Universidade Politécnica
Castelo Branco
Escola Superior de Tecnologia

Estudo Experimental de Redes 5G NR com OpenAirInterface (OAI)

Chelsea Africana M. Coimbra

Disengomoka M. Manuel Buengo

Orientador / Co-Orientador

Professor Doutor Hugo Rafael de Almeida e Marques

Professor Doutor Paulo Jorge Coelho Marques

Relatório do Projeto de final de curso/ apresentado à Escola Superior de Tecnologia da Universidade Politécnica de Castelo Branco para cumprimento dos requisitos necessários à obtenção do grau de Licenciado em Engenharia Eletrotécnica e das Telecomunicações, realizado sob a orientação científica do Professor Doutor Hugo Rafael de Almeida e Marques e do Professor Doutor Paulo Jorge Coelho Marques, da Universidade Politécnica de Castelo Branco.

Setembro 2026

Composição do júri

Presidente do júri

Doutor, José António Barros Vieira

Professor Adjunto da Unidade Técnico-Científica de Engenharia Eletrotécnica e Industrial.

Arguente

Doutor, Rogério Pais Dionísio

Professor Coordenador da Unidade Técnico-Científica de Engenharia Eletrotécnica e Industrial.

Orientador

Doutor, Hugo Rafael de Almeida e Marques

Professor Adjunto da Unidade Técnico-Científica de Engenharia Eletrotécnica e Industrial.

Co-Orientador

Doutor, Paulo Jorge Coelho Marques

Professor Adjunto da Unidade Técnico-Científica de Engenharia Eletrotécnica e Industrial.

Dedicatória

Dedicamos este trabalho aos nossos pais e irmãos, que sempre confiaram em nós e nos deram a oportunidade de estudar em Portugal, longe de casa. Apesar das dificuldades, nunca deixaram de acreditar em nós, e é por isso que aqui chegámos.

Agradecimentos

Aos nossos familiares, e a todos os que participaram neste processo de formação, com apoio financeiro e moral.

Aos docentes que nos acolheram e formaram ao longo deste percurso.

Ao nosso orientador, Professor Doutor Hugo Marques, e ao coorientador, Paulo Marques, pela orientação científica e acompanhamento dedicados a este trabalho.

À empresa Allbesmart, Lda., pelo apoio técnico e meios disponibilizados para a concretização deste projeto.

Aos nossos colegas, pelo companheirismo ao longo deste percurso académico.

Resumo

Este trabalho consiste no estudo experimental de uma rede 5G NR *Standalone*, implementada na plataforma OAIBOX™ (desenvolvida pela empresa Allbesmart, Lda.), utilizando a implementação de código aberto *OpenAirInterface*. Após a análise teórica da arquitetura do sistema, do núcleo de rede e dos mecanismos de segurança definidos pelo 3GPP, realizou-se um conjunto de ensaios laboratoriais que avaliaram o impacto de diferentes configurações da interface rádio (largura de banda, banda de frequência, TDD, FDD, modulação e MIMO) no desempenho da ligação, através da análise de KPIs (CQI, RSRP, RSRQ, SINR, BLER, RI e MCS) e da respetiva comparação com os modelos teóricos. Recorreu-se ainda à Inspeção Profunda de Pacotes para analisar o registo do UE e os mecanismos de segurança, explorou-se o *network slicing* através da criação de *slices* dedicadas, e testou-se a alteração do PLMN de uma rede privada, incluindo a reprogramação do cartão SIM. Os resultados validam experimentalmente os principais procedimentos do 5G NR e confirmam o potencial da OAIBOX™ como plataforma de ensino e investigação.

A realização deste projeto constituiu o primeiro contacto prático da equipa com redes 5G, nomeadamente com o ambiente Linux e com comandos AT, o que tornou o processo inicialmente exigente. Não obstante, a existência de normas bem estabelecidas e o apoio do material disponibilizado contribuíram para uma abordagem mais estruturada ao longo do trabalho. Este contacto direto permitiu ainda consolidar diversos conceitos de telecomunicações até então abordados apenas ao nível teórico durante o percurso académico, evidenciando se, em particular, a utilidade do Wireshark na análise do tráfego e dos mecanismos de segurança. Os valores obtidos em ambiente laboratorial confirmaram, dentro das margens expectáveis para o ambiente de propagação considerado, os modelos teóricos estudados.

A implementação de uma rede 5G completa com recurso a código aberto reduz significativamente os custos habitualmente associados ao equipamento de fabricantes comerciais, de arquitetura proprietária e fechada, inserindo este trabalho num conjunto mais alargado de iniciativas que promovem a utilização de código aberto em redes móveis. Esta redução de custos permite a estudantes e investigadores experimentar, em ambiente laboratorial, procedimentos de uma rede móvel de nova geração, neste caso o 5G, que de outro modo permaneceriam confinados à teoria.

Palavras chave

3GPP, 5G NR, OpenAirInterface, OAIBOX™, segurança 5G, network slicing.

Abstract

This work presents an experimental study of a 5G NR Standalone network, implemented on the OAIBOX™ platform (developed by Allbesmart, Lda.), using the OpenAirInterface open-source implementation. Following a theoretical characterisation of the system architecture, core network, and 3GPP security mechanisms, a set of laboratory tests assessed the impact of different radio interface configurations (bandwidth, frequency band, TDD, FDD, modulation, and MIMO) on link performance, through the analysis of KPIs (CQI, RSRP, RSRQ, SINR, BLER, RI, and MCS) and their comparison against theoretical models. Deep Packet Inspection was used to analyse UE registration and security mechanisms, network slicing was explored through dedicated slice configuration, and PLMN reconfiguration of a private network was tested, including SIM card reprogramming. The results validate the main 5G NR procedures and confirm the OAIBOX™'s potential as a teaching and research platform.

Carrying out this project constituted the team's first practical contact with 5G networks, namely with the Linux environment and AT commands, which initially made the process demanding. Nonetheless, the existence of well-established standards and the support of the available material contributed to a more structured approach throughout the work. This hands-on contact also allowed several telecommunications concepts, previously addressed only at a theoretical level during the academic path, to be consolidated, with particular emphasis on the usefulness of Wireshark in traffic and security mechanism analysis. The values obtained in the laboratory confirmed, within the margins expected for the propagation environment considered, the theoretical models studied.

Implementing a complete 5G network using open-source code significantly reduces the costs usually associated with equipment from commercial manufacturers, based on proprietary and closed architectures, placing this work within a broader set of initiatives that promote the use of open-source solutions in mobile networks. This cost reduction allows students and researchers to experiment, in a laboratory environment, with procedures of a next-generation mobile network, in this case 5G, which would otherwise remain confined to theory.

Keywords

3GPP, 5G NR, OpenAirInterface, OAIBOX™, segurança 5G, network slicing.

Índice geral

Composição do júri III
Dedicatória V
Agradecimentos VII
Resumo IX
Abstract XI
Índice geral XIII
Índice de figuras XIX
Índice de símbolos XXIII
Lista de tabelas XXV
Lista de abreviaturas, siglas e acrónimos XXVIII
1 Introdução 1
1.1 Enquadramento 1
1.2 Motivação e Problema 2
1.3 Objetivos 2
1.4 A Plataforma OAIBOX™ 3
1.5 Requisitos Técnicos do 5G NR (IMT-2020) 4
1.6 Especificações Normativas 3GPP Relevantes para o 5G NR 4
2 Fundamentos da Arquitetura do Sistema 5G NR 5
2.1 Arquitetura do Sistema 5G NR 5
2.2 Rede de Acesso Rádio (RAN) 6
2.2.1 Next Generation Node B (gNB) 7
2.2.2 Interface Rádio NR 7
2.2.3 Técnicas de transmissão da interface rádio 9
2.2.4 Bandas de Frequência do 5G NR 10
2.2.5 Modos de configuração e cenários de aplicação do gNB 10
2.3 Core da Rede 5G (CN5G) 12
2.3.1 Principais funções do 5G Core 12
2.3.2 Network Slicing 13
2.4 Arquitetura Protocolar do Sistema 5G NR 14
2.5 Interfaces do 5G Core 16
2.6 Procedimentos de acesso ao CN5G 16
2.6.1 Estabelecimento da ligação do gNB ao CN5G 17
2.6.2 Procedimento de registo e autenticação do UE 17
2.6.3 Procedimento de estabelecimento da sessão PDU 18

