phase, providing insights into aspects such as beam sweeping, measurement, reporting, and the selection criteria based on the standard.

A multi-path propagation channel is utilized, wherein signals emitted from a transmitting array undergo reflection from multiple scatterers before reaching a receiving array. The gNB deploys a half-wavelength spaced uniform rectangular array (URA) with $N = N_v \times N_h$ antenna elements, where N_v and N_h represent the number of antenna elements in the vertical and horizontal dimensions, respectively. The steering matrix $A(\theta, \phi) \in \mathbb{C}^{N_v \times N_h}$ is defined as the Kronecker product of the steering vectors of a URA in each dimension, and it is expressed as



(a) Tx array with 8×8 antenna elements

(b) Rx array with 2×2 antenna elements

Figure 4.1 : mMIMO beam patterns of Tx-Rx antennas.

$$A(\theta,\phi) = a_v(\theta,\phi) \otimes a_h(\theta,\phi), \tag{4.1}$$

where (θ,ϕ) denotes the elevation and azimuth angles of the signal, and the steering vectors of the vertical and horizontal dimensions are respectively given as

$$a_v(\theta,\phi) = [1,\cdots,e^{j(N_v-1)\pi\sin(\theta)\cos(\phi)}]^T, \tag{4.2}$$

$$a_h(\theta,\phi) = [1,\cdots,e^{j(N_h-1)\pi\sin(\theta)\cos(\phi)}]^T. \tag{4.3}$$

It is assumed that the channel is constant over a symbol period and narrowband. The channel for receiver u is provided by

$$\begin{aligned} H^{(u)} &= \sum_{l=1}^{L_p} \alpha_l A(\theta_l^T,\phi_l^T) \otimes A^*(\theta_l^R,\phi_l^R) \\ &\in \mathbb{C}^{N\times M}, \end{aligned} \tag{4.4}$$

where (θ_l^T,ϕ_l^T) and (θ_l^R,ϕ_l^R) are the angular pairs between the Tx and the Rx at path l, $l \in \{1,\ldots,L_p\}$, with complex gain α_l and $M = M_v \times M_h$ is the number of antenna elements of the URA at receiver u. The assumption is that the antenna array of the UE is correctly aligned with the gNB, allowing a receiver to attain the complete antenna array gain regardless of any orientation changes. Figure 4.1 displays the 2D array patterns for both Tx and Rx. Additionally, Figure 4.2 illustrates an example of

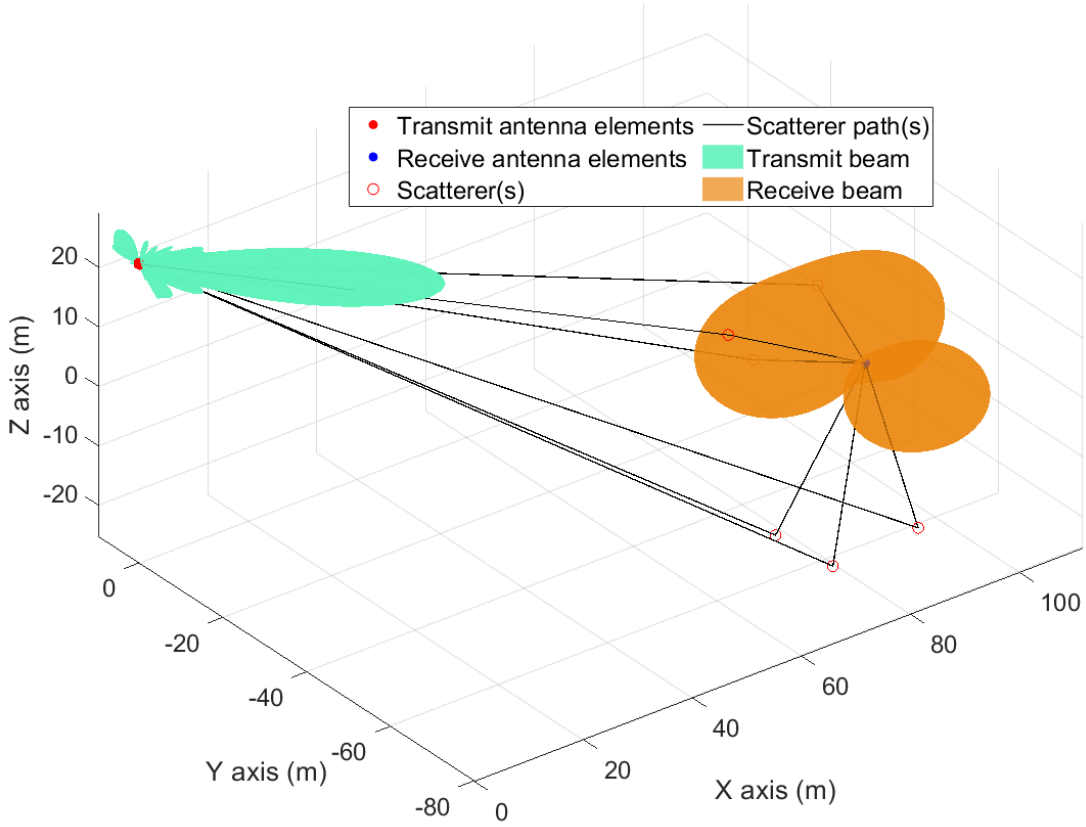


Figure 4.2 : Illustration of a mMIMO spatial perspective with Tx-Rx beams and scatterers.

a mMIMO spatial scenario, presenting a consolidated perspective of the Tx and Rx arrays, along with their beams and associated scatterers.

In the existence of eavesdroppers, legitimate users engage in communication through the gNB. For a specific legitimate user, an eavesdropper is randomly positioned at a distance following a normal distribution with a mean of 300 m and a standard deviation of $\sqrt{5000}$ m. The angle between the horizontal axis and the line connecting the user and its eavesdropper is uniformly distributed in the range $[0, 2\pi)$, as depicted in Figure 4.3. It is evident that an eavesdropper may be situated within the area between the gNB and UE or outside of it. The same capabilities and antenna configurations, including array size, sweep limits, and so forth, are assumed to be possessed by eavesdroppers as by the legitimate users.

In the first phase of beam management, a gNB initiates the transmission of beams sweeping across all directions in a burst at regular intervals, defined within azimuthal

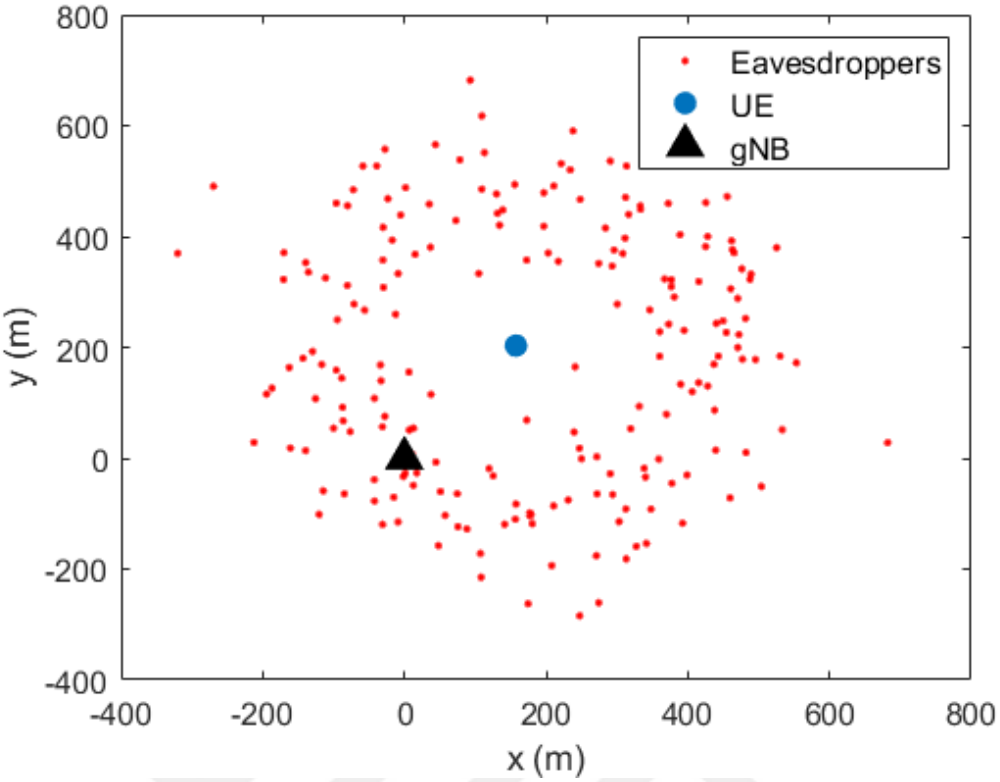


Figure 4.3 : The potential eavesdropper positions in a single-cell scenario.

and elevation limits. When a UE is in the process of synchronizing with the network, it reads the SSB and extracts essential signals such as the PSS, SSS, PBCH, and DMRS [81]. Each SSB covers a span of four OFDM symbols in time and 240 subcarriers in frequency (equivalent to 20 resource blocks). These SSBs are associated with specific beams, each beamformed in a different direction. A set of SSBs forms a synchronization signal (SS) burst set, covering a 5 ms window. The SS burst is broadcasted in various directions every 20 ms [86]. Specifically, a group of eight SSBs constitutes one SS burst set, aligning with the FR-1 from 3 to 7.125 GHz [4]. During the initial acquisition phase, the UE employs beam sweeping to meticulously select the most optimal beam.

Following the initial alignment of beams, the same beam pair link can be employed for subsequent transmissions, with the option to further refine beams using CSI-RS for downlink and sounding reference signal (SRS) for uplink if needed. In the event of beam failure, these paired links can be re-established.

Algorithm 1 Baseline beam selection algorithm

Input: Receiver u
Output: Selected beam pair index $b^{(u)}$

$P_{\max} = -\infty$
$b^{(u)} = 1$
for $i = 1$ to K_T **do**
    for $j = 1$ to K_R **do**
        Measure $P_{i,j}^{(u)}$
        if $P_{i,j}^{(u)} > P_{\max}$ **then**
            $P_{\max} = P_{i,j}^{(u)}$
            $b^{(u)} = (i-1)K_R + j$
        end if
    end for
end for

For beam management procedures, SS-RSRP Layer 1 measurements prove valuable. The correlation between reported and measured values for Layer 1 and Layer 3 RSRP is defined by 3GPP [94]. Following Layer 1 filtering at the receiver, RSRP measurement is conducted and reported for each beamformed signal $f_{i,j}$, where i and j denote the Tx and Rx beam indices, respectively. For simplicity, the aggregation of Tx-Rx powers, gain factors, and large-scale signal-to-noise ratio (SNR) values is represented by a single value γ_u. The measured RSRP, with additive noise power n, is determined as follows

$$P_{i,j}^{(u)} = \frac{\gamma_u}{N \times M} \left\| \tilde{H}^{(u)} f_{i,j} \right\|_2^2 + n, \tag{4.5}$$

where $\|\cdot\|_2$ stands for the l_2 norm. As the value in Eq. (4.5) corresponds to a particular beamformed signal, it is essential to identify the highest RSRP value by conducting a search across the entire spatial region. The best beam pair indices are then determined as follows

$$b^{(u)} = \underset{\substack{1 \le i \le K_T \\ 1 \le j \le K_R}}{\arg\max} P_{i,j}^{(u)}, \tag{4.6}$$

where K_T and K_R are the number of beams at Tx and Rx ends, respectively. Since the center frequency in this study is 3.5 GHz (n78), the SSB transmission pattern is

standardized as Case B [81] in which eight beams are considered in both Tx and Rx ends ($i, j \in \{1, \ldots, 8\}$). Thus, the best pair is searched over a total of 64 beam pairs, which are enumerated as $(i, j) \mapsto b = 8(i-1) + j,\ b \in \{1, \ldots, 64\}$. The baseline beam selection algorithm to identify the highest RSRP among all available beam pairs (for general K_T and K_R) is given in Algorithm 1.

It is important to highlight that the baseline beam selection algorithm, referred to as Algorithm 1, does not take into account either the minimum required RSRP level for reception or security considerations in the presence of potential eavesdroppers.

Algorithm 2 Secure beam selection algorithm

Input: Receiver u, RSRP matrices $P^{(u)}$, $P^{(e)}$
Output: Selected beam pair index $b^{(u)}$, Flags *CommPossible*, *SecureCommPossible*

CommPossible = False
SecureCommPossible = False
$P_{\text{max,all}} = -\infty$
$P_{\text{max,sec}} = -\infty$
for $i = 1$ to K_T **do**
    for $j = 1$ to K_R **do**
        if $P_{i,j}^{(u)} > P_{\text{max,all}}$ **then**
            $P_{\text{max,all}} = P_{i,j}^{(u)}$
            $b_{\text{max,all}} = (i-1)K_R + j$
        end if
        if $P_{i,j}^{(u)} \geq \beta$ **then**
            CommPossible = True
            if $P_{i,j}^{(e)} < \beta$ **then**
                SecureCommPossible = True
                if $P_{\text{max,sec}} < P_{i,j}^{(u)}$ **then**
                    SecureCommPossible = True
                    $P_{\text{max,sec}} = P_{i,j}^{(u)}$
                    $b_{\text{max,sec}} = (i-1)K_R + j$
                end if
            end if
        end if
    end for
end for
if *SecureCommPossible* **then**
    $b^{(u)} = b_{\text{max,sec}}$
else
    $b^{(u)} = b_{\text{max,all}}$
end if

4.1.2 Secure beam selection algorithm

The most secure beam pair for each hypothetical user is identified through a thorough search of all beam pairs using Algorithm 2. In this process, the chosen beam pair is the one that yields the highest RSRP above the threshold β for the UE, among those pairs resulting in RSRP levels below β for the eavesdropper. If no such pair is available, the pair that maximizes RSRP for the UE is selected, even if it cannot ensure secure communications.

4.1.3 DNN model for single-cell transmission

The best beam pair is identified through RSRP measurements, serving the specific objectives of beam selection as elucidated in Algorithms 1 and 2. Algorithm 1 prioritizes the highest RSRP, while Algorithm 2 focuses on security considerations. Hence, to find the best beam, the dual-sweep process must be executed over a time duration of $K_T \times K_R$ time slots for each receive beam. The optimal beam pair is then selected based on the comprehensive set of measurements conducted during this period. In order to reduce this signalling overhead the prediction of the best beam is made by utilizing a DNN where user location is input and the best beam pair index is output. In this part, the data generation, training and testing phases of DNN are explained for a single-cell transmission.

The best beam pair is determined by assessing the RSRP measurement, serving specific purposes as outlined in Algorithms 1 and 2 for achieving the highest RSRP and security, respectively. To identify the best beam, a dual-sweep must be conducted over a time duration of $K_T \times K_R$ time slots for each Rx beam. The selection of the best beam pair is based on a comprehensive set of measurements. To minimize this signaling overhead, the prediction of the best beam is accomplished through the utilization of a DNN. The input to the DNN is the user's location, and the output is the index of the best beam pair. This section elaborates on the data generation, training, and testing phases of the DNN for single-cell transmission.

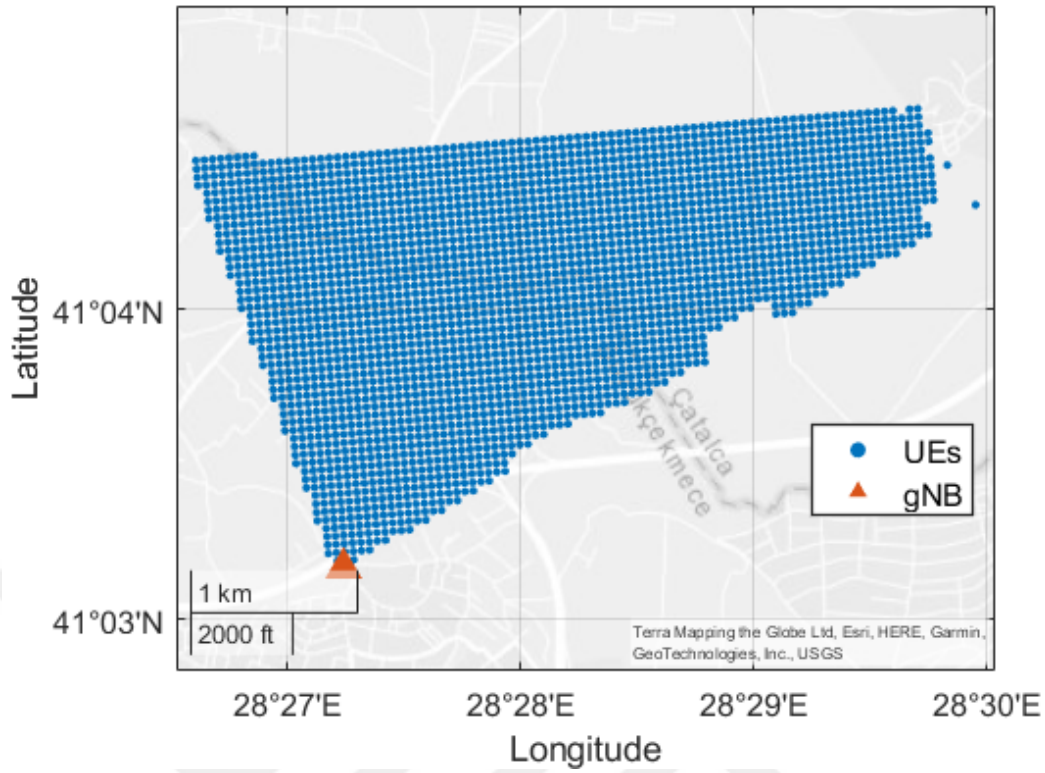


Figure 4.4 : User locations in a real cellular network served by a single cell.