2.7 Segurança na Rede 5G NR 19
2.7.1 Arquitetura de Segurança 19
2.7.2 Funções de hash 19
2.7.3 MAC e assinatura digital 19
2.7.4 Privacidade 20
2.7.5 Procedimento Integrado de Identificação e Autenticação do UE 23
2.7.6 Gestão e Hierarquia de Chaves 24
2.8 Indicadores de Desempenho (KPI) em Redes 5G NR 26
2.8.1 Definição dos Principais KPI Rádio 26
2.8.2 Modelos de propagação e cálculo teórico dos KPI 28
2.8.3 Classificação Qualitativa dos KPI 31
3 Experimentação laboratorial 32
3.1 Descrição do ambiente de experimentação utilizado 32
3.2 Ferramentas de Medição e Análise 34
3.3 Análise do impacto da largura de banda no desempenho da ligação 5G NR 34
3.3.1 Cálculos teóricos 35
3.4 Análise do impacto da banda de frequência e do cenário de propagação no desempenho da ligação 5G NR 37
3.4.1 Cálculos teóricos 39
3.5 Análise do impacto da configuração TDD no desempenho da ligação 5G NR 41
3.5.1 Cálculos teóricos 43
3.6 Análise do desempenho da ligação 5G NR em modo FDD 43
3.6.1 Cálculos teóricos 45
3.7 Análise do impacto do esquema de modulação e codificação no desempenho da ligação 5G NR 45
3.7.1 QPSK 45
3.7.2 16QAM 46
3.7.3 64QAM 48
3.7.4 256QAM 49
3.7.5 Cálculos teóricos 50
3.8 Testar configurações MIMO do 5G NR 51
3.8.1 SISO 1x1 51
3.8.2 MIMO 2x2 53
3.8.3 Resultados e discussão 54
3.8.4 Cálculos teóricos 55

3.9 Inspeção Profunda de Pacotes para melhor compreensão do 5G NR 55
3.9.1 Procedimento NG Setup 56
3.9.2 Encapsulamento de pacotes ICMP entre interfaces 5G NR 56
3.9.3 Registo do gNB na AMF 58
3.9.4 Interfaces atravessadas pelo tráfego de utilizador 58
3.9.5 Relação entre a topologia e os pacotes observados 59
3.9.6 TTL constante entre Uu e N3 59
3.9.7 Diagrama de encapsulamento do Echo Request 59
3.9.8 Presença do cabeçalho SDAP 60
3.9.9 Medição da latência entre interfaces 60
3.10 Compreender a Segurança no 5G NR 61
3.10.1 Algoritmos de segurança configurados 61
3.10.2 Procedimento de segurança NAS 62
3.10.3 Procedimento de autenticação (5G-AKA) 62
3.10.4 Procedimento de segurança AS 65
3.10.5 Proteção da mensagem NAS do UE até à SMF 67
3.10.6 Proteção do plano de utilizador 69
3.10.7 Interfaces de comunicação do UE 73
3.10.8 Correspondência com os mecanismos teóricos de segurança 73
3.10.9 Cifra simétrica ou assimétrica 74
3.11 Uso de Network Slicing em 5G usando uma xApp 74
3.11.1 Configuração da slice URLLC 74
3.11.2 Medição de desempenho da slice eMBB 75
3.11.3 Estabelecimento da sessão PDU na slice URLLC 76
3.11.4 Medição de desempenho da slice URLLC 78
3.11.5 Efeito da variação de PRBs no throughput 78
3.12 Configuração de PLMN e programação de cartões SIM 5G 79
3.12.1 Alteração do PLMN na configuração do gNB 79
3.12.2 Alteração do PLMN na configuração do CN5G 80
3.12.3 Atualização da base de dados do CN5G 81
3.12.4 Verificação e reprogramação do cartão SIM 82
3.12.5 Configuração final do modem e confirmação da ligação 84
3.13 Análise dos resultados obtidos 85
4 Conclusão 86
5 REFERÊNCIAS 87

Índice de figuras

Figura 2-1: Arquitetura de uma rede 5G [23] 6
Figura 2-2: Estrutura temporal da interface rádio NR 9
Figura 2-3: Arquitetura do Core da rede 5G (CN5G) [25] 12
Figura 2-4: Arquitetura protocolar do sistema 5G NR [25] 15
Figura 2-5: Diagrama simplificado do procedimento NG Setup entre o gNB e o CN5G 17
Figura 2-6: Diagrama simplificado do procedimento de registo e autenticação do UE18
Figura 2-7: Diagrama simplificado do procedimento de estabelecimento da Sessão PDU 19
Figura 2-8: Diagrama simplificado da transição entre o SUPI, o SUCI e o GUTI durante o procedimento de registo do UE.....20
Figura 2-9: Diagrama simplificado do fluxo de identificação e autenticação do UE.....24
Figura 3-1: Ambiente experimental utilizado para a realização dos ensaios 33
Figura 3-2: Evolução temporal dos KPIs (CQI, RSRP, RSRQ, SINR, BLER e taxa de transmissão) para uma largura de banda de 20 MHz.....34
Figura 3-3: Evolução temporal dos KPIs (CQI, RSRP, RSRQ, SINR, BLER e taxa de transmissão) para uma largura de banda de 40 MHz.....34
Figura 3-4: Evolução temporal dos KPIs para a banda n77 LoS.....37
Figura 3-5: Evolução temporal dos KPIs para a banda n78 LoS.....37
Figura 3-6: Evolução temporal dos KPIs para a banda n77 NLoS 38
Figura 3-7: Evolução temporal dos KPIs para a banda n78 NLoS 38
Figura 3-8: KPIs medidos para a configuração DDDFU (20 MHz) 41
Figura 3-9: KPIs medidos para a configuração DDDFU (40 MHz) 41
Figura 3-10: KPIs medidos para a configuração DDFUU (20 MHz) 42
Figura 3-11: KPIs medidos para a configuração DDFUU (40 MHz) 42
Figura 3-12: KPIs medidos em modo FDD (20 MHz).....44
Figura 3-13: KPIs medidos em modo FDD (40 MHz).....44
Figura 3-14: Evolução do bitrate para modulação QPSK em condição LoS 45
Figura 3-15: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação QPSK em condição LoS 46
Figura 3-16: Evolução do bitrate para modulação QPSK em condição NLoS.....46
Figura 3-17: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação QPSK em condição NLoS 46
Figura 3-18: Evolução do bitrate para modulação 16QAM em condição LoS 47
Figura 3-19: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação 16QAM em condição LoS.....47
Figura 3-20: Evolução do bitrate para modulação 16QAM em condição NLoS.....47
Figura 3-21: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação 16QAM em condição NLoS 47
Figura 3-22: Evolução do bitrate para modulação 64QAM em condição LoS 48
Figura 3-23: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação 64QAM em condição LoS.....48
Figura 3-24: Evolução do bitrate para modulação 64QAM em condição NLoS.....48
Figura 3-25: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação 64QAM em condição NLoS 48
Figura 3-26: Evolução do bitrate para modulação 256QAM em condição LoS 49