4.1.3.1 Data generation

The dataset construction of the terrain model begins with the selection of a real cellular cluster. Firstly, RSRP values are computed at 9700 geographic points uniformly distributed, as illustrated in Figure 4.4. This computation is performed using a map-based radio network planning software, utilizing the parameters of the deployed cells and real 3D terrain information of the region. Then, the calculated channel gains are supplemented with mMIMO antenna gains for all Tx-Rx beam pairs in a post-processing step. It is assumed that eight beams are available on both the Tx and Rx ends. Finally, the best beam pair for each hypothetical user is determined through an exhaustive search across all possible beam pairs, following Algorithm 2. The generation of the eavesdropper follows the previously explained random process (refer to Figure 4.3). During the training phase, it is presumed that the locations of eavesdroppers are known, facilitating the identification of the true optimal beam pair.

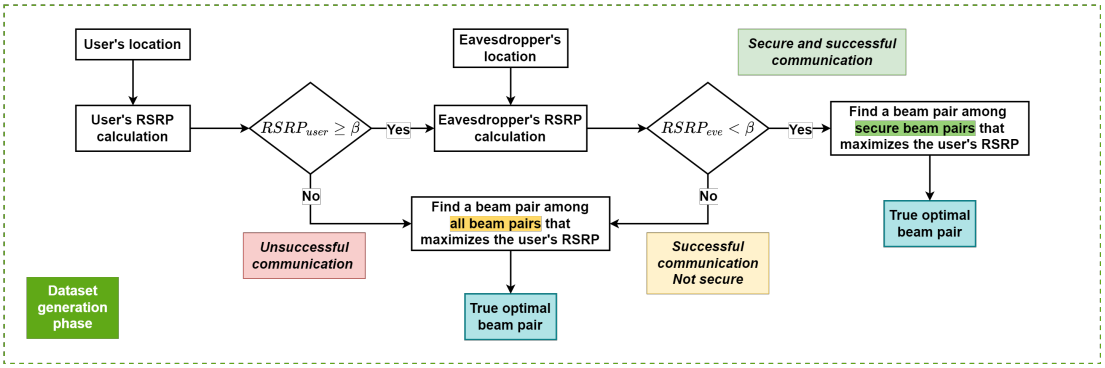


Figure 4.5 : The data generation step of the DNN model through an exhaustive search.

In the statistical channel model dataset, the same gNB and UE locations as in the terrain model are used. The dataset is generated using the 5G toolbox in Matlab [95] for the statistical model. A spatial scattering MIMO channel is configured, incorporating multiple scatterers, and both the gNB and UEs are equipped with URAs featuring 8-by-8 and 2-by-2 antenna elements, respectively.

To implement TRP beam sweeping, each SSB is beamformed in the generated burst using analog beamforming. The azimuth and elevation directions for the different beams are determined based on the number of SSBs in the burst and the specified sweep ranges. Subsequently, the individual blocks within the burst are beamformed to each of these directions. The resulting beamformed burst waveform is then transmitted over the configured spatially-aware scattering channel.

For receive-end beam sweeping, the transmitted beamformed burst waveform is successively received over each receive beam. In procedure P-1, with K_T transmit beams and K_R receive beams, each of the K_T beams is transmitted K_R times from the gNB, ensuring that each transmit beam is received over the M receive beams. In this study, both K_T and K_R are set equal to the number of SSBs in the burst, and only one burst is generated for simplicity.

After completing the dual-sweep over a time duration of $K_T \times K_R$ time slots for each receive beam, the best beam pair is selected based on the comprehensive set of measurements. The detailed process of data generation is illustrated step by step in Figure 4.5.

4.1.3.2 DNN architecture

Upon completion of dataset generation for both terrain and statistical models, the training phase of the DNN is initiated, utilizing a multilayer perceptron (MLP) as the neural network model. MLPs are effective for solving classification prediction challenges, leveraging their ability to capture complex patterns within layers of hidden neurons. [96]. In these tasks, inputs and outputs are associated with specific classes or labels. In this work, an MLP model is employed, where receiver locations serve as input to the neural network. The output comprises a ranking of the beam pairs between the Tx and Rx based on the selected coverage criteria.

Two distinct types of hyperparameters are found in DL models: model hyperparameters, which define the model's architecture, including the number of hidden layers and neurons per layer, shaping its complexity; and optimizer hyperparameters, which impact the training process (e.g., learning rate, batch size, and the number of epochs) [97]. Various parameter configurations were explored by systematically examining combinations within the model hyperparameters. The performance results of these experiments, presented in Table 4.1, encompass metrics such as loss, accuracy, recall, and precision. These metrics are instrumental in identifying the most suitable hyperparameters for our DNN model. It is important to note that these results pertain to the terrain model, where the prediction of a beam pair by the DNN involves selecting the one with the highest probability under security constraints. The numerical outcomes of the selected hyperparameters, highlighted in bold, are compared with benchmarks in Chapter 5.

After hyperparameter tuning, the proposed neural network comprises four hidden layers, each containing 96 neurons. Table 4.1 illustrates that adding more layers beyond four only marginally enhances model accuracy while maintaining the same number of neurons. Likewise, increasing the number of neurons results in improved accuracy but entails a significant increase in computational cost. Beyond a certain threshold of neurons per layer (e.g., more than 96), the model's accuracy plateaus, with no substantial improvements observed.

Table 4.1 : Experimental results of the different model hyperparameters.

Hidden layers	Neurons (each layer)	Loss	Accuracy (%)	Recall	Precision
3	24	1.1794	64.90	0.0988	0.0811
	96	0.9467	67.30	0.1179	0.1119
	384	0.9367	69.37	0.1399	0.1373
4	24	1.1074	66.37	0.1008	0.0833
	96	**0.9179**	**69.51**	**0.1318**	**0.1331**
	384	0.9310	69.86	0.1177	0.1170
5	24	1.1867	66.86	0.1011	0.0826
	96	0.9106	69.96	0.1226	0.1521
	384	0.9083	69.91	0.1208	0.1130

Each hidden layer incorporates a fully connected layer with leaky rectified linear units as the activation function, ensuring that all neurons contribute to the output, even if their inputs are negative. The input to the neural network consists of 3-dimensional receiver locations based on GPS data, making the input layer of size 3. The output layer's size is equal to the number of beam pairs.

The learning rate, governing the step size at each iteration, is set to 10^{-4}, while other optimizer hyperparameters, namely the mini-batch size and the number of epochs, are configured as 256 and 1000, respectively. The solver for training the neural network is adaptive moment estimation (Adam), chosen for its ability to handle noisy problems and suitability for most scenarios [98]. Class weighting is applied, assigning smaller weights to classes that occur more frequently in the dataset and larger weights to less frequent classes.

To measure the discrepancy between predicted and actual target values during training, the cross-entropy loss function is employed. This widely adopted measure for classification tasks quantifies the dissimilarity between predicted probabilities and true labels [99]. The objective is to minimize this loss function during training. As the predicted probabilities approach the true labels, the cross-entropy loss approaches zero, indicating a better model fit. The cross-entropy loss L_{CE} is calculated as

$$L_{CE} = -\frac{1}{T}\sum_{t=1}^{T}\sum_{k=1}^{K} w_k z_{tk} \ln y_{tk}, \tag{4.7}$$

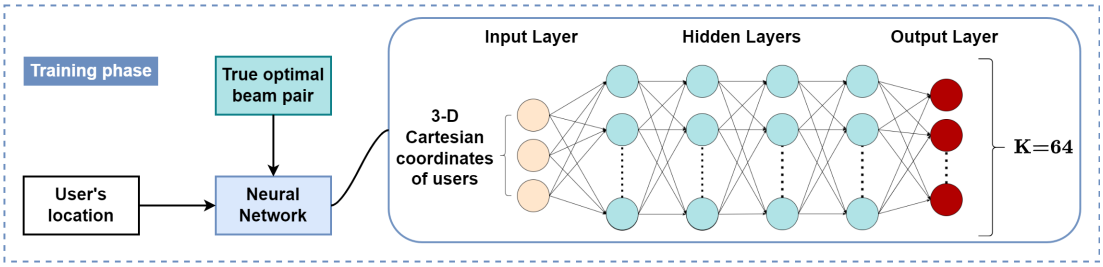


Figure 4.6 : The training step of the DNN model and its architecture.

where T is the number of samples, K is the number of classes, w_k is the weight for class k, z_{tk} is the indicator that the t-th sample belongs to the k-th class, and y_{tk} is the output for sample t for class k, derived from the softmax function. In essence, y_{tk} represents the probability that the network associates the t-th input with class k. The training phase of the DNN model and its architecture is illustrated in Figure 4.6.

In the testing phase, the trained network undergoes evaluation with previously unseen test data, employing the widely-used Top-K accuracy metric, commonly applied in neural network-based beam selection tasks [62,80].

For a given receiver location, the Top-K accuracy entails identifying K recommended beam pairs based on the neural network output. Subsequently, an exhaustive sequential search on these K beam pairs is conducted, and the one with the highest average RSRP is selected as the final prediction. The testing phase of the neural network is illustrated in Figure 4.7. In both datasets, the overall data is divided into 70% for training, 20% for validation, and 10% for testing.

Experiments conducted revealed an exponential increase in the complexity of the DNN with the number of layers. Utilizing the same number of neurons in each layer results in a complexity convergence to n^l, where n represents the number of neurons in each layer, and l is the number of layers. Additionally, adjustments in the number of beams at the Tx/Rx ends directly impact the total number of beam pair indices, serving as the output classes for the DNN, thereby influencing the DNN training process. Similarly, the incorporation of a multi-cell environment introduces new possible beam pairs, creating new output classes and influencing the dynamics of DNN training. Hence,

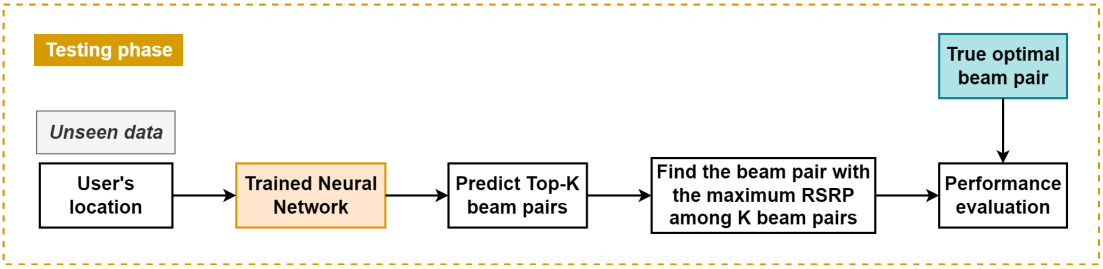


Figure 4.7 : The testing step of the DNN model with an unseen testing data.

variations in system parameters give rise to distinct scenarios, necessitating retraining of the DNN for adaptation.

4.2 Secure Multi-Point Coordinated Beamforming using Deep Learning

This section outlines the proposed beam selection procedure for secure multi-point coordinated beamforming. The beam selection problem in networks employing mMIMO and DPS-CoMP for secure radio coverage is addressed. The objective is to employ a DL-based secure multi-point coordinated beamforming method to enhance beam selection in 5G and beyond systems. The motivation behind this lies in improving the beam selection process in several aspects: (i) Enhancement of communication security: The method aims to choose a beam pair that not only maximizes the RSRP for the UE but also ensures that the RSRP for potential eavesdroppers remains below a specified threshold. (ii) Reduction in search space: Utilizing a DNN is intended to contribute to a decrease in both the time and energy expended during the beam selection process by narrowing down the search space. (iii) Utilization of CoMP for security: Besides its primary purpose, CoMP is employed to enhance data security against potential eavesdroppers.

A DNN-based CoMP beamforming scheme predicts the most secure beam pair indices between multiple coordinated TPs and the UE. The rationale for employing a DNN is to optimize latency, reduce signaling overhead, and minimize energy consumption during the beam search process by narrowing down the search space on both TPs, with a specific focus on enhancing communication security. Importantly, the proposed scheme relies solely on the coordinates of UEs as input, without incorporating

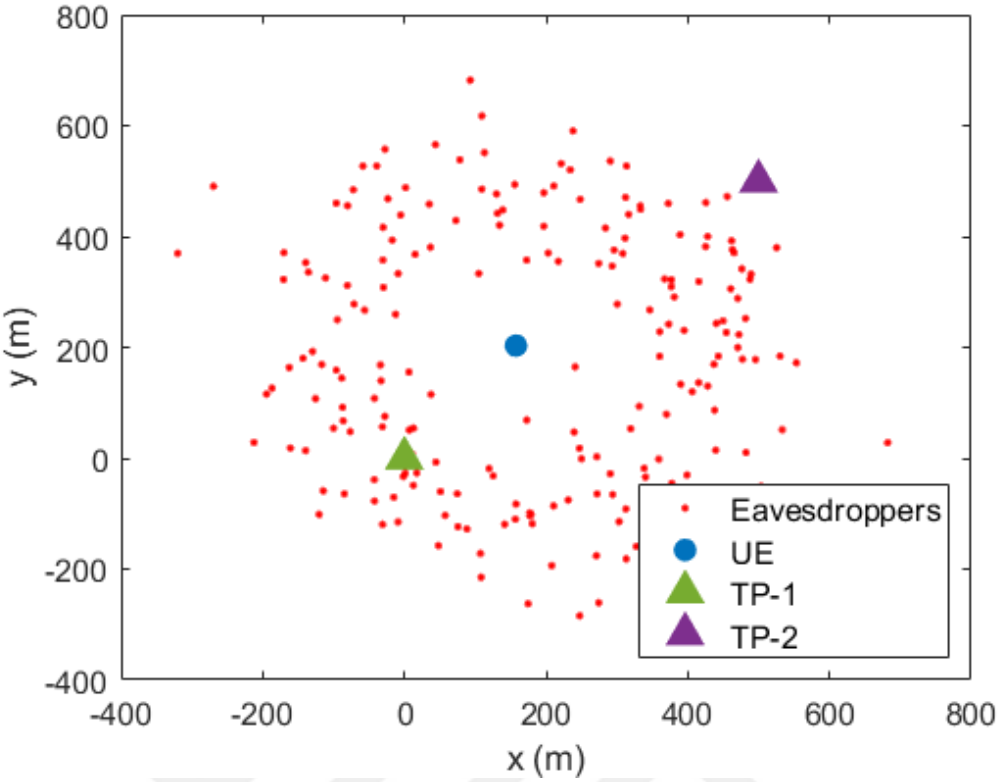


Figure 4.8 : The potential eavesdropper positions in a multi-point transmission scenario.

additional channel-based information such as AoA, RSRP levels, channel state information, etc.

To evaluate the proposed scheme, we use two distinct channel models: the terrain model and the statistical model. In terrain model, two geographically separated BSs are used to utilize DPS-CoMP scheme and assumed that UEs' data are available in both TPs. Furthermore, a statistical channel model is employed, generating data with 5G NR system variables, while UE and gNB locations are obtained from a real cellular network cluster. Two distinct scenarios are defined in both models: the first scenario aims to maximize RSRP and serves as a benchmark, while the second scenario, while also maximizing RSRP, is constrained by security considerations.

4.2.1 Channel model and antenna configuration

In the multi-point transmission channel model, the distribution of possible eavesdroppers remains consistent with the single-cell scenario, as illustrated for a CoMP environment with two TPs in Figure 4.8. It is assumed that eavesdroppers possess identical signal reception capabilities and antenna configurations, encompassing array geometry/size, azimuth and elevation limits, etc., as the legitimate users. Regardless of TP selection, the eavesdropper's location remains constant during communication.

In the CoMP system, two TPs are present, situated at different geographical sites, and UEs' data is accessible at all TPs for potential transmission. All TPs are assumed to be connected to a common central unit with zero delay. DPS-CoMP involves the real-time assessment of network conditions and UE locations to determine which TP should serve each user at any given time. This selection process is dynamic, changing rapidly as UEs move or network conditions fluctuate. The most suitable TP for serving a particular UE at any given time is determined based on the measurement of the best beam pairs between each TP and the UE. Hence, the selection of the best beam pair is achieved through an exhaustive search among all possible beam pairs.

A statistical model is used wherein signals are transmitted from multiple TPs and reflected from various scatterers toward a receiving array within a multi-path propagation channel. The antenna and channel configurations, including antenna array properties, the number of beams (eight beams at each Tx-Rx end), and channel characteristics, are assumed to be the same as in the single-cell scenario (see Figures 4.1 and 4.2).

Each TP conducts an exhaustive search by sweeping beams in all directions at fixed intervals within azimuthal and elevation limits. Subsequently, RSRP measurements are taken at a UE for each beamformed signal, and the results are reported. It's important to note that in the CoMP set, there are two TPs which double the search space from 64 to 128. This is because the same Rx beams of a specific user are swept for each TP.