Figura 3-27: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação 256QAM em condição LoS 49
Figura 3-28: Evolução do bitrate para modulação 256QAM em condição NLoS 49
Figura 3-29: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação 256QAM em condição NLoS 50
Figura 3-30: Evolução do bitrate para SISO (1x1) em condição LoS 51
Figura 3-31: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para SISO (1x1) em condição LoS 52
Figura 3-32: Evolução do bitrate para SISO (1x1) em condição NLoS 52
Figura 3-33: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para SISO (1x1) em condição NLoS 52
Figura 3-34: Evolução do bitrate para MIMO (2x2) em condição LoS 53
Figura 3-35: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para MIMO (2x2) em condição LoS 53
Figura 3-36: Evolução do bitrate para MIMO (2x2) em condição NLoS 53
Figura 3-37: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para MIMO (2x2) em condição NLoS 54
Figura 3-38: Pacotes do procedimento NG Setup (NGSetupRequest e NGSetupResponse) e detalhe dos campos do NGSetupRequest 56
Figura 3-39: Pacotes na interface Uu e camadas MAC-NR/RLC-NR/PDCP-NR/SDAP do pacote ICMP *Echo Request* 57
Figura 3-40: Pacote ICMP *Echo Request* na interface Uu 57
Figura 3-41: Pacotes ICMP nas interfaces N3 e N6, evidenciando a tradução do endereço de origem (NAT) pelo UPF 58
Figura 3-42: Diagrama do encapsulamento do pacote ICMP nas interfaces Uu, N3 e N6 59
Figura 3-43: Lista de pacotes ICMP nas interfaces Uu, N3 e N6, evidenciando o campo Time para cálculo da latência 60
Figura 3-44: config.yaml, algoritmos de integridade e cifra suportados pela AMF 61
Figura 3-45: dashboard do gNB, configuração por omissão 62
Figura 3-46: InitialUEMessage/Registration Request, campos 5GS mobile identity e UE Security Capability 62
Figura 3-47: Authentication request, campos RAND e AUTN 63
Figura 3-48: Authentication response, campo RES* 63
Figura 3-49: NAS Security Mode Command, algoritmos selecionados e Message Authentication Code 64
Figura 3-50: NAS Security Mode Command, capacidades de segurança do UE reenviadas pela rede (Replayed UE security capabilities) 64
Figura 3-51: NAS Security Mode Complete, confirmação de cifra e integridade 65
Figura 3-52: InitialContextSetupRequest, campos GUAMI e SecurityKey 65
Figura 3-53: AS Security Mode Command, securityAlgorithmConfig e MAC 66
Figura 3-54: RRC Reconfiguration, pdcp-Config da DRB (ausência de cipheringDisabled/integrityProtection) 67
Figura 3-55: Security header type e payload container da mensagem UL NAS Transport, interface N2 68
Figura 3-56: Parâmetros JSON do reencaminhamento à SMF, interface N11 68
Figura 3-57: Conteúdo NAS-SM em claro reencaminhado à SMF 68
Figura 3-58: PDCP-NR, pacote Downlink (SN=150951) 70

Figura 3-59: PDCP-NR, pacote Uplink (SN=50864) 70
Figura 3-60: dashboard do gNB, integridade ativada....70
Figura 3-61: PDCP-NR, pacote Downlink (SN=2314), campo Data com 65 bytes....71
Figura 3-62: PDCP-NR, pacote Uplink (SN=2022), campo Data com 65 bytes 71
Figura 3-63: Dashboard do gNB, cifra restrita a NEA2 72
Figura 3-64: PDCP-NR, pacote Downlink (SN=5587), payload cifrado....72
Figura 3-65: PDCP-NR, pacote Uplink (SN=4067), payload cifrado 73
Figura 3-66: Slice Configuration, criação da slice URLLC (SST 2, Start PRB 82, 24 PRBs) 75
Figura 3-67: Network Slicing, slices eMBB e URLLC configuradas 75
Figura 3-68: Bitrate, teste de velocidade na slice eMBB....75
Figura 3-69: OpenSpeedTest, resumo do teste de velocidade na slice eMBB....76
Figura 3-70: PuTTY, confirmação dos dois contextos PDP configurados (eMBB e URLLC)....76
Figura 3-71: Wireshark, pedido de sessão PDU com S-NSSAI URLLC (SST 2) e DNN oai.urllc 77
Figura 3-72: Wireshark, resposta da rede com o endereço IP atribuído na subnet da URLLC....77
Figura 3-73: Bitrate, evolução do teste de velocidade na slice URLLC....78
Figura 3-74: OpenSpeedTest, resumo do teste de velocidade na slice URLLC....78
Figura 3-75: Bitrate, efeito da variação de PRBs da slice URLLC no throughput....79
Figura 3-76: Programador de cartões SIM 5G e cartão SIM....79
Figura 3-77: OAIBOX™.yaml, campo plmn_list alterado para MCC 999 e MNC 99 ...80
Figura 3-78: Dashboard, NGSetupFailure após alteração do PLMN no gNB....80
Figura 3-79: config.yaml, served_guami_list e plmn_support_list da AMF, MCC 999 e MNC 99 81
Figura 3-80: nssf_slice_config.yaml, taInfoList e supportedSnssaiList da NSSF 81
Figura 3-81: oai_db.sql, variável @plmn configurada para 99999 82
Figura 3-82: Dashboard, NGSetupRequest e NGSetupResponse após correção do PLMN 82
Figura 3-83: PuTTY, estado do SIM antes da reprogramação....83
Figura 3-84: Terminal, reprogramação do SIM via program_uicc 83
Figura 3-85: PuTTY, AT+COPS=? após reprogramação....84
Figura 3-86: PuTTY, confirmação da célula servidora após reprogramação do SIM ..84

Índice de símbolos

BW	Largura de banda ocupada (Hz)
b_i	Número de bits do bloco de transporte i
C	Capacidade teórica de Shannon (bit/s)
d	Distância entre o gNB e o UE (m)
D_RB,slot	Volume de dados transportado por bloco de recurso por slot (bits)
EIRP_RE,dBm	Potência irradiada por elemento de recurso (dBm)
EIRP_total,dBm	Potência total irradiada (dBm)
f_c,GHz	Frequência central da portadora (GHz)
G_gNB,dB	Ganho de antena do gNB (dB)
G_UE,dB	Ganho de antena do UE (dB)
I	Potência da interferência de outros sinais (W)
L_cabo,dB	Perdas de cabo (dB)
M	Número de bits por símbolo da modulação
N	Potência do ruído (W)
NF_dB	Figura de ruído do recetor (dB)
N_RB	Número de blocos de recurso da largura de banda utilizada
N_RE	Número de elementos de recurso que contêm o sinal de referência
N_layers	Número de camadas espaciais (rank) da transmissão
N_scRB	Número de subportadoras por bloco de recurso (RB = 12)
N_slots,dir	Número de slots por segundo atribuídos a uma direção (DL/UL)
N_symb	Número de símbolos OFDM usados na medição
N_TB	Número total de blocos de transporte transmitidos
N_TB,err	Número de blocos de transporte recebidos com erro
PathLoss_Friis,dB	Perda de percurso, modelo de espaço livre (Friis) (dB)
PathLoss_UMa,dB	Perda de percurso, modelo Urban Macro (UMa) (dB)
PenetrationLoss_dB	Perda adicional por obstrução (dB)

P_N,dBm	Potência de ruído térmico (dBm)
P_TX,dBm	Potência de transmissão do gNB (dBm)
R	Taxa de codificação
RxS	Sensibilidade do recetor (dBm)
RxSL	Nível de sinal recebido em downlink (dBm)
S	Potência do sinal útil (W)
SE	Eficiência espectral teórica (bit/s/Hz)
s_l,r,k	Sinal recebido no símbolo OFDM l, bloco de recurso r e subportadora k
SNR	Relação sinal-ruído alvo, sem interferência (dB)
ΔT	Intervalo de tempo de transferência (s)