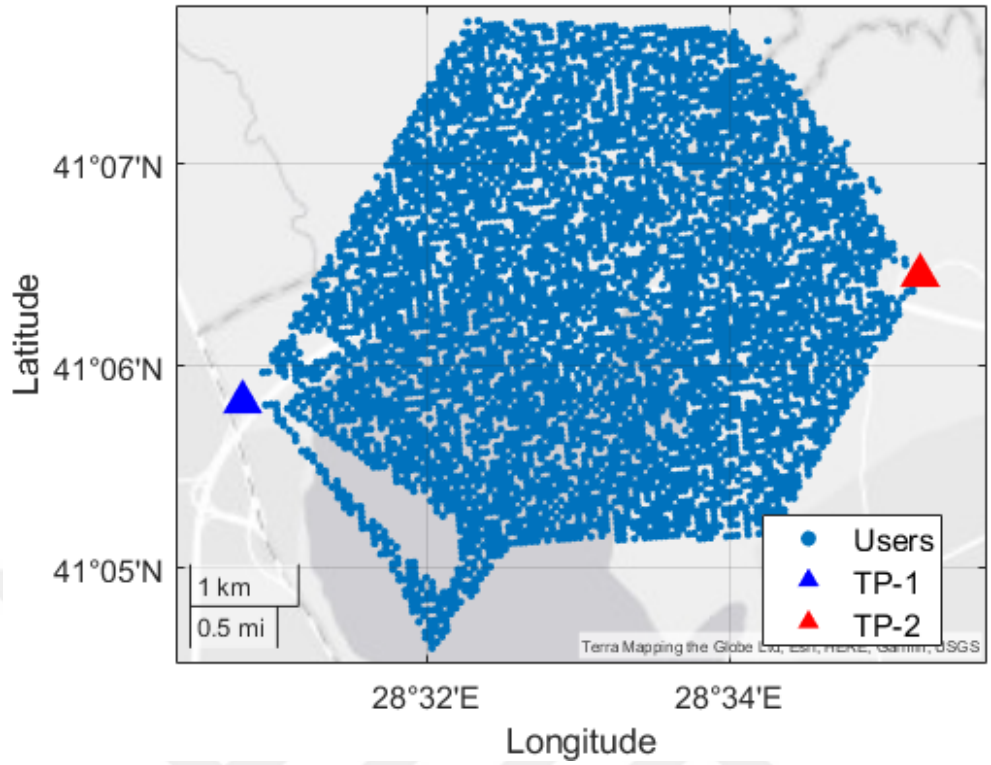


Figure 4.9 : User locations in a real cellular network served by two cells.

4.2.2 Multi-point secure beam selection algorithm

The primary objective of the proposed procedure is to identify the most suitable beam pair among TPs in the CoMP set. The aim is to maximize the RSRP for the legitimate user while ensuring that the eavesdropper's RSRP remains below β, if possible. The fulfillment of this condition is considered indicative of achieving secure and successful communication. It is assumed that an eavesdropper is present within the system, and the UE's knowledge of their location remains unspecified. A threshold value, denoted as β is defined, representing the minimum RSRP level required at the receiver's end (whether legitimate user or eavesdropper) for successful signal decoding, consistent with the single-cell scenario.

4.2.3 DNN model for multi-point transmission

A DNN-based approach is proposed to obviate the need for repetitive exhaustive searches and minimize communication overhead. The beam selection problem is

formulated as a classification task, aiming to identify the optimal Tx-Rx beam pair index by utilizing receiver coordinates as input for the DNN algorithm. Utilizing this out-of-band information, a trained DNN model generates a set of K promising beam pairs. Instead of conducting a comprehensive search across all potential beam pairs, the beam sweeping overhead is alleviated by focusing solely on the selected K beam pairs. It is worth noting that with an increasing number of beams and number of TPs in a CoMP set, the time overhead during beam sweeping also escalates.

4.2.3.1 Data generation

The first dataset for the proposed DNN involves a terrain model. Two TPs have been chosen from an actual cellular cluster located in the İstanbul/Büyükçekmece district of Türkiye, operating at 3.5 GHz. These geographically separated neighboring TPs have nearly opposite directions to effectively cover UEs situated between them. It is assumed that these TPs are connected to a common central unit with zero delay.

Within this cluster, 6000 hypothetical user locations have been selected, strategically positioned so that UEs at these locations can receive signals from both TPs. Employing the DPS-CoMP transmission scheme ensures that UEs' data is available at all TPs for transmission. The user and TP locations in this cluster are illustrated in Figure 4.9.

To prepare the data for training the DNN, RSRP values from both TPs are computed at these UE locations. This computation is carried out using a map-based radio network planning software, leveraging the parameters of the deployed cells and real 3D terrain information of the region. Subsequently, the calculated channel gains are aggregated with mMIMO antenna gains for all Tx-Rx beam pairs and for all TPs in a post-processing step. It is assumed that eight beams are available on both the Tx and Rx ends. In the final step, the best beam pair for each hypothetical user is determined through an exhaustive search across all possible beam pairs (a total of 128 beams), following Algorithm 2.

The second dataset of the multi-point transmission for the proposed DNN is generated through statistically simulated multi-path channels, incorporating 5G NR system variables. The same TP and UE locations from the terrain model are used. A spatial

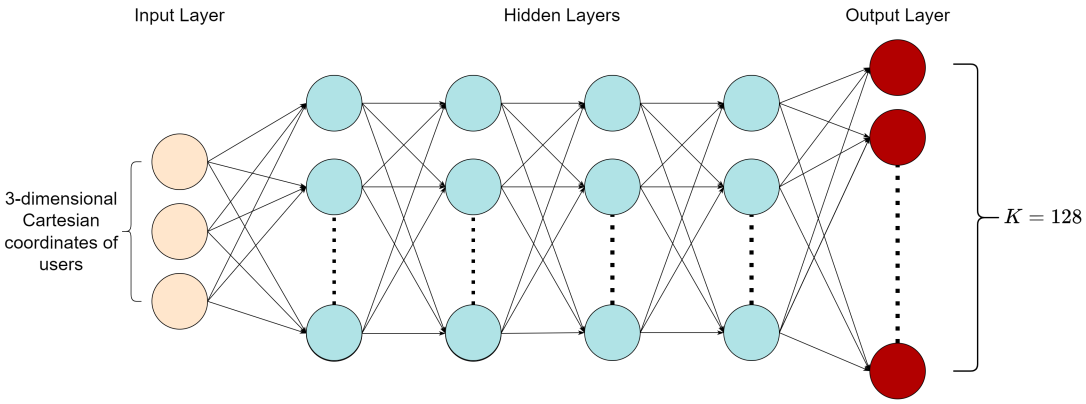


Figure 4.10 : The DNN architecture to predict beam pairs in multi-point transmission.

scattering MIMO channel is configured with multiple scatterers, and both TPs and UEs are equipped with URAs featuring 8-by-8 and 2-by-2 antenna elements, respectively.

Considering the specified number of beams at both the Tx and Rx ends, along with the defined sweep limits, the azimuth and elevation directions for various beams are determined. Subsequently, signals from each TP to each of these directions are beamformed and transmitted over the configured spatially-aware scattering channel. During the Rx-end beam sweeping process, the transmitted beamformed signals from each TP are sequentially received across each receive beam. Each of the K_T beams is transmitted K_R times, ensuring that each transmit beam is received over the M receive beams from each TPs.

After completing the dual-end sweep over a time duration of $K_T \times K_R$ time slots for each receive beam, the best beam pair is selected based on the comprehensive set of measurements obtained during the process.

4.2.3.2 DNN architecture

Similar to the approach for the single-cell scenario, the proposed neural network comprises four hidden layers, each with 96 neurons. In each hidden layer, a fully connected layer utilizes leaky rectified linear units as the activation function, enabling all network neurons to contribute to the output, even when their inputs are negative. The 3-D UE locations, derived from GPS data, serve as the input to the neural network.

Consequently, the input layer has a size of 3, while the output layer's size equals 128 (64 for each TP), representing the total number of beam pairs. The illustration of the DNN architecture is given in in Figure 4.10.

Subsequently, the trained DNN is tested with unseen data, considering the Top-K accuracy metric—a common performance measure in neural network-based beam selection tasks. The entire dataset is partitioned, allocating 70% for training, 20% for validation, and 10% for testing. Upon receiving a receiver location, the DNN recommends K beam pairs as the output. An exhaustive successive search on these Top-K beam pairs is then conducted, selecting the one with the highest RSRP or the highest RSRP with security constraints as the final prediction.

5. RESULTS AND DISCUSSION

In this chapter, the assessment of the effectiveness of the suggested DNN approach is provided by analyzing both the terrain model and the statistical model. The primary evaluation criterion employed is the Top-K accuracy measure. This metric is defined as the proportion of test cases in which the empirically determined optimal beam pair (identified through exhaustive search) is within the Top-K values of the softmax distribution generated by the DNN classifying the beam pairs, relative to the total number of test cases.

Four benchmarks are used to compare the performance of the proposed DNN method in terms of Top-K accuracy. Each of the following schemes generates K recommended beam pairs:

- Multi-class support vector machine (SVM) classifier: In the context of beam pair prediction, which involves a multi-class classification scenario, a multi-class SVM classifier is employed. The implementation utilizes an error-correcting output codes (ECOC) scheme, comprising $K(K-1)/2$ binary SVM models using the one-versus-one coding design. Here, K represents the number of unique class labels, with each class corresponding to a distinct beam pair index in our study.

- K-nearest neighbors algorithm (KNN): Classification using KNN considers the K nearest training data points to a given test data point and outputs the result based on a majority vote. In this study, the beam pairs assigned to the K nearest training data points (determined by GPS coordinates, i.e., Euclidean distances) for each test data point constitute a list of Top-K beam pairs, some of which may be repeated.

- Statistical choice: This approach arranges all beam pairs according to their relative frequency in the entire training data and selects the Top-K beam pairs for any given test data point.

- Random: In this scheme, K beam pairs are randomly and uniformly selected.

For both the terrain and statistical models in each transmission scheme (single-cell and multi-point), two distinct experiments are conducted:

(i) with the objective of maximizing RSRP while adhering to security constraints,

(ii) with the objective of maximizing RSRP without considering security.

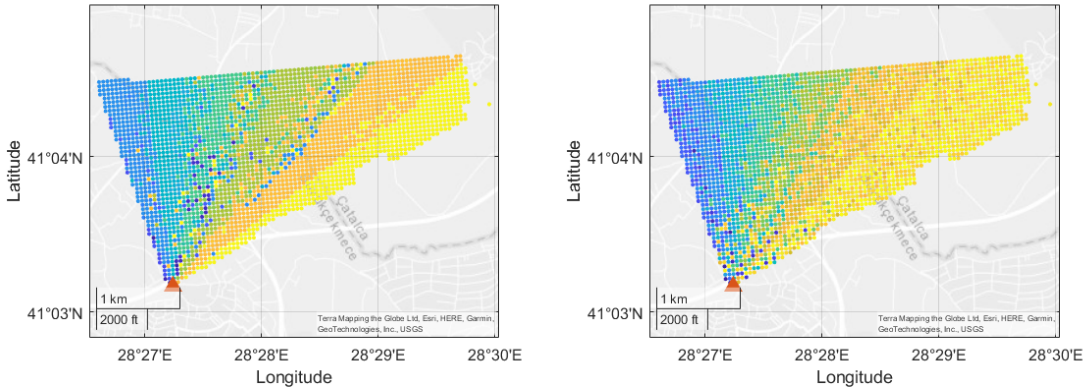
The second set of experiments serves as a baseline, demonstrating the extent of RSRP loss when security constraints are applied. The disparity in performance between the two experiments can be viewed as the trade-off in signal strength for ensuring communication security. Despite using the same DNN structure, characterized by the number of layers and neurons, for both experiments, the distinct best beam pairs for each objective necessitate separate DNNs for the two systems.

Depending on the locations of the UE and the eavesdropper, as well as the value of β, achieving secure communications, or even successful communications in some cases, may or may not be possible. To quantify these probabilities, two metrics are defined. The successful detection (SD) probability, P_{SD}, represents the likelihood of the UE receiving an RSRP above β. On the other hand, the secure and successful detection (SSD) probability, P_{SSD}, is the probability that the UE achieves an RSRP above β while the eavesdropper's RSRP remains below β. Once again, the distinction between these two metrics serves as an indicator of the cost incurred to attain a certain level of security.

5.1 Simulation Environment for Single-Cell Transmission Scenario

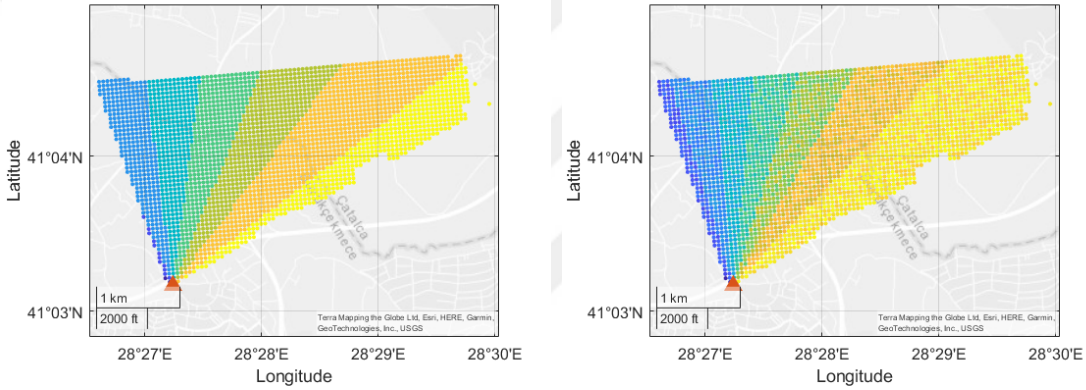
The first step of the study involves generating the dataset. Drawing from the described environmental configurations, two datasets—the terrain model and the statistical model—are created. These datasets, consisting of inputs and outputs, are then employed to train the proposed DNN scheme for both beam selection tasks, specifically maximizing RSRP with and without security constraints.

In Figures 5.1 and 5.2, the maps depict the Tx beams that yield the highest RSRP with and without security constraints, respectively, for all users. These figures are obtained through exhaustive search. The noticeable variability in the best Tx beams



(a) for the terrain model (b) for the statistical model

Figure 5.1 : The best Tx beams with security constraints for each user. Each color belongs to a different Tx beam.



(a) for the terrain model (b) for the statistical model

Figure 5.2 : The best Tx beams without security constraints for each user. Each color belongs to a different Tx beam.

under security constraints highlights that the beam achieving the highest RSRP is not consistently the best choice when taking security into account.

The simulation parameters for the single-cell transmission scenario are detailed in Table 5.1, encompassing essential 5G NR system variables relevant to beam management. Additionally, the table includes parameters specifying the dataset size used for training, validating, and testing the DNN. This comprehensive inclusion ensures that critical variables for both beam management and the DNN training process are clearly outlined, providing a thorough understanding of the simulation setup.

Table 5.1 : Simulation parameters for the single-cell transmission scenario.

Parameter	Value
Center frequency	3.5 GHz
SSB pattern	Case B
SSB length	8
Transmit array size, [rows cols]	[8 8]
Transmit azimuthal sweep limits	[-60, 60] (in 15° increments)
Transmit elevation sweep limits	[-90, 0]
Transmitter height	25 m
Receive array size, [rows cols]	[2 2]
Receive azimuthal sweep limits	[-180, 180] (in 60° increments)
Receive elevation sweep limits	[0, 90]
Receiver height	1.5 m
SNR	30 dB
RSRP mode	SSS with DMRS
Number of scatterers for each receiver (for the statistical model)	6
The security threshold β	-60 dBm [100]
Total number of users	9700
Total number of training data	6790
Total number of validation data	2037
Total number of test data	873

5.1.1 Terrain model

In this model, radio coverage levels are used based on real 3D terrain data obtained for an actual cellular cluster within an LTE network serving subscribers. RSRP values are gathered from this cell, taken at 9700 uniformly distributed geographic points, as illustrated in Figure 4.4. To model the influence of mMIMO for hypothetical users at these locations, the current panel antenna gain is subtracted from the RSRP level. Subsequently, the mMIMO antenna gains for each Tx-Rx beam pair are added.

For a specific legitimate user, an eavesdropper is choosen from 200 potential locations around the user, with a mean distance of 300 m, as depicted in Figure 4.3. Subsequently, the assessment is made as to whether the signal can be received with sufficient power at the location of a hypothetical eavesdropper. The received power of the legitimate user u in dBm is given by

$$P_{i,j}^{(u)} = P_T + G_{T_i}^{(u)} + G_{R_j}^{(u)} - P_L^{(u)}, \tag{5.1}$$

where P_T represents the transmit power in dBm, and $G_{T_n}^{(s)}$ and $G_{R_m}^{(s)}$ denote the antenna gains in dB for the n^{th} Tx beam and m^{th} Rx beam, respectively, as observed by user s (or eavesdropper). Additionally, $P_L^{(s)}$ represents the path loss in dB from the transmitter to user s (or eavesdropper). The same definitions as in Eq. (5.1) are applicable for the wiretap links for an eavesdropper, as shown below,

$$P_{i,k}^{(e)} = P_T + G_{T_i}^{(e)} + G_{R_k}^{(e)} - P_L^{(e)}. \tag{5.2}$$

5.1.2 The statistical channel model

Since the data for the terrain model is site-specific, influenced by unique channel behaviors tied to the terrain structure, we chose to generate additional results for a more generalized scenario. In this statistical model, the entire scenario, including the 5G NR system and parameters listed in the simulation parameters table, user and gNB locations, antenna array configurations, etc., is maintained. However, instead of relying on the channel behavior specific to the terrain model, a spatial scattering MIMO channel with six scatterers for each user is employed. An eavesdropper is randomly placed around them, and the air interface follows a channel model incorporating free space path loss.

Following the dual-end sweeping, SS-RSRP is measured for each beam pair using DMRS in addition to SSS, assuming the SSB information is known at the receiver. Ultimately, the optimal beam pair is determined based on the RSRP measurement for the intended purpose of beam selection, as explained in the algorithms for the highest RSRP and security, respectively. The secure and successful detection condition, defined earlier with the same threshold value, is also applied in this scenario. Eavesdroppers for each user follow similar reception procedures. However, due to the absence of coordination between the gNB and the eavesdropper, and as the eavesdropper measures its own RSRP based on the Tx beam selected for the legitimate user and can improve its RSRP only through receive-end beam sweeping, this procedure becomes single-end sweeping.