Lista de tabelas

Tabela 1:1 Evolução das gerações de redes móveis 1
Tabela 1:2 Plataformas 5G de código aberto mais relevantes 2
Tabela 1:3 Requisitos técnicos definidos pela especificação IMT-2020 4
Tabela 1:4 Séries normativas 3GPP principais e respetivo domínio funcional 4
Tabela 2:1 Comparação entre as arquiteturas 5G NSA e SA 5
Tabela 2:2 Parâmetros por numerologia (μ) 8
Tabela 2:3 Número máximo de blocos de recursos por largura de banda (μ=1, SCS=30 kHz) 8
Tabela 2:4 Numerologia e espaçamento entre subportadoras (SCS) na interface rádio NR 9
Tabela 2:5 Gamas de frequência do 5G NR (FR1 e FR2) 10
Tabela 2:6 Principais funções de rede do 5G Core 13
Tabela 2:7 Classificação e especificações técnicas 3GPP da arquitetura protocolar 15
Tabela 2:8 Principais interfaces do sistema 5G 16
Tabela 2:9 Esquemas de proteção do SUCI 22
Tabela 2:10 Comparação entre SUPI, SUCI e GUTI 23
Tabela 2:11 Principais KPI rádio utilizados na avaliação experimental. 26
Tabela 2:12 Escala qualitativa de classificação dos KPI rádio. 31
Tabela 3:1 Especificações técnicas dos equipamentos utilizados 33
Tabela 3:2 Ferramentas de medição e análise utilizadas 34
Tabela 3:3 RSRP teórico e desvio face ao valor medido 35
Tabela 3:4 Bitrate teórico (por alocação de slots TDD) e bitrate máximo medido, por direção 36
Tabela 3:5 Resumo dos KPIs medidos por banda e cenário de propagação 39
Tabela 3:6 RSRP teórico e desvio face ao valor medido 39
Tabela 3:7 SINR teórico e comparação com o valor medido 40
Tabela 3:8 Capacidade de Shannon e bitrate máximo medido 40
Tabela 3:9 Resumo de bitrate medido por configuração TDD 42
Tabela 3:10 Bitrate teórico e desvio face ao valor medido, por configuração TDD 43
Tabela 3:11 Resumo dos KPIs e do bitrate medidos em modo FDD 44
Tabela 3:12 Capacidade de Shannon e bitrate máximo medido, modo FDD 45
Tabela 3:13 RSRP, RSRQ, SINR, CQI, BLER, MCS e bitrate medidos, por ordem de modulação e cenário de propagação 50
Tabela 3:14 Eficiência espectral teórica e medida, por ordem de modulação e cenário de propagação 51
Tabela 3:15 Bitrate DL e UL medido e Rank Indicator, por configuração de antena e cenário de propagação 54
Tabela 3:16 Capacidade de Shannon e bitrate de downlink medido, por configuração de antena 55
Tabela 3:17 Interfaces observadas no encapsulamento do *Echo Request* e evolução do TTL 58
Tabela 3:18 Latência acumulada entre interfaces (Echo Request/Reply) 60
Tabela 3:19 InitialContextSetupRequest, campos GUAMI e SecurityKey 66
Tabela 3:20 Resumo da proteção observada no plano de utilizador, por configuração 73
Tabela 3:21 Condições de alocação de PRBs testadas 78

Lista de abreviaturas, siglas e acrónimos

AES-CMAC	*Advanced Encryption Standard – Cipher-based Message Authentication Code*
5G-AKA	*5G Authentication and Key Agreement*
AMF	*Access and Mobility Management Function*
AS	*Access Stratum*
AUSF	*Authentication Server Function*
BS	*Base Station*
BLER	*Block Error Rate*
CN	*Core Network*
CN5G	*5G Core Network*
CQI	*Channel Quality Indicator*
CSI	*Channel State Information*
CU	*Central Unit*
DL	*Downlink*
DMRS	*Demodulation Reference Signal*
DPI	*Deep Packet Inspection*
DRB	*Data Radio Bearer*
DU	*Distributed Unit*
EPC	*Evolved Packet Core*
ETSI	*European Telecommunications Standards Institute*
FDD	*Frequency Division Duplex*
FR1 / FR2	*Frequency Range 1 / 2*
GAA	*Generic Authentication Architecture*
GBA	*Generic Bootstrapping Architecture*
GPRS	*General Packet Radio System*
GSM	*Global System for Mobile Communications*
GTP-U	*GPRS Tunnelling Protocol – User Plane*
GUAMI	*Globally Unique AMF Identifier*
GUTI	*Globally Unique Temporary Identifier*
IMT-2020	*International Mobile Telecommunications-2020*
HARQ	*Hybrid Automatic Repeat reQuest*
IP	*Internet Protocol*
IMSI	*International Mobile Subscriber Identity*
ITU-R	*International Telecommunication Union – Radiocommunication Sector*
KPI	*Key Performance Indicator*
LTE	*Long Term Evolution*

LoS / NLoS	*Line-of-Sight / Non-Line-of-Sight*
MAC	*Medium Access Control*
MCC	*Mobile Country Code*
MCS	*Modulation and Coding Scheme*
MIMO	*Multiple-Input Multiple-Output*
MNC	*Mobile Network Code*
MSIN	*Mobile Subscription Identification Number*
NAS	*Non-Access Stratum*
NAT	*Network Address Translation*
NB-IoT	*Narrowband IoT*
NF	*Network Function*
NGAP	*NG Application Protocol*
NR	*New Radio*
NSA / SA	*Non-Standalone / Standalone*
NRF	*Network Repository Function*
NSSF	*Network Slice Selection Function*
O-RAN	*Open Radio Access Network*
OAI	*OpenAirInterface*
OSA	*OpenAirInterface Software Alliance*
OFDM	*Orthogonal Frequency Division Multiplexing*
PDCCH	*Physical Downlink Control Channel*
PDCP	*Packet Data Convergence Protocol*
PCF	*Policy Control Function*
PDU	*Protocol Data Unit*
PLMN	*Public Land Mobile Network*
PRB	*Physical Resource Block*
QPSK	*Quadrature Phase Shift Keying*
RAN	*Radio Access Network*
RB	*Resource Block*
RE	*Resource Element*
RF	*Radio Frequency*
RI	*Rank Indicator*
RLC	*Radio Link Control*
ROHC	*Robust Header Compression*
RRC	*Radio Resource Control*
RSRP	*Reference Signal Received Power*
RSRQ	*Reference Signal Received Quality*

RSSI	*Received Signal Strength Indicator*
RTT	*Round-Trip Time*
RU	*Radio Unit*
RxSL	*Receiver Sensitivity Level*
S-NSSAI	*Single Network Slice Selection Assistance Information*
SBA	*Service-Based Architecture*
SCS	*Subcarrier Spacing*
SD	*Slice Differentiator*
SMF	*Session Management Function*
SDAP	*Service Data Adaptation Protocol*
SIDF	*Subscription Identifier De-concealing Function*
SINR	*Signal-to-Interference-plus-Noise Ratio*
SNR	*Signal-to-Noise Ratio*
SQN	*Sequence Number*
SST	*Slice/Service Type*
SUCI	*Subscription Concealed Identifier*
SUPI	*Subscription Permanent Identifier*
TAC	*Tracking Area Code*
TAI	*Tracking Area Identity*
TDD	*Time Division Duplex*
UDM	*Unified Data Management*
UE	*User Equipment*
UICC	*Universal Integrated Circuit Card*
UPF	*User Plane Function*
UL	*Uplink*
UMa	*Urban Macro*
USIM	*Universal Subscriber Identity Module*
URLLC	*Ultra-Reliable Low-Latency Communications*
USRP	*Universal Software Radio Peripheral*

1 Introdução

1.1 Enquadramento

A evolução das redes móveis tem sido impulsionada pela necessidade de suportar serviços de comunicação cada vez mais exigentes, cada geração introduzindo melhorias ao nível da capacidade de transmissão, da latência, da fiabilidade e da diversidade de serviços disponibilizados. Da 1G, exclusivamente analógica e vocacionada para voz, até à 4G, *Long Term Evolution* (LTE), já totalmente digital e baseada em *Internet Protocol* (IP), cada transição resultou de limitações concretas da geração anterior, normalizadas progressivamente pelo *3rd Generation Partnership Project* (3GPP) a partir da 3G. A própria 2G, assente no *Global System for Mobile Communications* (GSM), já tinha marcado a transição para a comunicação digital antes da constituição do 3GPP.

A crescente diversificação de aplicações evidenciou, no entanto, requisitos que a 4G não fora concebida para satisfazer isoladamente, nomeadamente latências muito reduzidas, densidades de dispositivos muito superiores e débitos de dados multi-gigabit. Para lhes dar resposta, a *International Telecommunication Union - Radiocommunication Sector* (ITU-R), no âmbito da especificação *International Mobile Telecommunications-2020* (IMT-2020), definiu três classes de utilização para a quinta geração (5G): banda larga móvel melhorada (*enhanced Mobile Broadband* - eMBB), comunicações ultra-fiáveis e de baixíssima latência (*Ultra-Reliable Low-Latency Communications* - URLLC) e comunicações maciças do tipo máquina (*massive Machine-Type Communications* - mMTC). O 3GPP respondeu com uma nova interface rádio, o *New Radio* (NR), e uma arquitetura de núcleo de rede orientada a serviços (*Service-Based Architecture* - SBA). É precisamente esta arquitetura que constitui o objeto de estudo do presente trabalho, detalhado nas secções seguintes.