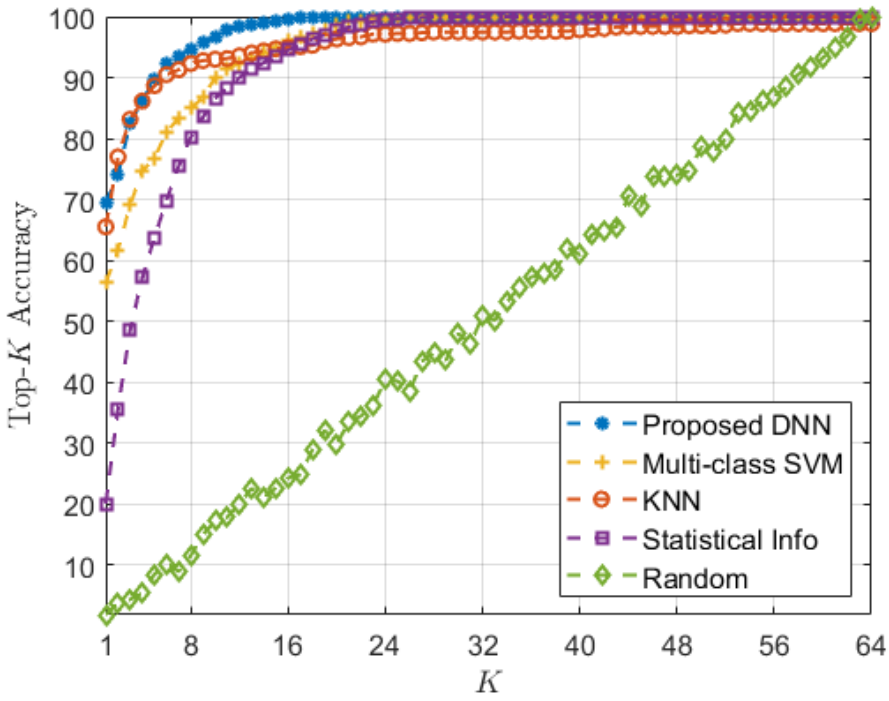


Figure 5.3 : Comparison of prediction performance for the terrain model with security constraints in a single-cell scenario.

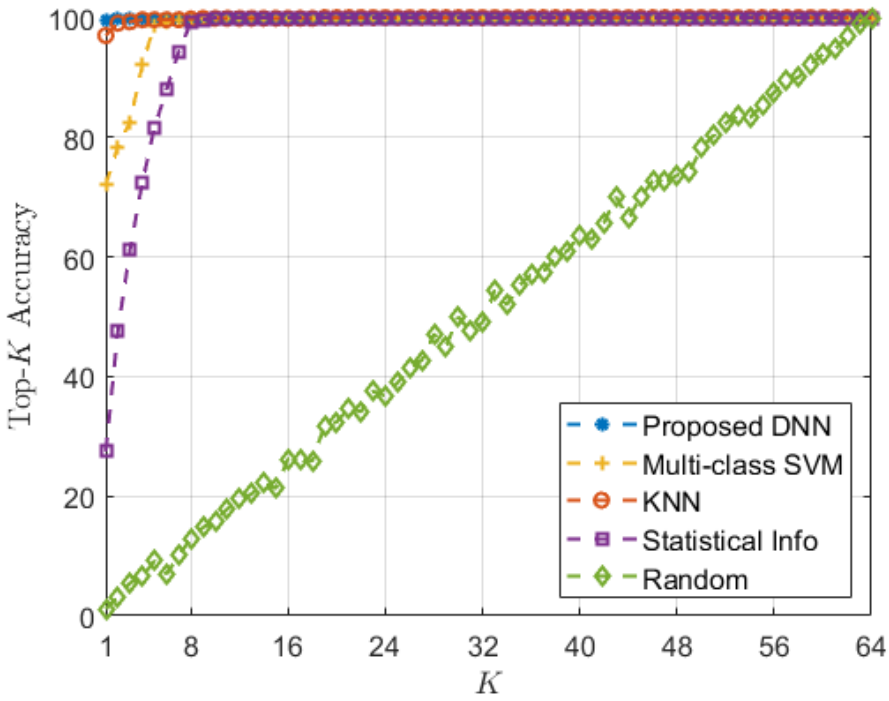


Figure 5.4 : Comparison of prediction performance for the terrain model without security constraints in a single-cell scenario.

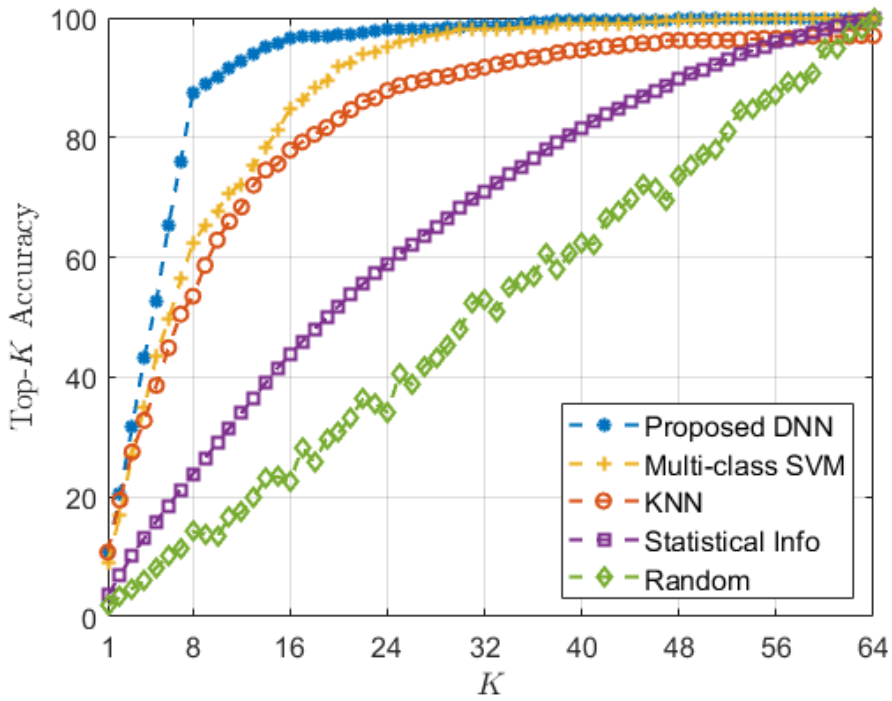


Figure 5.5 : Comparison of prediction performance for the statistical model with security constraints in the single-cell scenario.

5.1.3 Prediction performance of DNN

The Top-K accuracy of the proposed DNN under the terrain model settings, with and without security constraints, is presented in Figures 5.3 and 5.4, respectively. When security is not an objective, we observe that the proposed DNN is highly effective, achieving over 98% accuracy even with $K = 1$. In contrast, when security constraints are imposed, the accuracy reaches 90% with $K = 6$. This indicates that identifying the best beam pair for secure communications among all 64 beam pairs is a more challenging task than finding the beam pair that provides the highest RSRP.

It can be concluded that, based on the accuracy requirements, the proposed DNN has the potential to significantly reduce beam selection overhead when compared to exhaustive search. This improvement is particularly notable with low values of K, where sufficiently good performance can be attained. For example, Figure 5.3 shows that for K values of 5, 8, and 16, Top-K accuracy levels are 89.69%, 94.73%, and 99.66%, respectively, leading to 12.8-, 8-, and 4-fold overhead reduction.

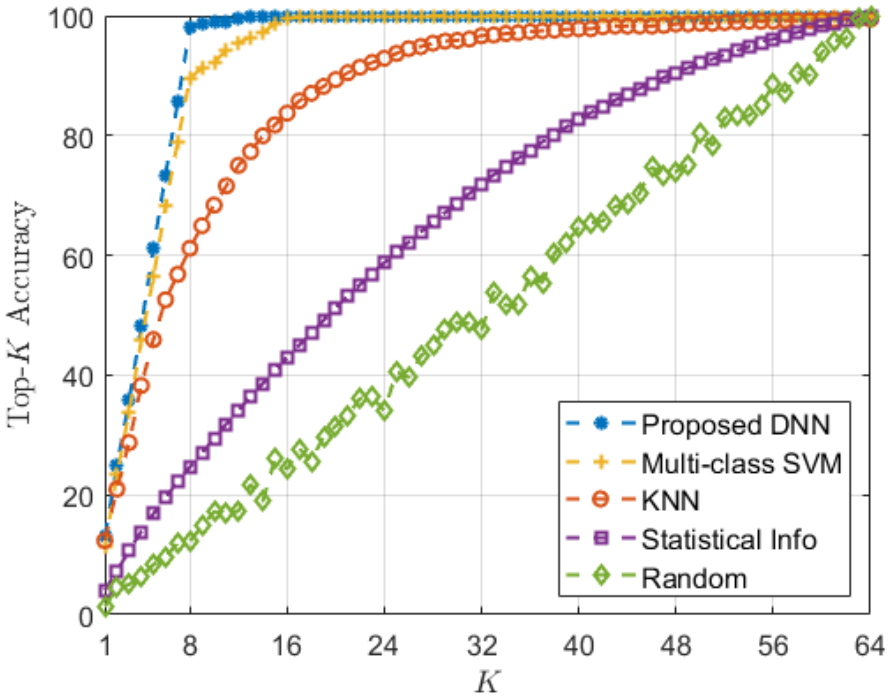


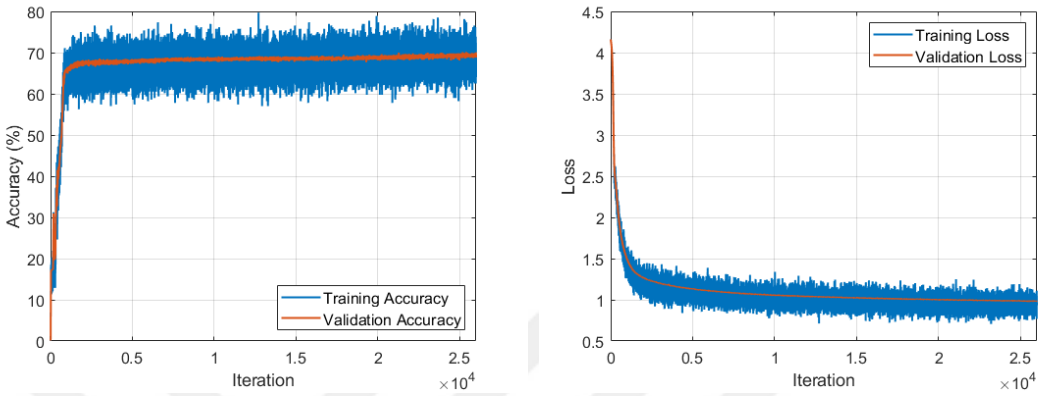
Figure 5.6 : Comparison of prediction performance for the statistical model without security constraints in the single-cell scenario.

The Top-K accuracy under the statistical model settings, with and without security constraints, is presented in Figures 5.5 and 5.6, respectively. A similar pattern emerges: when security constraints are not considered (Figure 5.6), the accuracy reaches 97.53% when $K = 8$. However, when security is taken into account, the accuracy is 90.10% with $K = 8$ and increases to 97.87% when $K = 16$.

Moreover, the proposed DNN surpasses other methods, particularly for lower values of K, underscoring the performance advantages of the DNN in terms of overhead reduction. Numerical results for accuracy, precision, and recall metrics comparing the proposed DNN with multi-class SVM and KNN are presented in Table 5.2 when $K = 1$ in the terrain model. Figure 5.7 also displays the training progress of the proposed DNN in terms of accuracy and loss. In predicting the best beam ($K = 1$) under a security constraint for the terrain data, the final validation loss (as defined in Eq.4.7) and the accuracy of the DNN are found to be 0.92 and 69.5%, respectively. Furthermore, Figure5.7(b) illustrates that both the validation and training loss of the proposed model are well-fitted, confirming that our model does not encounter overfitting or underfitting issues.

Table 5.2 : Classification metrics comparison of the proposed DNN with other learning schemes when $K = 1$ in the terrain model.

Learning scheme	Accuracy (%)	Recall	Precision
Proposed DNN	69.51	0.1318	0.1331
Multi-class SVM	56.36	0.0309	0.0357
KNN	65.52	0.0931	0.0982



(a) Training and validation accuracy

(b) Training and validation loss

Figure 5.7 : The training and validation curves of the proposed DNN subject to accuracy and loss when $K = 1$.

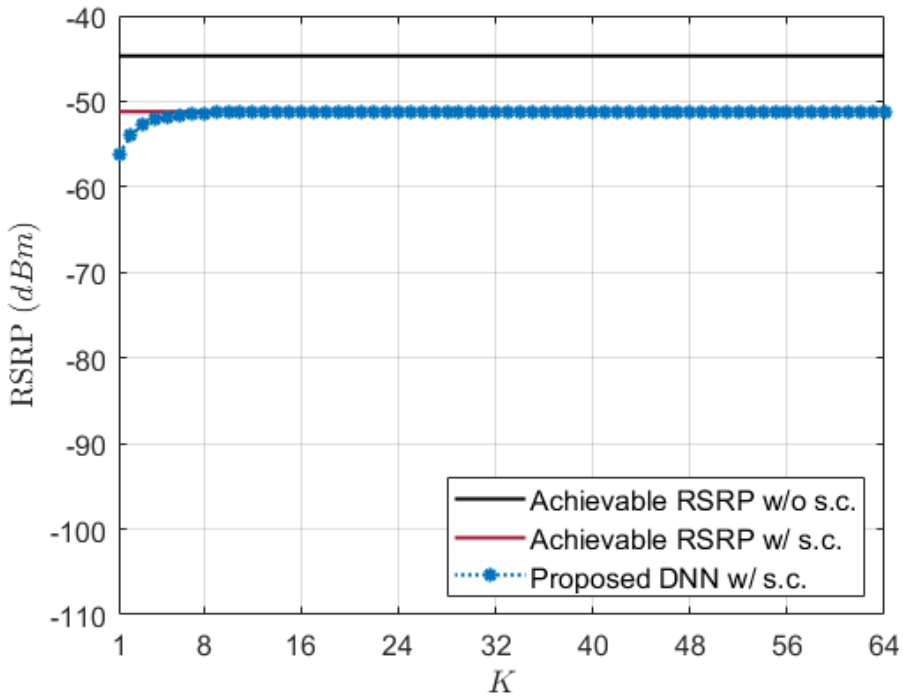


Figure 5.8 : Achievable RSRP values under varying conditions of security constraints (s.c.), along with the RSRP levels accomplished by the proposed DNN employing the Top-K beam pairs in the single-cell terrain model.

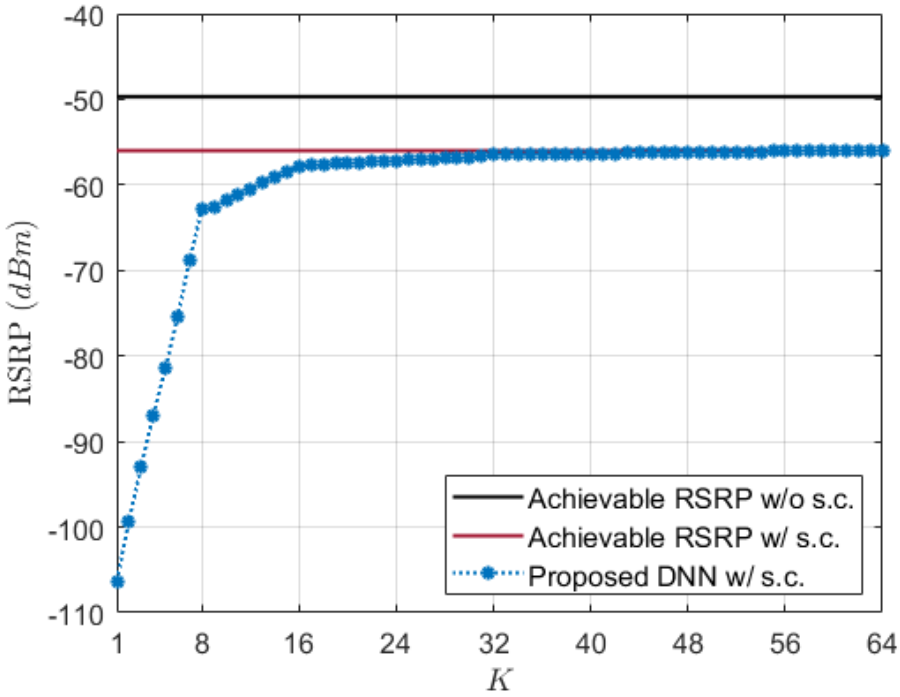


Figure 5.9 : Achievable RSRP values under varying conditions of security constraints (s.c.), along with the RSRP levels accomplished by the proposed DNN employing the Top-K beam pairs in the single-cell statistical model.

5.1.4 The achievable RSRP levels

In Figures 5.8 (for the terrain model) and 5.9 (for the statistical model), RSRP levels are depicted for three cases: (i) the highest attainable RSRP level without considering security constraints, identified through exhaustive search across all feasible beam pairs; (ii) the highest attainable RSRP level under imposed security constraints, determined through exhaustive search across all possible beam pairs (refer to Algorithm 2 on page 53); and (iii) the average RSRP level achieved by employing the proposed DNN scheme for beam selection over the Top-K beam pairs.