A Tabela 1:1 sintetiza esta evolução, situando cada geração no tempo, na técnica de acesso utilizada e na *release* 3GPP correspondente, e evidenciando a dimensão do salto técnico introduzido pelo 5G.

Tabela 1:1 Evolução das gerações de redes móveis

Geração	Ano	Tecnologia-chave	Débito de pico	Release 3GPP	Serviços
1G	~1980	Analógico, só voz	Não aplicável	Sem 3GPP	Voz analógica
2G	1991	GSM digital, SMS	114 kbit/s (GPRS)	Pré-3GPP (ETSI)	Voz digital, SMS
3G	2001	UMTS / HSPA	~14 Mbit/s	99, 5, 6	Multimédia, videochamada, internet móvel
4G	2009	LTE, IP nativo	1 Gbit/s (LTE-A)	8, 10, 13	Banda larga móvel, vídeo HD, VoLTE, IoT (NB-IoT)
5G	2019	5G NR, SBA	20 Gbit/s	15, 16, 17, 18	eMBB, URLLC, mMTC, network slicing

1.2 Motivação e Problema

A implementação e avaliação experimental de redes 5G NR constituem um desafio técnico significativo, uma vez que envolvem a integração de diferentes componentes de *hardware* e *software*, bem como a configuração de múltiplos parâmetros da rede de acesso rádio (RAN) e do núcleo de rede (doravante designado por *Core Network* - CN). Embora as redes comerciais permitam a disponibilização de serviços 5G, as soluções assentam, maioritariamente, em *hardware* proprietário e *software* de código fechado (ex.: Ericsson, Nokia, Huawei, ZTE e, mais recentemente, Samsung), limitando o acesso aos mecanismos internos de funcionamento da rede e a possibilidade de alterar parâmetros de configuração para fins de experimentação.

Acresce que a implementação de infraestruturas experimentais baseadas em soluções comerciais está frequentemente associada a custos elevados de aquisição de equipamento especializado e, em determinados cenários, à necessidade de utilização de espetro licenciado. Estes fatores constituem limitações importantes para atividades de ensino, investigação e desenvolvimento, particularmente quando o objetivo consiste em analisar o comportamento da rede sob diferentes configurações da interface rádio.

Neste contexto, a comunidade científica tem desenvolvido plataformas 5G NR de código aberto, compatíveis com as especificações do 3GPP, capazes de funcionar sobre equipamentos de rádio definido por *software* (*Software Defined Radio* - SDR). Estas plataformas permitem implementar redes experimentais em ambiente laboratorial, oferecendo um elevado grau de configurabilidade e acesso aos diferentes componentes da pilha protocolar, constituindo uma alternativa viável às soluções comerciais para fins de ensino, investigação e validação experimental. As plataformas mais conhecidas encontram-se identificadas na Tabela 1:2

Tabela 1:2 Plataformas 5G de código aberto mais relevantes

Plataforma	RAN	CN	Funções de rede
OAI	Sim	Sim	7
srsRAN*	Sim	Não (usa Open5GS ou OAI)	Não aplicável
Open5GS	Não	Sim	8
Free5GC	Não	Sim	10

* Após a aquisição da empresa SRS pela Rohde & Schwarz, o código da srsRAN foi financiado pelo Departamento de Defesa dos Estados Unidos da América e transferido para a Linux Foundation sob o novo nome OCUDU.

1.3 Objetivos

O presente trabalho tem como objetivo geral a implementação e avaliação experimental de uma rede 5G NR baseada no código OAI, implementado pela plataforma OAIBOX™[21], com vista à análise do comportamento da interface rádio em diferentes cenários de configuração.

Para concretizar este projeto, definiram-se os seguintes objetivos específicos:

- implementar e configurar uma rede 5G NR em ambiente laboratorial utilizando a plataforma OAIBOX™;
- caracterizar a arquitetura da rede, identificando os principais componentes da rede de acesso rádio (*Radio Access Network* - RAN) e do *Core* da rede (CN), bem como as interfaces que os interligam;
- analisar os procedimentos de estabelecimento da ligação entre o equipamento do utilizador (*User Equipment* - UE), a estação base (*Next Generation Node B* - gNB) e a rede principal;
- identificar as principais especificações do 3GPP aplicáveis aos procedimentos analisados;
- monitorizar e interpretar os principais indicadores-chave de desempenho (*Key Performance Indicators* - KPIs) e métricas de comunicação disponibilizados pela plataforma experimental;
- avaliar experimentalmente o impacto de diferentes configurações da interface rádio no desempenho da rede.

Para apoiar a realização dos ensaios experimentais, recorreram-se ainda a ferramentas complementares de medição e análise, nomeadamente um analisador de espectro, utilizado para observar sinais de radiofrequência, e *o* Wireshark, utilizado na captura e análise do tráfego dos planos de controlo e de utilizador.

1.4 A Plataforma OAIBOX™

Com o objetivo de implementar uma rede 5G NR em ambiente laboratorial, no presente trabalho foi utilizada a plataforma OAIBOX™, desenvolvida pela empresa Allbesmart, Lda [21]. Esta plataforma disponibiliza uma solução experimental *end-to-end*, permitindo a implementação da rede de acesso rádio (RAN) e do *Core* da rede (CN), constituindo uma infraestrutura adequada para a realização de ensaios experimentais em ambiente controlado.

A OAIBOX™ tem por base o projeto open *source* designado por *OpenAirInterface* (OAI), iniciado pela EURECOM [22] e atualmente desenvolvido pela *OpenAirInterface Software Alliance* (OSA). A OAI disponibiliza uma implementação da arquitetura 4G LTE e 5G NR, compatível com as especificações definidas pelo 3GPP, permitindo implementar e configurar diferentes componentes da rede móvel para fins de investigação, desenvolvimento e experimentação.

A instalação e configuração de uma rede baseada diretamente no OAI envolvem a integração de múltiplos componentes de *hardware* e *software*, bem como a configuração de diversos parâmetros da interface rádio e do núcleo de rede. Neste contexto, a OAIBOX™ atua como uma camada de abstração sobre essa complexidade, integrando numa única plataforma os diferentes componentes necessários ao funcionamento de uma rede experimental 5G, nomeadamente *software* desenvolvido pela OAI e *hardware* de diversos fabricantes parceiros, como a *Quectel*, a *Ettus*/*National Instruments* (NI), a *Benetel*, a *Pi-Radio* e a *Liteon*, entre outros.

Esta integração permite disponibilizar um ambiente experimental previamente configurado, reduzindo o esforço associado à instalação e configuração manual da infraestrutura de rede. Consequentemente, a atividade experimental pode centrar-se na configuração dos parâmetros da interface rádio, na monitorização dos indicadores de

desempenho e na análise do impacto das diferentes configurações sobre o comportamento da rede 5G NR, objetivos que constituem o foco do presente trabalho.

1.5 Requisitos Técnicos do 5G NR (IMT-2020)

A Tabela 1:3 sintetiza os principais requisitos técnicos definidos pela ITU-R para o 5G, no âmbito da especificação IMT-2020. Estes valores correspondem a metas de referência para condições ideais de laboratório, e não a garantias de desempenho em ambiente real; trata-se de uma distinção relevante para a interpretação dos resultados experimentais apresentados adiante neste trabalho.

Tabela 1:3 Requisitos técnicos definidos pela especificação IMT-2020

Parâmetro de Desempenho	**Especificação IMT-2020**
Taxa de pico	20 Gbit/s (DL) e 10 Gbit/s (UL)
Latência de interface	1 ms para serviços URLLC
Densidade de dispositivos	10^6 dispositivos/km²
Disponibilidade do sistema	99,999%
Eficiência energética	Redução de consumo até 90% na infraestrutura
Autonomia de dispositivos IoT	Até 10 anos para dispositivos LPWA (*Low Power Wide Area*)
Capacidade de tráfego	1 Tbit/s/km²
Mobilidade suportada	Até 500 km/h (ferroviário) e 1000 km/h (aeronáutico)

1.6 Especificações Normativas 3GPP Relevantes para o 5G NR

As especificações técnicas do 3GPP encontram-se organizadas em séries numeradas, cada uma associada a um domínio funcional do sistema. A Tabela 1:4 apresenta as séries normativas principais para o enquadramento inicial do presente trabalho e a respetiva função no sistema 5G, servindo de mapeamento inicial para os capítulos subsequentes.

Tabela 1:4 Séries normativas 3GPP principais e respetivo domínio funcional

Série	**Norma**	**Função**
21.xxx	TS 21.916[8]	Descrição geral da *Release* / visão global do 5G
22.xxx	TS 22.261[9]	Requisitos de serviço do sistema 5G
23.xxx	TS 23.501[10]	Arquitetura geral do 5G *Core* (CN5G)
23.xxx	TS 23.502[11]	Procedimentos e fluxos do sistema 5G
24.xxx	TS 24.501[1]	Protocolo NAS (*Non-Access-Stratum*) do *Core* 5G
29.xxx	TS 29.500[12]	APIs da *Service Based Architecture* (SBA) do *Core*
33.xxx	TS 33.501[13]	Arquitetura e procedimentos de Segurança do 5G
38.xxx	TS 38.300[14]	Arquitetura geral e protocolos da NG-RAN (5G NR)

2 Fundamentos da Arquitetura do Sistema 5G NR

2.1 Arquitetura do Sistema 5G NR

A arquitetura do sistema 5G NR, normalizada pelo 3GPP, foi concebida para responder aos requisitos definidos pela ITU-R no âmbito do IMT-2020. Comparativamente às gerações anteriores de redes móveis, esta arquitetura introduz uma infraestrutura de comunicações mais flexível, escalável e eficiente, capaz de suportar maiores taxas de transmissão, menor latência, elevada fiabilidade das comunicações, maior eficiência espectral e uma elevada densidade de dispositivos ligados em simultâneo.

A implementação de uma rede 5G pode seguir duas arquiteturas distintas:

- *Non-Standalone* (NSA)
- *Standalone* (SA).

A arquitetura NSA foi introduzida como uma solução de transição entre as redes 4G LTE e o 5G, permitindo reutilizar a infraestrutura LTE já existente. Nesta configuração, a estação base 5G (gNB) opera em conjunto com uma estação base LTE (eNB), enquanto as funções da rede principal continuam a ser asseguradas pela rede *core* do 4G, Evolved *Packet Core* (EPC).

Em contrapartida, a arquitetura SA corresponde a uma implementação integralmente baseada em tecnologia 5G. Nesta configuração, a rede de acesso rádio comunica diretamente com o *Core* da rede, eliminando a dependência da infraestrutura LTE e permitindo explorar todas as funcionalidades nativas do sistema 5G. Entre estas destacam-se a arquitetura orientada a serviços SBA, o suporte para *network slicing*, mecanismos avançados de gestão da mobilidade e uma utilização mais eficiente dos recursos da rede.

A Tabela 2:1 apresenta uma comparação resumida entre as arquiteturas NSA e SA, evidenciando as principais diferenças entre ambas.

Tabela 2:1 Comparação entre as arquiteturas 5G NSA e SA

Característica	**NSA**	**SA**
Rede principal	*Evolved Packet Core* (EPC)	5G *Core* (CN5G)
Dependência da infraestrutura LTE	Sim	Não
Estação base LTE (eNB)	Utilizada	Não utilizada
Estação base 5G (gNB)	Sim	Sim
Suporte das funcionalidades nativas do 5G	Parcial	Completo
Arquitetura utilizada no presente trabalho	Não	Sim

Embora ambas as arquiteturas coexistam atualmente nas redes comerciais, a plataforma OAIBOX™, utilizada no presente trabalho, implementa uma rede 5G SA. Consequentemente, as secções seguintes incidem exclusivamente sobre esta arquitetura.

Conforme ilustrado na Figura 2-1, uma rede 5G SA é constituída por três blocos funcionais principais:

- Equipamento do Utilizador (User Equipment - UE);

- Rede de Acesso Rádio (RAN);
- Core da rede 5G (CN5G).

Estes blocos funcionais comunicam através de interfaces normalizadas pelo 3GPP, assegurando o estabelecimento da ligação rádio, a gestão das comunicações e o encaminhamento do tráfego entre o equipamento do utilizador e as redes de dados. A descrição detalhada da RAN, do CN5G e das respetivas interfaces de comunicação é apresentada nas secções seguintes.

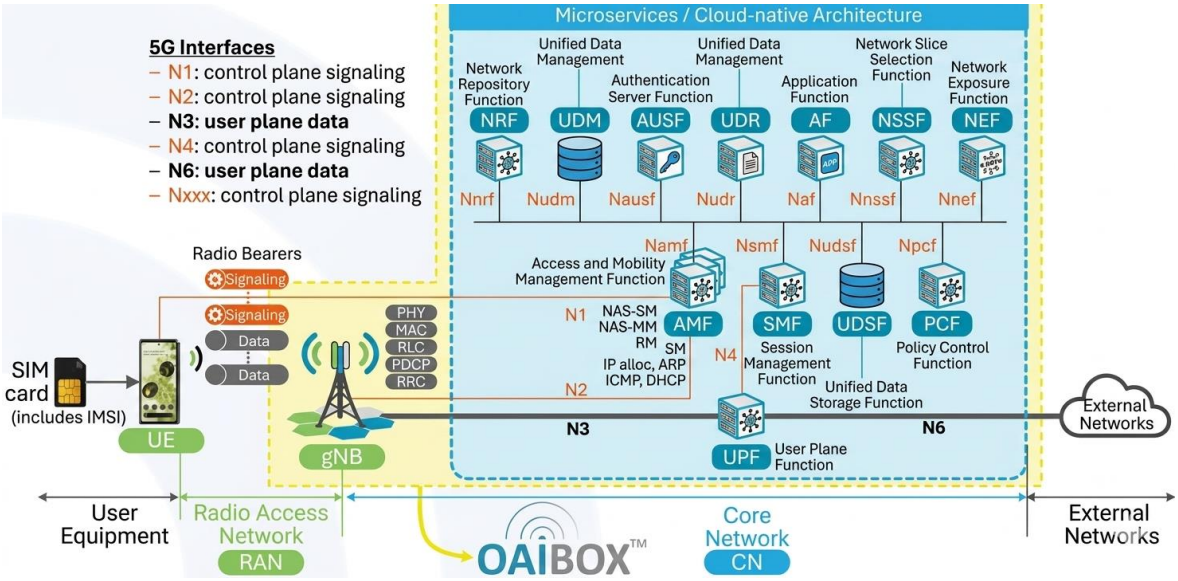


Figura 2-1: Arquitetura de uma rede 5G [23]

2.2 Rede de Acesso Rádio (RAN)

A RAN constitui o elemento do sistema 5G responsável por estabelecer a ligação entre o UE e o CN5G através da interface rádio Uu. A RAN assegura a transmissão e receção de informação entre os equipamentos do utilizador e a rede, disponibilizando os mecanismos necessários para o acesso ao sistema, gestão dos recursos rádio, mobilidade e encaminhamento do tráfego.

No sistema 5G NR, a rede RAN é composta por um ou mais gNBs, que implementam as funções da interface rádio (PHY, MAC, RLC, PDCP e RRC), analisadas na secção 2.2.2 e asseguram a interligação com a rede core através das interfaces NG. Comparativamente às gerações anteriores, para o 5G o 3GPP introduz uma arquitetura mais flexível para o gNB, permitindo que determinadas funções possam ser implementadas de forma centralizada (gNB monolítico) ou distribuída (gNB desagregado), de acordo com os requisitos de desempenho e com o cenário de implementação.

Para além de assegurar a comunicação rádio com o UE, a RAN desempenha um papel determinante na otimização da utilização do espetro radioelétrico, adaptando continuamente os parâmetros de transmissão às condições instantâneas do canal rádio. Esta adaptação permite maximizar a eficiência espectral e assegurar a qualidade da comunicação mesmo perante variações das condições de propagação.

No contexto do presente trabalho, a RAN corresponde ao componente da rede onde são configurados e avaliados os principais parâmetros da interface rádio, nomeadamente

a largura de banda, a frequência de operação, a modulação e outros mecanismos de transmissão que influenciam diretamente os indicadores de desempenho (KPIs) que serão analisados nos ensaios experimentais no capítulo 3.