As observed, there is a 6.51 dB decline in the highest achievable RSRP level when security constraints are applied in the terrain model, while this decrease is 6.31 dB for the statistical model. This disparity in the highest achievable RSRP level can be interpreted as the expense of ensuring communication security, whenever required. In the terrain model, the proposed approach achieves 96.73% (0.1444 dB difference) and

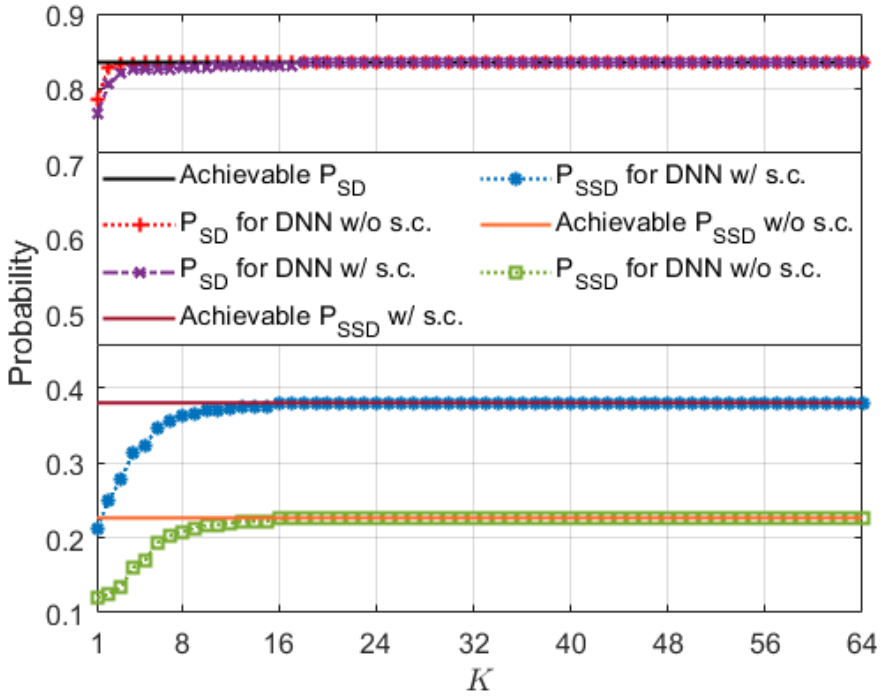


Figure 5.10 : Achievable probabilities for P_{SD} and P_{SSD} under different security constraints, and the corresponding probabilities achieved by the proposed method using Top-K beam pairs in the terrain model in a single-cell scenario.

99.89% (0.0047 dB difference) of the achievable RSRP level with security constraints when utilizing the Top-8 and Top-16 beam pairs, respectively, for beam selection. Conversely, these percentages are at 20.90% (6.7993 dB difference) and 66.13% (1.7961 dB difference) with the Top-8 and Top-16 beam pairs, respectively, for the statistical model.

5.1.5 The achievable P_{SD} and P_{SSD} probabilities

We present the SD and SSD probabilities (with and without security constraints) for both the terrain model and the statistical model in Figures 5.10 and 5.11, respectively. It should be noted that neither model results in a P_{SD} value of 1. This indicates that, due to the placement of the UEs, there are cases where it is not possible for the UE to achieve an RSRP exceeding β with any of the beam pairs, leading to communication failure. Moreover, since the attainable P_{SSD} falls below P_{SD} (and consequently, below 1), there are instances where security cannot be ensured, irrespective of the selected

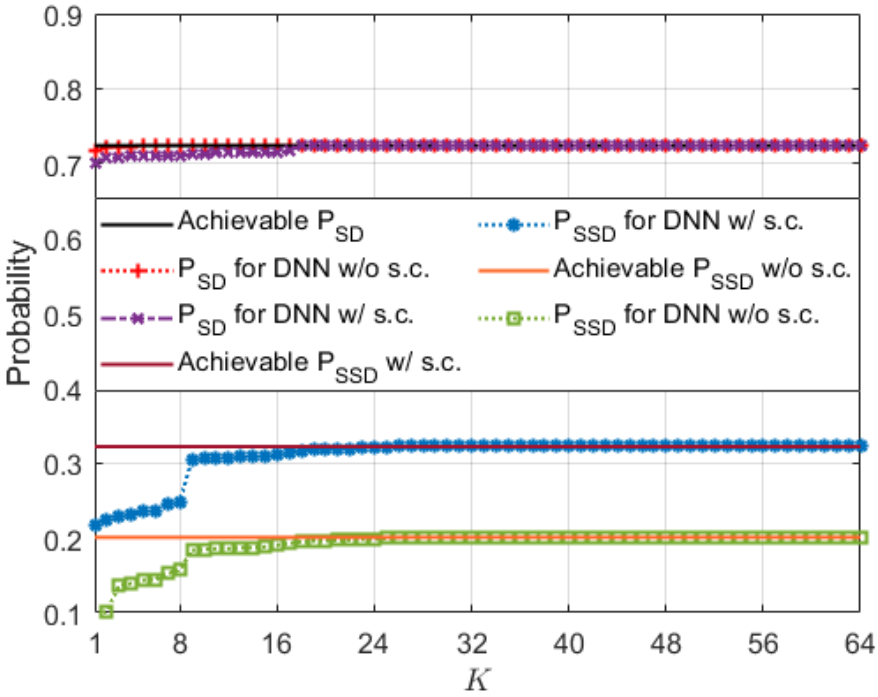
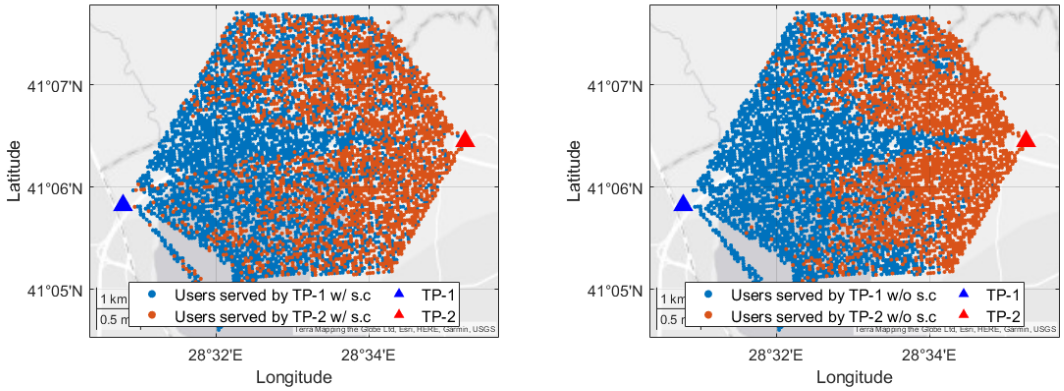


Figure 5.11 : Achievable probabilities for P_{SD} and P_{SSD} under different security constraints, and the corresponding probabilities achieved by the proposed method using Top-K beam pairs in the statistical model in a single-cell scenario.

beam pair. This limitation arises from the positioning of the eavesdropper, even if successful communication is feasible.

There is a meaningful difference between the achievable P_{SSD} values obtained from the DNN systems with and without security constraints, demonstrating that the proposed method significantly improves communication security. For the terrain model, when the Top-8 and Top-16 beam pairs are used for beam selection, P_{SSD} turns out to be 95.19% and 99.71% of the achievable P_{SSD} value, which is 0.3803. This is 1.6812 times the achievable P_{SSD} by the system with no security constraints, 0.2265. Similarly, for the statistical model, Top-8 and Top-16 P_{SSD} values are 77.23% and 96.80% of the achievable P_{SSD} value, which is 0.3219. This is 1.6055 times the achievable P_{SSD} by the system with no security constraints, 0.2005. We also observe that the curves for P_{SD} for both models when security constraints are imposed are almost identical to the P_{SD} curves for the system without security constraints. Therefore, we conclude that the proposed method does not compromise communication success to enhance security.



(a) with security constraints

(b) without security constraints

Figure 5.12 : Users distribution based on the serving TP.

5.2 Simulation Environment for Multi-Point Transmission Scenario

The dataset used to train the DNN is generated for two distinct tasks related to beam selection: maximizing RSRP with and without security constraints. In Figures 5.12(a) and 5.12(b), the selected TP for each UE, which provides the highest RSRP with and without security constraints, respectively, is illustrated on the map. These figures are generated through exhaustive search, revealing that under security constraints, the best beam pairs, and consequently, the best TP, exhibit greater variability. This emphasizes that the beam maximizing RSRP may not always be the optimal choice when security is a consideration.

In our model, we incorporate UE and BS locations, representing TPs in the CoMP set, derived from an actual cellular cluster. System parameters, including operating frequency, antenna properties, and dataset size for the DNN, are provided in Table 5.3.

5.2.1 Terrain model

In this model, RSRP levels are obtained from two geographically separated BSs, assumed to be TPs in a CoMP set with perfect synchronization. These RSRP levels are based on real 3D terrain data obtained from an actual cellular cluster within an LTE network serving subscribers. The RSRP values are collected from these cells at 6000 uniformly distributed geographic points, as illustrated in Figure 4.9. To simulate

Table 5.3 : Simulation parameters for the multi-point transmission scenario.

Parameter	Value
Center frequency	3.5 GHz
Number of beams at each Tx-Rx ends	8
Transmit array size, [rows cols]	[8 8]
Transmit azimuthal sweep limits	[-60 60] (in 15° increments)
Transmit elevation sweep limits	[-90 0]
Transmitter height	25 m
Receive array size, [rows cols]	[2 2]
Receive azimuthal sweep limits	[-180 180] (in 60° increments)
Receive elevation sweep limits	[0 90]
Receiver height	1.5 m
SNR	30 dB
Number of scatterers for each receiver and eavesdropper	6
The security threshold (β)	-60 dBm [100]
Total number of users	6000
Total number of training data	4200
Total number of validation data	1260
Total number of test data	540

the impact of mMIMO for hypothetical users at these locations, the existing panel antenna gain of each TP is subtracted from the calculated RSRP level. Subsequently, the mMIMO antenna gains for each Tx-Rx beam pair are added.

DPS involves the real-time assessment of network conditions and UE locations to determine the optimal TP for serving each user at any given moment. The selection of the most suitable TP for a specific UE is based on the measurement of the best beam pairs between each TP and the UE. This involves an exhaustive search among all possible beam pairs to select the one with the highest RSRP or the highest RSRP under security considerations. The remaining variables, including eavesdroppers' distribution, antenna configurations, and received power calculations (as given in Eq. 5.1 and 5.2) remain consistent with the single-cell scenario.

5.2.2 The statistical channel model

Given that the data for the terrain model is site-specific and exhibits unique channel behavior influenced by the terrain structure, we have chosen to produce additional outcomes for a more generalized scenario. In this statistical model, we maintain

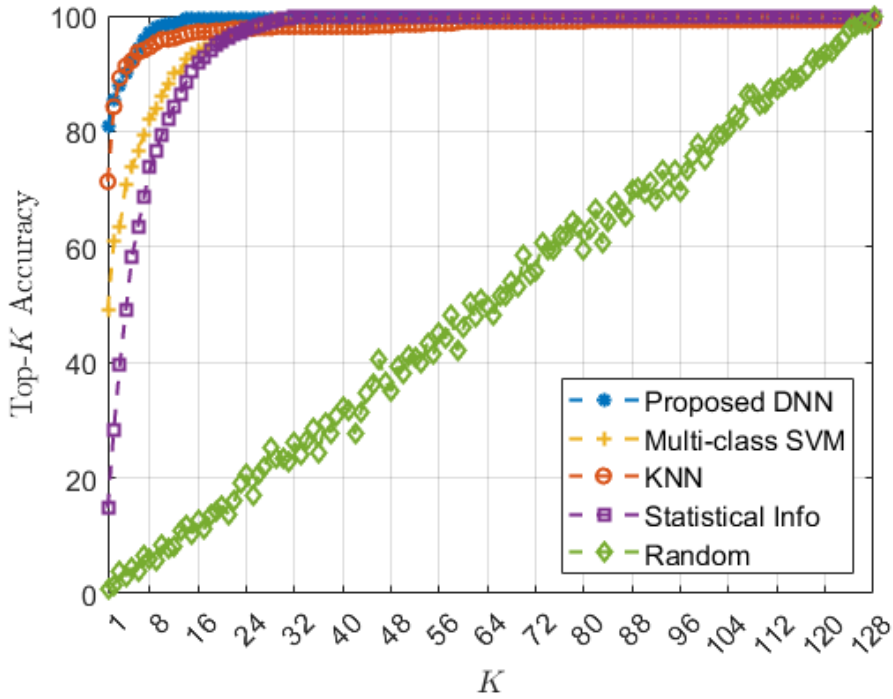


Figure 5.13 : Comparison of prediction performance for the terrain model with security constraints in the multi-point scenario.

the entirety of the scenario, encompassing the 5G NR system and other parameters outlined in Table 5.3, as well as user and gNB locations, antenna array configurations, and so forth. However, instead of relying on the terrain model's specific channel behavior, we employ a spatial scattering MIMO channel configured with six scatterers for each user. An eavesdropper is randomly positioned in their vicinity, and the air interface adheres to a channel model that incorporates free space path loss.

After the completion of dual-end sweeping, RSRP is measured for each beam pair (128 in total, with 64 in each TP) at the receiver. Subsequently, the best beam pair is determined based on the RSRP value for the intended purpose of beam selection, and consequently, TP selection. These purposes are defined separately for experiments focusing on achieving the highest RSRP and ensuring security. The TP selection for each UE is decided based on the index of the selected beam pair, where indices 1 to 64 correspond to TP-1, and indices 65 to 128 correspond to TP-2. Eavesdroppers for each UE follow the same reception procedures from their respective ends. However, due to the lack of coordination between the TPs and the eavesdropper, each eavesdropper measures its own RSRP based on the Tx beam selected for the legitimate user. Any

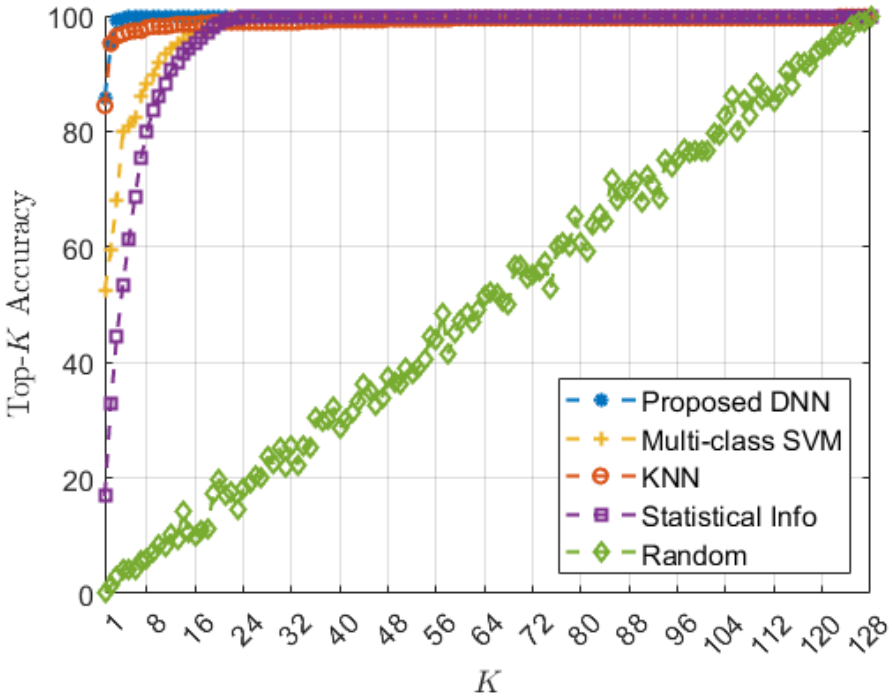


Figure 5.14 : Comparison of prediction performance for the terrain model without security constraints in the multi-point scenario.

potential improvement in RSRP for the eavesdropper can only be achieved through sweeping its Rx-end beams. Consequently, this procedure becomes a single-end sweeping.

5.2.3 Prediction performance of DNN

In multi-point transmission scenario, the Top-K accuracy results for the proposed DNN in the terrain model, both with and without security constraints, can be found in Figures 5.13 and 5.14, respectively. In cases where security considerations are not paramount, the proposed DNN demonstrates remarkable accuracy, surpassing 99% even when $K = 3$. However, the introduction of security constraints results in a slight reduction in prediction accuracy, albeit still impressive at 99% even when K is increased to 13. This underscores the complexity of the task of identifying the optimal beam pair for secure communication among the 128 possible pairs, a challenge more intricate than selecting the pair with the highest RSRP.