2.2.1 Next Generation Node B (gNB)

O gNB corresponde à estação base do sistema 5G NR, sendo responsável pela gestão da interface rádio entre o UE e o CN5G. Constitui o principal elemento da RAN, assegurando simultaneamente funções de controlo e de encaminhamento do tráfego de utilizador. Entre as suas principais responsabilidades destacam-se o estabelecimento e manutenção da ligação rádio, a configuração dos recursos de transmissão, o controlo da mobilidade, a gestão do acesso à rede e o encaminhamento do tráfego para o CN5G através das interfaces normalizadas pelo 3GPP.

Durante o funcionamento da rede, o gNB monitoriza continuamente a qualidade do canal rádio através das medições reportadas pelo UE. Com base nesta informação, adapta dinamicamente diferentes parâmetros de transmissão, como o esquema de modulação e codificação, a potência de transmissão e a atribuição de recursos rádio, procurando maximizar a eficiência espectral e manter a qualidade da comunicação. O gNB é igualmente responsável pelo agendamento (*scheduling*) das transmissões em *Downlink* (DL) e *Uplink* (UL). Este mecanismo determina a atribuição temporal e espectral dos recursos rádio aos diferentes equipamentos ligados à célula, tendo em consideração critérios como a qualidade do canal, os requisitos de qualidade de serviço e a disponibilidade de recursos.

Nas implementações mais recentes, o 3GPP prevê ainda a possibilidade de o gNB ser dividido funcionalmente em duas entidades: a *Central Unit* (CU) e a *Distributed Unit* (DU). A CU concentra as funções de controlo e parte do processamento dos protocolos superiores, enquanto a DU executa as funções associadas ao processamento em tempo real da interface rádio. No entanto, em muitas implementações práticas, a DU encontra-se ainda ligada a uma *Radio Unit* (RU), responsável pelas funções de radiofrequência e pela conversão entre os sinais digitais e os sinais transmitidos e recebidos pelas antenas. Embora a RU não faça parte da divisão funcional CU/DU definida pelo 3GPP, constitui um elemento amplamente adotado nas arquiteturas atuais. Esta desagregação permite maior flexibilidade na implementação da rede, mantendo, do ponto de vista funcional, a CU e a DU como partes integrantes de um único gNB.

A plataforma OAIBOX™, utilizada neste projeto, suporta esta arquitetura desagregada, incluindo as entidades CU e DU e a sua ligação a uma Radio Unit (RU), refletindo a organização adotada nas implementações Open RAN (O-RAN) atuais.

2.2.2 Interface Rádio NR

A interface rádio NR estabelece a comunicação sem fios entre o UE e o gNB, constituindo o principal meio de transporte da informação entre o utilizador e a rede. O seu funcionamento é definido pelas especificações da série 3GPP TS 38.xxx[18], que estabelecem os procedimentos de transmissão, sincronização, acesso ao meio e gestão dos recursos rádio.

Ao contrário das gerações anteriores, a interface rádio NR foi concebida para proporcionar uma maior flexibilidade de configuração, permitindo adaptar os parâmetros físicos às diferentes bandas de frequência e aos diversos cenários de utilização previstos para o 5G.

Entre os parâmetros de configuração mais relevantes destacam-se a frequência de operação, a largura de banda, a numerologia, o espaçamento entre subportadoras (*Subcarrier Spacing* - SCS) e o número de blocos de recursos físicos (*Physical Resource Blocks* - PRBs) doravante designado por N_PRB. Cada PRB é constituído por 12 subportadoras, sendo a unidade mínima de recurso tempo-frequência designada por elemento de recurso (*Resource Element* - RE), correspondente a uma subportadora num único símbolo OFDM (*Orthogonal Frequency Division Multiplexing*). Estes parâmetros determinam diretamente a capacidade de transmissão, a latência e a eficiência espectral da ligação.

A Tabela 2:2 apresenta os parâmetros de configuração associados a cada numerologia suportada pelo 5G NR [20].

Tabela 2:2 Parâmetros por numerologia (μ)

μ	Δf (kHz)	Duração do slot	Slots por frame	Duração do símbolo OFDM
0	15	1 ms	10	71,43 μs
1	30	500 μs	20	35,71 μs
2	60	250 μs	40	17,86 μs
3	120	125 μs	80	8,93 μs
4	240	62,5 μs	160	4,46 μs
5	480	31,25 μs	320	2,23 μs

No presente trabalho, a largura de banda assume particular importância, uma vez que constitui um dos principais parâmetros experimentais avaliados. O aumento da largura de banda permite disponibilizar um maior número de blocos de recursos para transmissão, aumentando potencialmente a capacidade da interface rádio e, consequentemente, o débito máximo alcançável, desde que as restantes condições da ligação permaneçam favoráveis. A Tabela 2:3 apresenta o número máximo de blocos de recursos configuráveis para transmissão, por largura de banda de canal, considerando a numerologia μ=1 (SCS de 30 kHz), utilizada nos ensaios descritos na secção 3.3.

Tabela 2:3 Número máximo de blocos de recursos por largura de banda (μ=1, SCS=30 kHz)

Largura de banda (MHz)	10	15	20	25	30	40	50
N_PRB	24	38	51	65	78	106	133

A informação transmitida através da interface rádio é organizada segundo uma estrutura temporal baseada em radio *frames*, *subframes*, *slots* e símbolos OFDM, permitindo uma utilização eficiente dos recursos rádio e uma adaptação dinâmica às diferentes configurações da rede. A duração dos *slots* depende da numerologia (μ), estando diretamente relacionada com o espaçamento entre subportadoras (SCS), conforme já apresentado na Tabela 2:2. Em condições normais de operação, cada *slot* é constituído por 14 símbolos OFDM, independentemente da numerologia utilizada. A Figura 2-2 apresenta a estrutura temporal da interface rádio NR e a relação entre a numerologia, o espaçamento entre subportadoras e a duração dos *slots*.

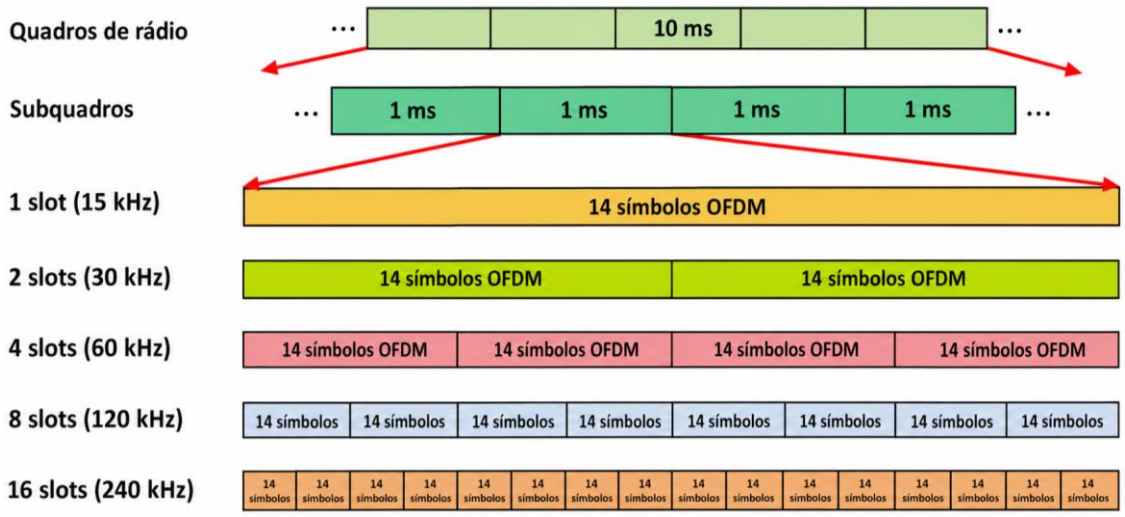


Figura 2-2: Estrutura temporal da interface rádio NR

A Tabela 2:4 apresenta a numerologia e o respetivo espaçamento entre subportadoras e duração do *slot.*

Tabela 2:4 Numerologia e espaçamento entre subportadoras (SCS) na interface rádio NR

Numerologia (μ)	**0**	**1**	**2**	**3**	**4**
SCS (kHz)	15	30	60	120	240
Duração do *Slot* (ms)	1	0,5	0,25	0,125	0,0625

2.2.3 Técnicas de transmissão da interface rádio

O desempenho da interface rádio é influenciado não apenas pelas condições de propagação do canal, mas também pelos mecanismos de adaptação da transmissão implementados pelo sistema. Entre os principais destacam-se o esquema de modulação, o *Modulation and Coding Scheme* (MCS) e a utilização de múltiplas antenas através da tecnologia *Multiple-Input Multiple-Output* (MIMO).