Depending on specific accuracy requirements, the proposed DNN significantly diminishes beam selection overhead in comparison to exhaustive search, particularly

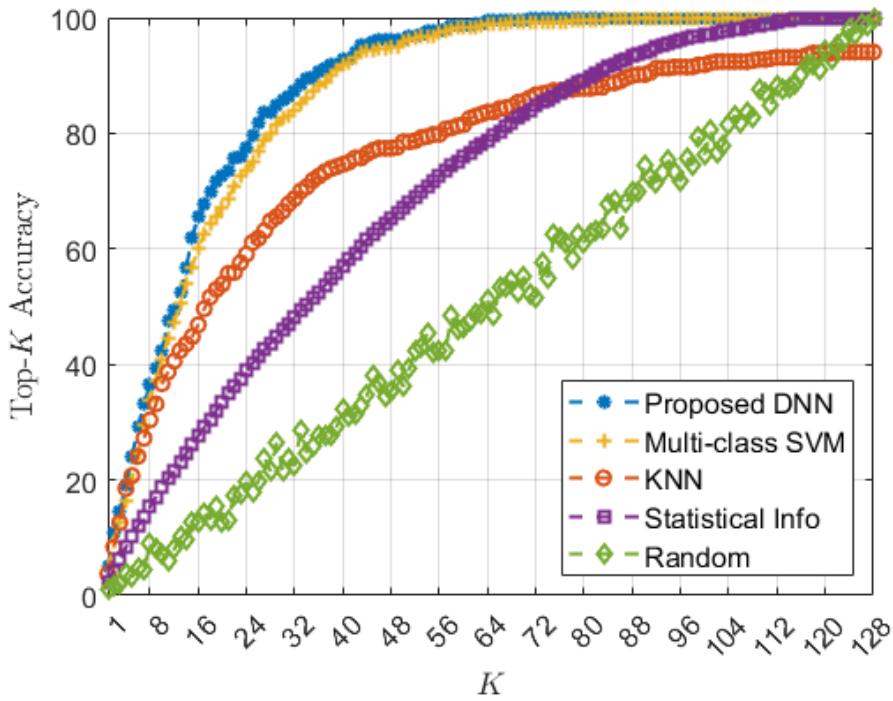


Figure 5.15 : Comparison of prediction performance for the statistical model with security constraints in the multi-point scenario.

with lower values of K. For example, as illustrated in Figure 5.13, K values of 1, 8, and 16 achieve Top-K accuracy levels of 80.74%, 97.04%, and 99.63% respectively, resulting in respective overhead reductions of 128-fold, 16-fold, and 8-fold. Moreover, the DNN consistently outperforms other methods, especially at lower K values, underscoring its effectiveness in reducing overhead.

In the statistical channel model, where data is generated through the statistical simulation of multi-path channels for identical UE and TP locations, Figures 5.15 and 5.16 present the Top-K accuracy results with and without security constraints, respectively.We observe a consistent pattern here: the accuracy, when security constraints are not considered (Figure5.16), peaks at 96.85% for $K = 16$. Conversely, when security is taken into account, the accuracy is 90.74% for $K = 36$ and rises to 96.3% for $K = 46$.

5.2.4 The achievable RSRP levels

In the multi-point transmission scenario, as depicted in Figures 5.17 (illustrating the terrain model) and 5.18 (representing the statistical model), RSRP levels are

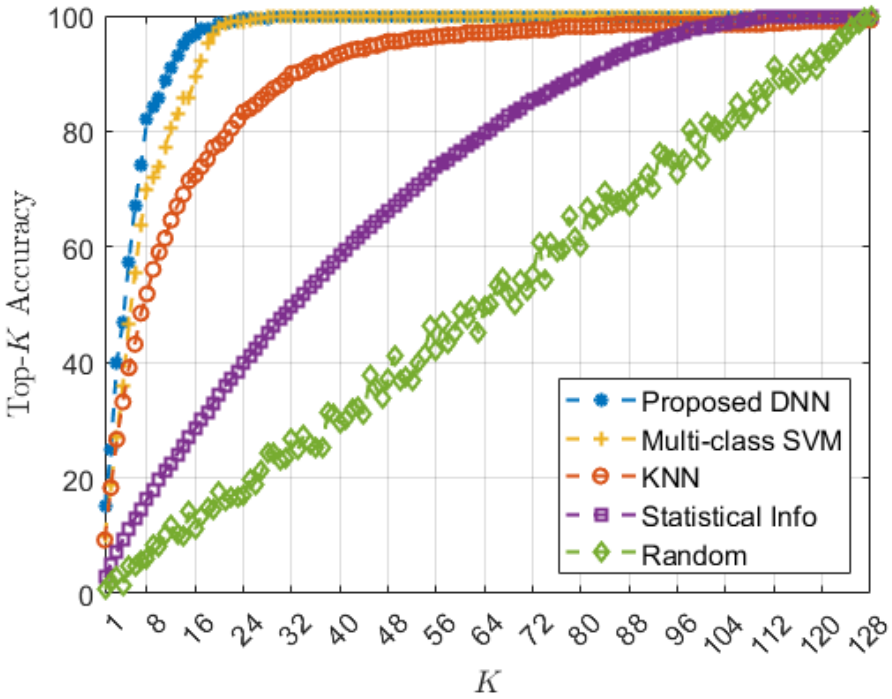


Figure 5.16 : Comparison of prediction performance for the statistical model without security constraints in the multi-point scenario.

presented across three scenarios: (i) the maximum achievable RSRP level, wherein security constraints are disregarded, determined through an exhaustive exploration of all possible beam pairs, (ii) the highest achievable RSRP level under the imposition of security constraints, established through an exhaustive search encompassing all potential beam pairs (refer to Algorithm 2 on page 53), and (iii) the average RSRP level attained through the utilization of the proposed DNN scheme, with beam selection executed over the Top-K beam pairs.

As noted, there exists a 1.18 dB reduction in the highest achievable RSRP level when security constraints are implemented in the terrain model, while this reduction is 3.8 dB in the statistical model. This variation in the highest achievable RSRP level can be considered as the trade-off for fortifying communication security whenever deemed feasible. For the terrain model, the proposed method achieves 99.33% (with a 0.4321 dB difference) and 99.99% (with a 0.003 dB difference) of the achievable RSRP level under security constraints when utilizing the Top-8 and Top-16 beam pairs, respectively, for beam selection. Conversely, these metrics stand at 98.39% (with a 0.8049 dB difference) and 99.42% (with a 0.2855 dB difference) with the Top-8

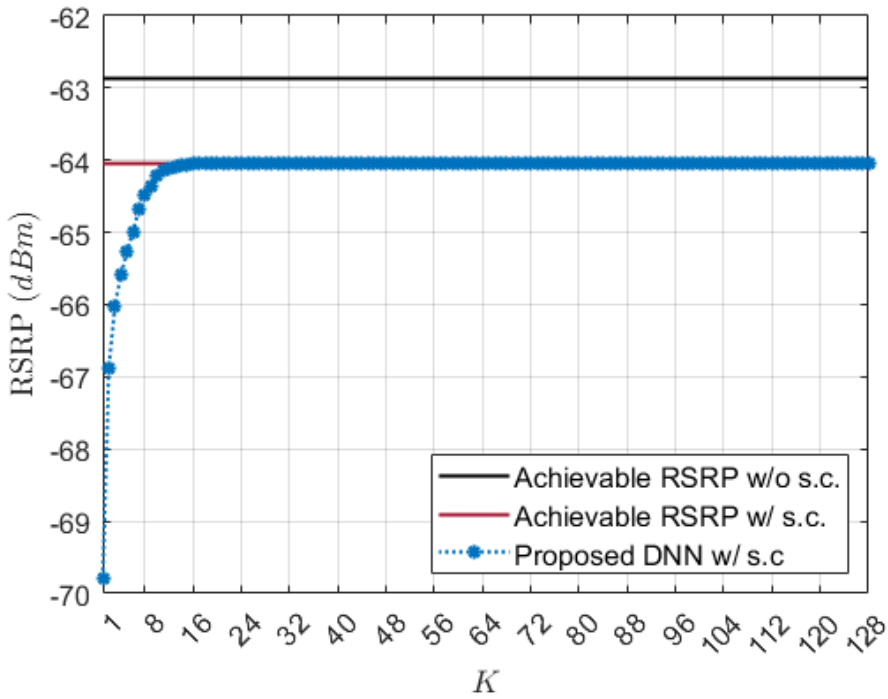


Figure 5.17 : Achievable RSRP values under varying conditions of security constraints (s.c.), along with the RSRP levels attained by the proposed DNN employing the Top-K beam pairs in the multi-point terrain model.

and Top-16 beam pairs, respectively, for the statistical model. Based on these results, we can conclude that the optimal beam predictions of our proposed DNN method, even subject to security constraints, attain the achievable value at significantly lower K values. This underscores the efficiency of employing DNNs in such tasks as opposed to an exhaustive search.

5.2.5 The achievable P_{SD} and P_{SSD} probabilities

The SD and SSD probabilities (with and without security constraints) are given in Figures 5.19 (for the terrain model) and 5.20 (for the statistical model). It should be noted that neither model leads to a P_{SD} value of 1. This implies that, due to the placement of the UEs, there are cases where it is not possible for the UE to observe an RSRP that exceeds β with any of the beam pairs. Consequently, communication will fail. Additionally, as the achievable P_{SSD} is below P_{SD} (and by extension, below 1), there are instances where security cannot be attained, regardless of the beam pair used.

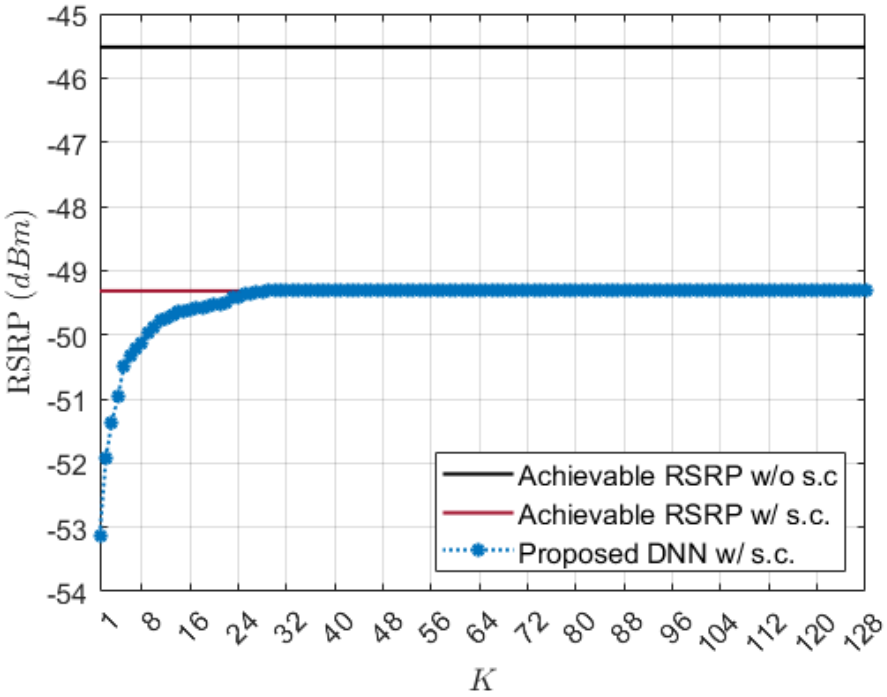


Figure 5.18 : Achievable RSRP values under varying conditions of security constraints (s.c.), along with the RSRP levels attained by the proposed DNN employing the Top-K beam pairs in the multi-point statistical model.

This is due to the placement of the eavesdropper, even if successful communication is possible.

It is evident that there is a meaningful difference between the achievable P_{SSD} values obtained from the DNN systems with and without security constraints. This observation demonstrates that the proposed method significantly enhances communication security.

For the terrain model, when utilizing the Top-8 and Top-16 beam pairs for beam selection, P_{SSD} is found to be 96.25% and 99.06% of the achievable P_{SSD} value, which is 0.3954. This represents a 2.0143-fold increase over the achievable P_{SSD} in the system without security constraints, which is 0.1963. Similarly, for the statistical model, the Top-8 and Top-16 P_{SSD} values are 54.67% and 74.40% of the achievable P_{SSD} value, which is 0.5352. This corresponds to a 1.3389-fold increase over the achievable P_{SSD} in the system without security constraints, which is 0.3972.

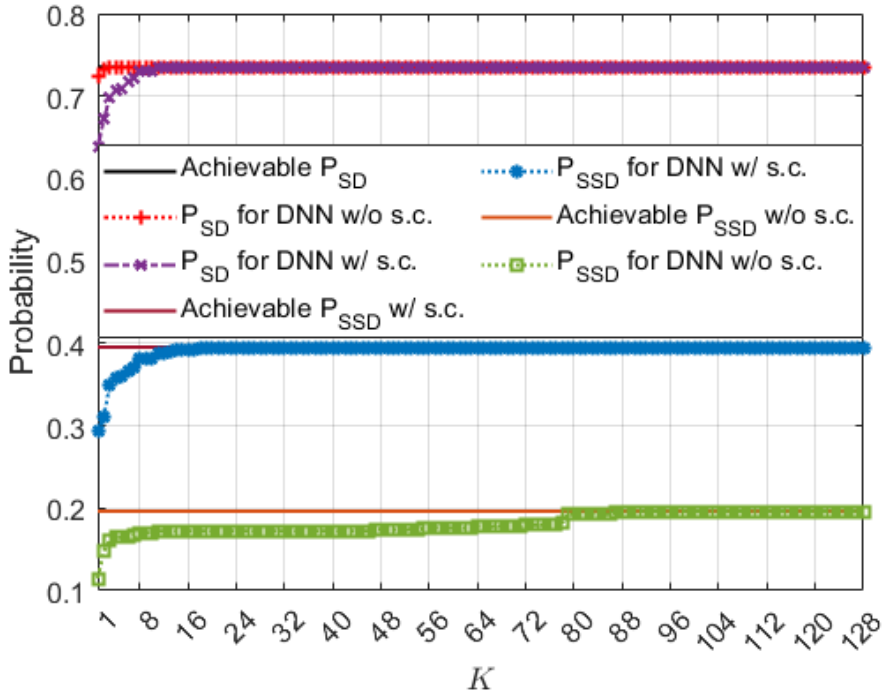


Figure 5.19 : The achievable P_{SD} and P_{SSD} probabilities with and without security constraints (s.c.), and the P_{SD} and P_{SSD} probabilities the proposed method achieves using the Top-K beam pairs for the terrain model in the multi-point scenario.

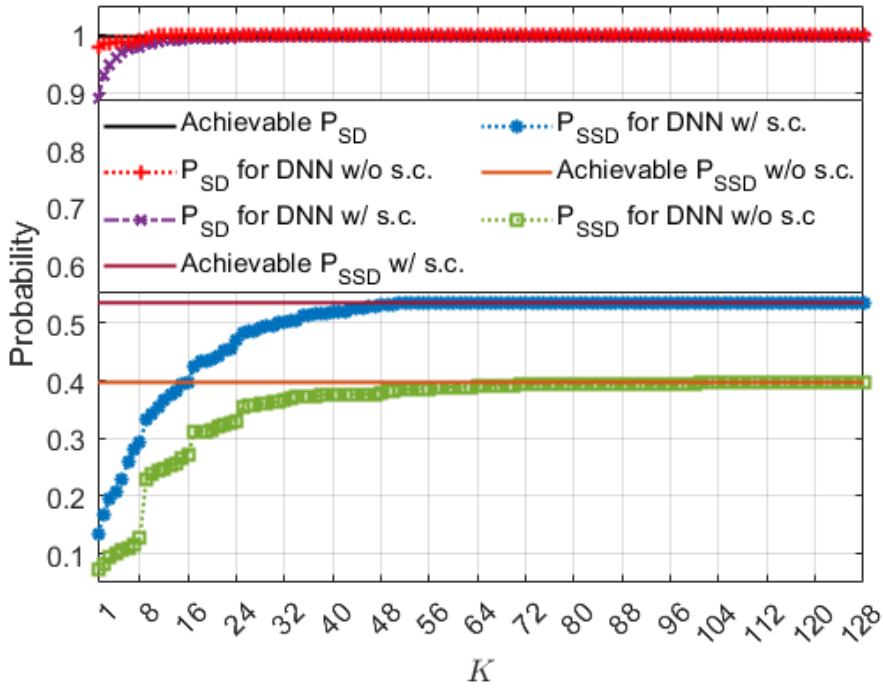


Figure 5.20 : The achievable P_{SD} and P_{SSD} probabilities with and without security constraints (s.c.), and the P_{SD} and P_{SSD} probabilities the proposed method achieves using the Top-K beam pairs for the statistical model in the multi-point scenario.

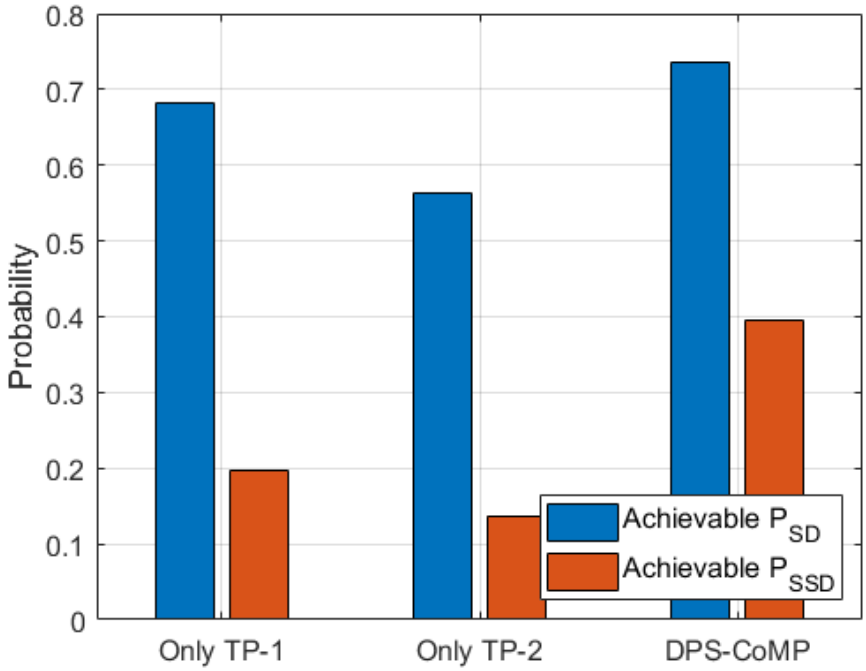


Figure 5.21 : The achievable P_{SD} and P_{SSD} probabilities with and without DPS-CoMP for the terrain model.

It is noteworthy that the curves for P_{SD} for both models, when security constraints are imposed, closely align with the P_{SD} curves for the system without security constraints. Therefore, we can infer that the proposed method does not compromise communication success to enhance security.

5.3 Examining Security in Single-Cell vs. Multi-Point Transmission

Figure 5.21 for the terrain model and Figure 5.22 for the statistical model illustrate a hypothetical scenario where users are exclusively served by a single TP, indicating a single-cell scenario. A significant improvement in P_{SSD} performance is observed when employing DPS-CoMP transmission. For example, in the absence of CoMP in the terrain model, secure and successful communication can only be achieved at around a rate of 20%. However, with the implementation of the DPS-CoMP scheme, P_{SSD} increases to 39.54%, signifying a 100% improvement in terms of security.. Intrinsically, CoMP also enhances P_{SD} by ensuring user data availability at each TP.

Similar trends are evident in the statistical model, where secure and successful communication can only be achieved at a rate of 35% in the absence of CoMP.

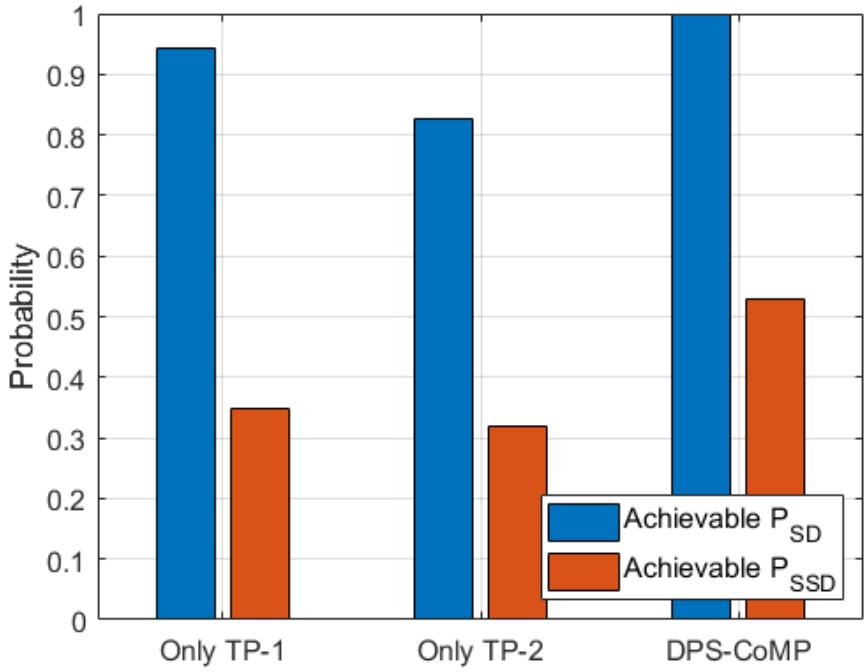


Figure 5.22 : The achievable P_{SD} and P_{SSD} probabilities with and without DPS-CoMP for the statistical model.

However, when multi-point transmission is employed, P_{SSD} increases significantly from 51.76% to 66.64%, while P_{SD} increases from 5.91% to 20.86%. Based on these results, the utilization of the DPS-CoMP scheme in the statistical model leads to a P_{SD} probability that nearly reaches 1. This indicates that successful communication (though not guaranteed to be secure at all times) is consistently maintained.

6. CONCLUSIONS AND FUTURE WORKS

In this thesis, we propose a deep learning-based secure beam selection method for both single-cell and multi-point coordinated transmission schemes in 5G and beyond systems. We introduce two transmission models. The first model utilizes a DNN for secure initial access and beam alignment in a single-serving cell scenario. Here, the DNN automates the SSB beam sweeping procedure, acting as a proof of concept to showcase the compatibility of our proposed DNN with established standards. Departing from the conventional approach of selecting the beam pair with the highest RSRP, our method prioritizes choosing a beam pair that not only maximizes RSRP for the UE but also endeavors to keep the RSRP observed by potential eavesdroppers below a predefined threshold. This approach achieves a certain level of security against eavesdropping attacks through the intrinsic features of mMIMO and beamforming, without relying on additional security measures.

The second model delves into the beam selection challenges within networks employing mMIMO and DPS-CoMP for ensuring secure radio coverage. Here, we introduce a DNN-based CoMP beamforming scheme aimed at predicting the most secure beam pair indices between multiple coordinated TPs and the UE. This proposal aligns with the same rationale as the single-cell scenario, emphasizing the overarching goal of enhancing security and efficiency in beam selection processes.

The improvements provided by the proposed method are threefold:

- Communication security is enhanced by selecting a beam pair that not only maximizes the RSRP for the UE but also maintains the RSRP for potential eavesdroppers below a certain threshold.
- The use of a DNN to reduce the search space contributes to a reduction in both the time and energy consumed during the beam selection process.

- In addition to its primary purpose, CoMP is leveraged to secure data against eavesdroppers.

Importantly, the proposed method relies solely on location information and does not depend on any channel parameters or estimation procedures. Furthermore, no additional physical layer security method is employed, and no modifications to existing standards are necessary.

Our approach is practical and aligns with 5G NR signaling without necessitating modifications to the standard. Nevertheless, variations in system parameters, as detailed in Tables 5.1 and 5.3, introduce distinct scenarios. Consequently, each change requires retraining the DNN for adaptation.

To delineate and assess our proposed DL-based method, we employ two scenarios. The first scenario, referred to as the terrain model, sources its data from a network planning software. This software computes RSRP values using parameters extracted from various currently operational cells, along with authentic 3D terrain data. For a more thorough comprehension of the efficacy of our proposed method, we introduce a second scenario, designated as the statistical model. This scenario involves the utilization of synthetically generated data using a statistical channel model, incorporating 5G NR system variables as outlined in the 3GPP, providing a robust and comprehensive evaluation framework.

Numerical assessments for single-cell transmission reveal the potential for a substantial reduction in the beam pair search space, with an impressive 92.19% decrease—from 64 down to 5—with an accuracy rate of 89.69%. Furthermore, achieving a high accuracy of 99.66% is still feasible with a 75% reduction in the beam pair search space, bringing it down to 16 from the original 64. This dynamic optimization underscores the efficiency of the proposed approach.

Moreover, the enhancement in secure communication probability is noteworthy, demonstrating an improvement of up to 68.12% compared to a system without security constraints. This substantial increase underscores the efficacy of our method in fortifying the security aspects of the communication system.

In the context of multi-point coordinated transmission, we observe significant achievements. A notable reduction of up to 96.1%—from 128 down to 5—in the beam pair search space is attainable, maintaining a very high accuracy of 99.82% for the terrain model. Alternatively, achieving a high accuracy rate of 99.63% is viable with a 50% reduction—bringing the beam pair search space down to 64 from the original 128 in the statistical model. This showcases the versatility of our approach in optimizing the search space for varied accuracy requirements.

When comparing the single-cell and multi-point coordinated transmission schemes in terms of security, we observe a notable increase in the probability of secure and successful communication. The enhancement ranges from 66.64% to 100%, contingent upon the choice of the channel model. This shift underscores the effectiveness of our approach in fortifying the security aspect, presenting a considerable improvement in the likelihood of secure and successful communication across varying transmission scenarios.

6.1 Suggestions for Future Works

Several promising avenues for future research can be explored. One potential direction involves the design of a DNN scheme for optimizing beam refinement procedures at both the Tx and Rx ends. This could contribute to further enhancing the efficiency of the beam alignment process in wireless communication systems.

Additionally, investigating multi-cell scenarios, particularly those involving CoMP, presents an intriguing area of research. Focusing on aspects such as beam switching and beam recovery, with a dedicated emphasis on security considerations, could provide valuable insights into the complexities of secure communication in advanced network configurations.

Another avenue for exploration is the development of a DNN scheme tailored for other CoMP schemes, such as JT-CoMP. Conducting a comparative analysis of various CoMP schemes from a security perspective would offer valuable insights into their respective strengths and weaknesses. This comparative study could contribute to the optimization and selection of CoMP schemes based on their security attributes.

In summary, future research could delve into refining beam procedures, exploring multi-cell scenarios with a security focus, and extending DNN schemes to other CoMP configurations, fostering advancements in secure and efficient communication systems.

REFERENCES

[1] **Björnson, E.**, **Hoydis, J. and Sanguinetti, L.** (2017). Massive MIMO Networks: Spectral, Energy, and Hardware Efficiency, *Foundations and Trends® in Signal Processing*, *11*(3-4), 154–655.

[2] **Heng, Y. and et. al.** (2021). Six Key Challenges for Beam Management in 5.5G and 6G Systems, *IEEE Communications Magazine*, *59*(7), 74–79.

[3] **Marsch, P. and Fettweis, G.P.** (2011). *Coordinated Multi-Point in Mobile Communications: From Theory to Practice*, Cambridge University Press.

[4] **3GPP** (2017). Study on new radio access technology Physical layer aspects, **Technical report (TR) 38.802**, 3rd Generation Partnership Project (3GPP), Version 14.2.0, `https://www.3gpp.org/DynaReport/38802`.

[5] **Ma, K.**, **Wang, Z.**, **Tian, W.**, **Chen, S. and Hanzo, L.** (2021). Deep Learning for Beam Management: Opportunities, State-of-the-Arts and Challenges, *CoRR*, *abs/2111.11177*, `https://arxiv.org/abs/2111.11177`, `2111.11177`.

[6] **Shi, W.**, **Jiang, X.**, **Hu, J.**, **Teng, Y.**, **Wang, Y.**, **He, H.**, **Dong, R.**, **Shu, F. and Wang, J.** (2022). Physical layer security techniques for data transmission for future wireless networks, *Security and Safety*, *1*.

[7] **Boccardi, F.**, **Heath, R.W.**, **Lozano, A.**, **Marzetta, T.L. and Popovski, P.** (2014). Five disruptive technology directions for 5G, *IEEE Communications Magazine*, *52*(2), 74–80.

[8] **Heath, R.W.** (2019). Going Toward 6G [From the Editor], *IEEE Signal Processing Magazine*, *36*(3), 3–4.

[9] **Dang, S.**, **Amin, O.**, **Shihada, B. and Alouini, M.S.** (2019). From a Human-Centric Perspective: What Might 6G Be?, *ArXiv*, *abs/1906.00741*, `https://api.semanticscholar.org/CorpusID:173990810`.

[10] **Saad, W.**, **Bennis, M. and Chen, M.** (2020). A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems, *IEEE Network*, *34*(3), 134–142.

[11] **Bi, Q.** (2019). Ten Trends in the Cellular Industry and an Outlook on 6G, *IEEE Communications Magazine*, *57*(12), 31–36.

[12] **Gui, G.**, **Liu, M.**, **Tang, F.**, **Kato, N. and Adachi, F.** (2020). 6G: Opening New Horizons for Integration of Comfort, Security, and Intelligence, *IEEE Wireless Communications*, *27*(5), 126–132.

[13] **Letaief, K.B.**, **Chen, W.**, **Shi, Y.**, **Zhang, J. and Zhang, Y.J.A.** (2019). The Roadmap to 6G: AI Empowered Wireless Networks, *IEEE Communications Magazine*, *57*(8), 84–90.

[14] **Huang, T.**, **Yang, W.**, **Wu, J.**, **Ma, J.**, **Zhang, X. and Zhang, D.** (2019). A Survey on Green 6G Network: Architecture and Technologies, *IEEE Access*, *7*, 175758–175768.

[15] **David, K.**, **Elmirghani, J.**, **Haas, H. and You, X.H.** (2019). Defining 6G: Challenges and Opportunities [From the Guest Editors], *IEEE Vehicular Technology Magazine*, *14*(3), 14–16.

[16] **David, K. and Berndt, H.** (2018). 6G Vision and Requirements: Is There Any Need for Beyond 5G?, *IEEE Vehicular Technology Magazine*, *13*(3), 72–80.

[17] **Božanić, M. and Sinha, S.** (2021). *Mobile Communication Networks: 5G and a Vision of 6G*, Springer International Publishing, `https://link.springer.com/book/10.1007/978-3-030-69273-5`.

[18] **Tariq, F.**, **Khandaker, M.R.A.**, **Wong, K.K.**, **Imran, M.A.**, **Bennis, M. and Debbah, M.** (2020). A Speculative Study on 6G, *IEEE Wireless Communications*, *27*(4), 118–125.

[19] **Calvanese Strinati, E.**, **Barbarossa, S.**, **Gonzalez-Jimenez, J.L.**, **Ktenas, D.**, **Cassiau, N.**, **Maret, L. and Dehos, C.** (2019). 6G: The Next Frontier: From Holographic Messaging to Artificial Intelligence Using Subterahertz and Visible Light Communication, *IEEE Vehicular Technology Magazine*, *14*(3), 42–50.

[20] **Lu, L.**, **Li, G.Y.**, **Swindlehurst, A.L.**, **Ashikhmin, A. and Zhang, R.** (2014). An Overview of Massive MIMO: Benefits and Challenges, *IEEE Journal of Selected Topics in Signal Processing*, *8*(5), 742–758.

[21] **Rusek, F.**, **Persson, D.**, **Lau, B.K.**, **Larsson, E.G.**, **Marzetta, T.L.**, **Edfors, O. and Tufvesson, F.** (2013). Scaling Up MIMO: Opportunities and Challenges with Very Large Arrays, *IEEE Signal Processing Magazine*, *30*(1), 40–60.

[22] **Yang, S. and Hanzo, L.** (2015). Fifty Years of MIMO Detection: The Road to Large-Scale MIMOs, *IEEE Communications Surveys & Tutorials*, *17*(4), 1941–1988.

[23] **Björnson, E.**, **Sanguinetti, L.**, **Wymeersch, H.**, **Hoydis, J. and Marzetta, T.L.** (2019). Massive MIMO is a reality—What is next?: Five promising research directions for antenna arrays, *Digital Signal Processing*, *94*, 3–20, `https://www.sciencedirect.com/science/`

article/pii/S1051200419300776, special Issue on Source Localization in Massive MIMO.

[24] **Obeed, M.**, **Salhab, A.M.**, **Alouini, M.S. and Zummo, S.A.** (2019). On Optimizing VLC Networks for Downlink Multi-User Transmission: A Survey, *IEEE Communications Surveys & Tutorials*, *21*(3), 2947–2976.

[25] **Chen, C.**, **Zhong, W.D.**, **Yang, H. and Du, P.** (2018). On the Performance of MIMO-NOMA-Based Visible Light Communication Systems, *IEEE Photonics Technology Letters*, *30*(4), 307–310.

[26] **von Butovitsch, P.**, **Astely, D.**, **Furuskär, A.**, **Göransson, B.**, **Hogan, B.**, **Karlsson, J. and Larsson, E.** (2020). Advanced antenna systems for 5G networks, **White paper**, Ericsson, https://www.ericsson.com/en/reports-and-papers/white-papers/advanced-antenna-systems-for-5g-networks.

[27] **Yang, P.**, **Xiao, Y.**, **Xiao, M. and Li, S.** (2019). 6G Wireless Communications: Vision and Potential Techniques, *IEEE Network*, *33*(4), 70–75.

[28] **Ordóñez, L.G.**, **Palomar, D.P. and Fonollosa, J.R.** (2011). Fundamental diversity, multiplexing, and array gain tradeoff under different MIMO channel models, *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp.3252–3255.

[29] **Larsson, E.G.**, **Edfors, O.**, **Tufvesson, F. and Marzetta, T.L.** (2014). Massive MIMO for next generation wireless systems, *IEEE Communications Magazine*, *52*(2), 186–195.

[30] **Rappaport, T.**, **Heath, R.**, **Daniels, R. and Murdock, J.** (2015). *Millimeter Wave Wireless Communications*, Communications Engineering and Emerging Technology Series from Ted Rappaport Series, Prentice Hall.

[31] **Mattigiri, S. and Warty, C.** (2013). A study of fundamental limitations of small antennas: MIMO approach, *2013 IEEE Aerospace Conference*, pp.1–8.

[32] **Goldsmith, A.** (2005). *Wireless Communications*, Cambridge University Press.

[33] **Li, Q.**, **Li, G.**, **Lee, W.**, **Lee, M.i.**, **Mazzarese, D.**, **Clerckx, B. and Li, Z.** (2010). MIMO techniques in WiMAX and LTE: a feature overview, *IEEE Communications Magazine*, *48*(5), 86–92.

[34] **Kim, B.H. and Malladi, D.P.** (U.S. Patent US8271043B2, Sept. 2012). *Approach to a unified SU-MIMO/MU-MIMO operation*.

[35] **Osseiran, A.**, **Monserrat, J. and Mohr, W.** (2011). *Mobile and Wireless Communications for IMT-Advanced and Beyond*, Wiley.

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

https://www.sciencedirect.com/science/article/pii/S1389128617301950.

[37] **Singh, S.**, **Kumar, A.**, **Khurmi, S.S. and Singh, T.** (2012). Coordinated Multipoint (CoMP) Reception and Transmission for LTE-Advanced/4G, *International Journal of Computer Science and Technology*, *3*.

[38] **3GPP** (2023). Security architecture and procedures for 5G System, **Technical specification (TS) 33.501**, 3rd Generation Partnership Project (3GPP), Version 17.11.1, https://www.3gpp.org/DynaReport/33501.

[39] **3GPP** (2013). Coordinated multi-point operation for LTE with non-ideal backhaul, **Technical report (TR) 36.874**, 3rd Generation Partnership Project (3GPP), Version 12.0.0, https://www.3gpp.org/DynaReport/36874.

[40] **Solaija, M.S.J.**, **Salman, H.**, **Kihero, A.B.**, **Sağlam, M.I. and Arslan, H.** (2021). Generalized Coordinated Multipoint Framework for 5G and Beyond, *IEEE Access*, *9*, 72499–72515.

[41] **Hamamreh, J.M.**, **Furqan, H.M. and Arslan, H.** (2019). Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey, *IEEE Communications Surveys & Tutorials*, *21*(2), 1773–1828.

[42] **Wu, Y.**, **Khisti, A.**, **Xiao, C.**, **Caire, G.**, **Wong, K.K. and Gao, X.** (2018). A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead, *IEEE Journal on Selected Areas in Communications*, *36*(4), 679–695.

[43] **Grover, K.**, **Lim, A. and Yang, Q.** (2014). Jamming and Anti-Jamming Techniques in Wireless Networks: A Survey, *Int. J. Ad Hoc Ubiquitous Comput.*, *17*(4), 197–215.

[44] **Yılmaz, M.H. and Arslan, H.** (2015). A survey: Spoofing attacks in physical layer security, *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*, pp.812–817.

[45] **Wyner, A.D.** (1975). The wire-tap channel, *The Bell System Technical Journal*, *54*(8), 1355–1387.

[46] **Jameel, F.**, **Wyne, S.**, **Kaddoum, G. and Duong, T.Q.** (2019). A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security, *IEEE Communications Surveys & Tutorials*, *21*(3), 2734–2771.

[47] **Arslan, H. and Furqan, H.** (2023). *Physical Layer Security for Wireless Sensing and Communication*, IET security series, Institution of Engineering and Technology, https://digital-library.theiet.org/content/books/sc/pbse018e.

[48] **Zeng, K.** (2015). Physical layer key generation in wireless networks: challenges and opportunities, *IEEE Communications Magazine*, *53*(6), 33–39.

[49] **Wang, N.**, **Wang, P.**, **Alipour-Fanid, A.**, **Jiao, L. and Zeng, K.** (2019). Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities, *IEEE Internet of Things Journal*, *6*(5), 8169–8181.

[50] **Chen, R.**, **Li, C.**, **Yan, S.**, **Malaney, R. and Yuan, J.** (2019). Physical Layer Security for Ultra-Reliable and Low-Latency Communications, *IEEE Wireless Communications*, *26*(5), 6–11.

[51] **Damianou, A. and Lawrence, N.D.** (2013). Deep Gaussian Processes, ***C.M. Carvalho and P. Ravikumar**, editors, Proceedings of the Sixteenth International Conference on Artificial Intelligence and Statistics*, volume 31 of *Proceedings of Machine Learning Research*, PMLR, Scottsdale, Arizona, USA, pp.207–215.

[52] **Garnelo, M.**, **Schwarz, J.**, **Rosenbaum, D.**, **Viola, F.**, **Rezende, D.J.**, **Eslami, S.M.A. and Teh, Y.W.** (2018). *Neural Processes*, `1807.01622`.

[53] **Zhou, Z.H. and Feng, J.** (2017). Deep Forest: Towards An Alternative to Deep Neural Networks, *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, IJCAI-17*, pp.3553–3559, `https://doi.org/10.24963/ijcai.2017/497`.

[54] **Zhang, C.**, **Patras, P. and Haddadi, H.** (2019). Deep Learning in Mobile and Wireless Networking: A Survey, *IEEE Communications Surveys & Tutorials*, *21*(3), 2224–2287.

[55] **Arvinte, M.**, **Tavares, M. and Samardzija, D.** (2019). Beam Management in 5G NR using Geolocation Side Information, *2019 53rd Annual Conference on Information Sciences and Systems (CISS)*, pp.1–6.

[56] **Klautau, A.**, **Batista, P.**, **González-Prelcic, N.**, **Wang, Y. and Heath, R.W.** (2018). 5G MIMO Data for Machine Learning: Application to Beam-Selection Using Deep Learning, *2018 Information Theory and Applications Workshop (ITA)*, pp.1–9.

[57] **Araújo, D.C. and de Almeida, A.L.F.** (2019). Beam Management Solution Using Q-Learning Framework, *2019 IEEE 8th International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP)*, pp.594–598.

[58] **Polese, M.**, **Restuccia, F. and Melodia, T.** (2021). DeepBeam: Deep Waveform Learning for Coordination-Free Beam Management in MmWave Networks, *Proceedings of the Twenty-Second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, MobiHoc '21, Association for Computing Machinery, New York, NY, USA, p.61–70, `https://doi.org/10.1145/3466772.3467035`.

[59] **Cousik, T.S. and et. al.** (2021). Fast Initial Access with Deep Learning for Beam Prediction in 5G mmWave Networks, *MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM)*, pp.664–669.

[60] **Nguyen, K.N.**, **Ali, A.**, **Mo, J.**, **Ng, B.L.**, **Va, V. and Zhang, J.C.** (2022). *Beam Management with Orientation and RSRP using Deep Learning for Beyond 5G Systems*, `https://arxiv.org/abs/2202.02247`.

[61] **Alrabeiah, M. and Alkhateeb, A.** (2020). Deep Learning for mmWave Beam and Blockage Prediction Using Sub-6 GHz Channels, *IEEE Transactions on Communications*, *68*(9), 5504–5518.

[62] **Sim, M.S.**, **Lim, Y.G.**, **Park, S.H.**, **Dai, L. and Chae, C.B.** (2020). Deep Learning-Based mmWave Beam Selection for 5G NR/6G With Sub-6 GHz Channel Information: Algorithms and Prototype Validation, *IEEE Access*, *8*, 51634–51646.

[63] **Jagyasi, D. and Coupechoux, M.** (2021). DNN Based Beam Selection in mmW Heterogeneous Networks, ***S. Lasaulce, P. Mertikopoulos and A. Orda,*** *editors, Network Games, Control and Optimization*, Springer International Publishing, Cham, pp.172–184.

[64] **Chafaa, I.**, **Negrel, R.**, **Belmega, E.V. and Debbah, M.** (2022). Self-Supervised Deep Learning for mmWave Beam Steering Exploiting Sub-6 GHz Channels, *IEEE Transactions on Wireless Communications*, *21*(10), 8803–8816.

[65] **Heng, Y.**, **Mo, J. and Andrews, J.G.** (2022). Learning Site-Specific Probing Beams for Fast mmWave Beam Alignment, *IEEE Transactions on Wireless Communications*, *21*(8), 5785–5800.

[66] **Brilhante, D.d.S.**, **Manjarres, J.C.**, **Moreira, R.**, **de Oliveira Veiga, L.**, **de Rezende, J.F.**, **Müller, F.**, **Klautau, A.**, **Leonel Mendes, L. and P. de Figueiredo, F.A.** (2023). A Literature Survey on AI-Aided Beamforming and Beam Management for 5G and 6G Systems, *Sensors*, *23*(9), `https://www.mdpi.com/1424-8220/23/9/4359`.

[67] **Patel, Harshal** (2021). *Beam refinement and beam tracking using Machine Learning Techniques in 5G NR RAN*, Master thesis,Faculty of Computing, Blekinge Institute of Technology, Sweden.

[68] **Wang, Boqiang** (2021). *Adaptive Beam Management in 5G-NR: A Machine Learning Perspective*, Master thesis, Department of Electrical and Information Technology, Lund University, Sweden.

[69] **Kaya, A.O. and Viswanathan, H.** (2021). Deep Learning-based Predictive Beam Management for 5G mmWave Systems, *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pp.1–7.

[70] **Na, W.**, **Bae, B.**, **Cho, S. and Kim, N.** (2019). Deep-learning Based Adaptive Beam Management Technique for Mobile High-speed 5G mmWave Networks, *2019 IEEE 9th International Conference on Consumer Electronics (ICCE-Berlin)*, pp.149–151.

[71] **Aldalbahi, A.**, **Shahabi, F. and Jasim, M.** (2021). Instantaneous Beam Prediction Scheme against Link Blockage in mmWave Communications, *Applied Sciences*, *11*(12), `https://www.mdpi.com/2076-3417/11/12/5601`.

[72] **Siyad, C.I. and Tamilselvan, S.** (2020). Deep Learning Enabled Physical Layer Security to Combat Eavesdropping in Massive MIMO Networks, *2nd Int. Conf. on Comp. Nets. and Comm. Tech.*, pp.643–650.

[73] **Hoang, T.M.**, **Liu, D.**, **Luong, T.V.**, **Zhang, J. and Hanzo, L.** (2022). Deep Learning Aided Physical-Layer Security: The Security Versus Reliability Trade-Off, *IEEE Transactions on Cognitive Communications and Networking*, *8*(2), 442–453.

[74] **Mismar, F. and Evans, B.** (2019). Deep Learning in Downlink Coordinated Multipoint in New Radio Heterogeneous Networks, *IEEE Wireless Comm. Letters*, *8*, 1040–1043.

[75] **Schneider, S.**, **Karl, H.**, **Khalili, R. and Hecker, A.** (2023). Multi-Agent Deep Reinforcement Learning for Coordinated Multipoint in Mobile Networks, *IEEE Tran. on Network and Service Management*, 1–1.

[76] **Özmat, U.**, **Demirkol, M.F.**, **Demirci, N. and Yazıcı, M.A.** (2020). Enhancing Physical Layer Security with Coordinated Multi-Point Transmission in 5G and Beyond Networks, *2020 28th Signal Processing and Communications Applications Conference (SIU)*, pp.1–4.

[77] **Ozmat, U.**, **Demirkol, M.F. and Yazici, M.A.** (2020). Service-Based Coverage for Physical Layer Security with Multi-Point Coordinated Beamforming, *2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pp.1–6.

[78] **Ozmat, U.**, **Yazici, M.A. and Demirkol, M.F.** (2024). Secure Initial Access and Beam Alignment Using Deep Learning in 5G and Beyond Systems, *IEEE Access*, *12*, 46–59.

[79] **Ozmat, U.**, **Yazici, M.A. and Demirkol, M.F.** (2023). Secure Multi-Point Coordinated Beamforming using Deep Learning in 5G and Beyond Networks, *2023 IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (IEEE CAMAD 2023)*, Edinburgh, United Kingdom (Great Britain), p. 6.

[80] **Giordani, M.**, **Polese, M.**, **Roy, A.**, **Castor, D. and Zorzi, M.** (2019). A Tutorial on Beam Management for 3GPP NR at mmWave Frequencies, *IEEE Communications Surveys & Tutorials*, *21*(1), 173–196.

[81] **3GPP** (2023). NR; Physical channels and modulation, **Technical specification (TS) 38.211**, 3rd Generation Partnership Project (3GPP), Version 17.6.0, https://www.3gpp.org/DynaReport/38211.

[82] **3GPP** (2023). NR; Physical layer procedures for control, **Technical specification (TS) 38.211**, 3rd Generation Partnership Project (3GPP), Version 17.7.0, https://www.3gpp.org/DynaReport/38213.

[83] **3GPP** (2023). NR; Physical layer procedures for data, **Technical specification (TS) 38.214**, 3rd Generation Partnership Project (3GPP), Version 17.7.0, https://www.3gpp.org/DynaReport/38214.

[84] **3GPP** (2023). NR; Medium Access Control (MAC) protocol specification, **Technical specification (TS) 38.215**, 3rd Generation Partnership Project (3GPP), Version 17.6.0, https://www.3gpp.org/DynaReport/38321.

[85] **3GPP** (2023). NR; NR and NG-RAN Overall description; Stage-2, **Technical report (TR) 38.300**, 3rd Generation Partnership Project (3GPP), Version 17.6.0, https://www.3gpp.org/DynaReport/38300.

[86] **3GPP** (2023). NR; Physical layer measurements, **Technical specification (TS) 38.215**, 3rd Generation Partnership Project (3GPP), Version 17.3.0, https://www.3gpp.org/DynaReport/38215.

[87] **3GPP** (2022). Study on New Radio (NR) access technology, **Technical report (TR) 38.912**, 3rd Generation Partnership Project (3GPP), Version 17.0.0, https://www.3gpp.org/DynaReport/38912.

[88] **Li, Y.N.R.**, **Gao, B.**, **Zhang, X. and Huang, K.** (2020). Beam Management in Millimeter-Wave Communications for 5G and Beyond, *IEEE Access*, *8*, 13282–13293.

[89] **3GPP** (2023). NR; Radio Resource Control (RRC); Protocol specification, **Technical specification (TS) 38.215**, 3rd Generation Partnership Project (3GPP), Version 17.6.0, https://www.3gpp.org/DynaReport/38331.

[90] **Giordani, M.**, **Mezzavilla, M. and Zorzi, M.** (2016). Initial Access in 5G mmWave Cellular Networks, *IEEE Communications Magazine*, *54*(11), 40–47.

[91] **Attaoui, W.**, **Bouraqia, K. and Sabir, E.** (2022). Initial Access & Beam Alignment for mmWave and Terahertz Communications, *IEEE Access*, *10*, 35363–35397.

[92] **Giordani, M.**, **Mezzavilla, M.**, **Barati, C.N.**, **Rangan, S. and Zorzi, M.** (2016). Comparative analysis of initial access techniques in 5G mmWave cellular networks, *2016 Annual Conference on Information Science and Systems (CISS)*, pp.268–273.

[93] **Kamboj, A.K.**, **Jindal, P. and Verma, P.** (2021). Machine learning-based physical layer security: techniques, open challenges, and applications, *Wireless Networks*, *8*, 5351–5383.

[94] **3GPP** (2022). NR; Requirements for support of radio resource management, **Technical specification (TS) 38.133**, 3rd Generation Partnership Project (3GPP), Version 17.7.0, https://www.3gpp.org/DynaReport/38133.

[95] The MathWorks Inc., Natick, Massachusetts, United State, (2023). 5G Toolbox version: 2.6 (R2023a), https://www.mathworks.com/help/5g/.

[96] **GUPTA, P. and SINHA, N.K.**, (2000). CHAPTER 14 - Neural Networks for Identification of Nonlinear Systems: An Overview, **N.K. SINHA and M.M. GUPTA**, editors, Soft Computing and Intelligent Systems, Academic Press Series in Engineering, Academic Press, San Diego, pp.337–356, https://www.sciencedirect.com/science/article/pii/B9780126464900500172.

[97] **Yang, L. and Shami, A.** (2020). On hyperparameter optimization of machine learning algorithms: Theory and practice, *Neurocomputing*, *415*, 295–316, https://www.sciencedirect.com/science/article/pii/S0925231220311693.

[98] **Kingma, D. and Ba, J.** (2014). Adam: A Method for Stochastic Optimization, *International Conference on Learning Representations*.

[99] **Robert, C.** (2014). Machine Learning, a Probabilistic Perspective, *CHANCE*, *27*(2), 62–63.

[100] **Rudd, R. and Kirtay, S.** (2021). Coverage thresholds for 5G services, **Commission for communications regulation consultants report**, Plum Consulting London LLP, London, UK, Report no: 21/118a, https://www.comreg.ie/media/2021/11/ComReg-21118a.pdf.

CURRICULUM VITAE

Name SURNAME: Utku ÖZMAT

EDUCATION:

- **B.Sc.:** 2012, Istanbul University, Engineering Faculty, Electrical and Electronics Engineering Department
- **M.Sc.:** 2016, Istanbul Technical University, Department of Electronics and Communication Engineering, Telecommunications Engineering Programme
- **Ph.D.:** 2024, Istanbul Technical University, Department of Applied Informatics, Cybersecurity Engineering and Cryptography Programme

PROFESSIONAL EXPERIENCE AND REWARDS:

- **2021- :** 5G Program Management Expert, Turk Telekom, Istanbul/Türkiye.
- **2019-2021:** Senior R&D Engineer, ULAK Communication Inc., Istanbul/Türkiye.
- **2018-2019:** Senior R&D Engineer, Huawei, Istanbul/Türkiye.
- **2015-2018:** Global Product Support Engineer, NETAŞ, Istanbul/Türkiye.
- **2013-2015:** Research Assistant, Istanbul Gedik University, Engineering Faculty, Electrical and Electronics Engineering Department, Istanbul/Türkiye.

PUBLICATIONS, PRESENTATIONS AND PATENTS ON THE THESIS:

- **Ozmat U.**, Yazıcı M. A., and Demirkol M. F., "Secure Initial Access and Beam Alignment using Deep Learning in 5G and Beyond Systems," in *IEEE Access*, vol. 12, pp. 46-59, 2024, doi: 10.1109/ACCESS.2023.3347502.
- **Ozmat U.**, Yazıcı M. A., and Demirkol M. F., "Secure Multi-Point Coordinated Beamforming using Deep Learning in 5G and Beyond Networks," *2023 IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Edinburgh, UK, 2023, pp.1-6.
- **Ozmat U.**, Demirkol M. F., and Yazıcı M. A., "Service-Based Coverage for Physical Layer Security with Multi-Point Coordinated Beamforming," *2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Pisa, Italy, 2020, pp. 1-6.

- **Özmat U.**, Demirkol M. F., Demirci N. and Yazıcı M. A., "Enhancing Physical Layer Security with Coordinated Multi-Point Transmission in 5G and Beyond Networks," *2020 28th Signal Processing and Communications Applications Conference (SIU)*, Gaziantep, Turkey, 2020, pp. 1-4.

OTHER PUBLICATIONS, PRESENTATIONS AND PATENTS:

- **Ozmat U.**, Ulgen O. and Gunaydin E., "Bit Error Rate Analysis of Non-Orthogonal Multiple Access (NOMA) Technique in 5G with Different Power and User Scenarios," *2018 Advances in Wireless and Optical Communications (RTUWO)*, Riga, Latvia, 2018, pp. 45-49.
- Ulgen O., **Ozmat U.**, and Gunaydin E., "Hybrid Implementation of Millimeter Wave and Visible Light Communications for 5G Networks," *2018 26th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, 2018, pp. 1-4.