À medida que aumenta a ordem da modulação, cresce o número de bits transportados por símbolo, permitindo aumentar a eficiência espectral. Em contrapartida, estas modulações exigem melhores condições do canal rádio, uma vez que apresentam maior sensibilidade ao ruído e à interferência. A seleção da modulação é efetuada dinamicamente através do MCS, mecanismo que combina o esquema de modulação com a respetiva taxa de codificação (*Coding Rate*). Esta adaptação é realizada pelo gNB com base no *Channel Quality Indicator* (CQI) reportado pelo UE, permitindo selecionar, para cada instante de transmissão, a configuração que oferece o melhor compromisso entre débito, robustez e fiabilidade da ligação rádio.

Outro mecanismo fundamental é a tecnologia MIMO, que utiliza múltiplas antenas de transmissão e receção para aumentar a capacidade do sistema e melhorar a robustez da comunicação. Dependendo da configuração adotada, o MIMO pode explorar técnicas de diversidade espacial, multiplexagem espacial ou formação de feixe (*beamforming*),

permitindo aumentar o débito de transmissão, melhorar a cobertura rádio e utilizar de forma mais eficiente os recursos espectrais disponíveis.

Embora estes mecanismos desempenhem um papel determinante no desempenho da interface rádio, o presente trabalho incide principalmente sobre a avaliação experimental da influência de diferentes configurações da interface rádio NR, com particular enfoque na largura de banda configurada e no seu impacto nos indicadores de desempenho analisados experimentalmente.

2.2.4 Bandas de Frequência do 5G NR

O 3GPP organiza o espetro radioelétrico atribuído ao 5G NR em duas gamas de frequência distintas, definidas na norma TS 38.104[3], com requisitos técnicos e condições de teste diferenciados: a *Frequency Range 1* (FR1) e a *Frequency Range 2* (FR2).

A FR1, coloquialmente designada por sub-6 GHz, inclui as bandas baixas, tradicionalmente utilizadas em redes móveis anteriores e caracterizadas por maior alcance de cobertura, e as bandas médias, que oferecem um compromisso equilibrado entre capacidade e cobertura, sendo por isso as mais utilizadas nas implementações comerciais e experimentais de 5G SA na Europa. A FR2 corresponde às ondas milimétricas (*millimetre waves* - mmWave), permitindo larguras de banda de canal muito superiores às da FR1, mas sofrendo maior atenuação em espaço livre e menor penetração em obstáculos, o que exige densidades de estações base substancialmente superiores.

A Tabela 2:5 sintetiza as principais características técnicas de cada gama de frequência, incluindo os respetivos intervalos, as larguras de banda de canal suportadas e os cenários de utilização típicos.

Tabela 2:5 Gamas de frequência do 5G NR (FR1 e FR2)

Característica	FR1 (sub-6 GHz)	FR2 (mmWave)
Intervalo de frequências	410 MHz a 7125 MHz	24,25 GHz a 71 GHz
Subdivisão	Bandas baixas e bandas médias	FR2-1 (24,25-52,6 GHz) e FR2-2 (52,6-71 GHz)
Largura de banda de canal	5 MHz a 100 MHz	50 MHz a 2000 MHz
Propagação	Maior alcance e penetração em obstáculos	Maior atenuação; menor penetração
Utilização típica	Implementações comerciais e experimentais de 5G SA	Cenários de elevada capacidade e curto alcance

2.2.5 Modos de configuração e cenários de aplicação do gNB

Como referido na secção 2.2.1, a CU concentra as funções de controlo e de processamento das camadas superiores (RRC e PDCP), enquanto a DU executa o processamento em tempo real das camadas inferiores (RLC, MAC e PHY). O 3GPP prevê, na norma TS 38.401[17], diferentes formas de implementar esta divisão funcional, distintas da arquitetura totalmente integrada (monolítica) já apresentada. Estas formas de configuração não alteram o comportamento lógico do gNB perante o UE ou o CN5G, mas têm implicações relevantes na forma como a rede é fisicamente implementada, sendo por isso escolhidas em função do cenário de aplicação pretendido.

Na configuração monolítica, todas as funções do gNB, desde a camada física até ao RRC, são executadas numa única entidade física, colocada junto da antena. Esta abordagem simplifica a implementação e reduz a latência interna de processamento, sendo por isso adequada a cenários de menor escala, como redes privadas, campi universitários ou ambientes de teste e desenvolvimento, nos quais a simplicidade de configuração é mais relevante do que a capacidade de coordenação entre múltiplas células. É esta a configuração adotada na plataforma OAIBOX™ utilizada no presente trabalho, pelas razões que se detalham mais adiante nesta secção.

Como alternativa, o 3GPP prevê a divisão funcional do gNB em duas ou três entidades distintas, ligadas entre si por interfaces normalizadas: a CU, a DU e, opcionalmente, a *Radio Unit* (RU). A RU corresponde à unidade responsável pelas funções mais próximas da antena, nomeadamente a conversão entre o sinal digital e o sinal de radiofrequência, a amplificação de potência, e, nas configurações que assim o prevejam, parte do processamento da camada física associado à formação de feixes (*beamforming*). Esta separação pode ocorrer em diferentes pontos da pilha protocolar, correspondendo a oito opções de divisão (*split options*) definidas pelo 3GPP, das quais se destacam duas pela sua relevância prática:

- A divisão de alto nível (*Option 2*), na qual a CU concentra as camadas RRC e PDCP, enquanto a DU executa as camadas RLC, MAC e PHY, sendo ambas ligadas através da interface F1. Esta configuração é a mais utilizada em implementações comerciais, uma vez que os requisitos de latência e de débito entre a CU e a DU são relativamente moderados, permitindo o uso de redes de transporte convencionais baseadas em Ethernet.
- A divisão de baixo nível (*Option 7.2*), na qual apenas as funções mais próximas da antena, executadas na RU, permanecem separadas da DU, que concentra as restantes funções da camada física e das camadas superiores. Esta configuração exige uma rede de *fronthaul* com latência muito reduzida e elevado débito, mas permite uma centralização mais completa do processamento em banda base, favorecendo técnicas de coordenação entre células como o CoMP (*Coordinated Multipoint*).

A escolha entre estas configurações depende, assim, do cenário de aplicação: implementações densas e urbanas, com um elevado número de pontos de acesso próximos entre si, beneficiam da centralização proporcionada pela divisão CU/DU/RU, uma vez que permite partilhar recursos de processamento e coordenar a transmissão entre células vizinhas, reduzindo a interferência e melhorando a eficiência espectral global da rede. Em contrapartida, cenários de menor densidade, redes privadas ou ambientes experimentais, como o do presente trabalho, não retiram benefício proporcional desta centralização, sendo a configuração monolítica suficiente e preferível pela sua simplicidade de implementação, configuração e diagnóstico.

No presente trabalho, a plataforma OAIBOX™ implementa o gNB de forma monolítica, executando localmente todas as camadas protocolares descritas na secção 2.4, o que se revela adequado ao ambiente de laboratório utilizado, uma vez que dispensa a necessidade de configurar uma rede de *fronthaul* dedicada e simplifica a captura e análise da sinalização trocada com o CN5G, aspeto central para os objetivos experimentais do presente trabalho.

2.3 Core da Rede 5G (CN5G)

O CN5G constitui a rede principal do sistema 5G e é responsável pelas funções de controlo, autenticação, gestão das sessões de comunicação e encaminhamento do tráfego entre a rede de acesso rádio e as redes de dados externas. Comparativamente ao *Evolved Packet Core* (EPC) utilizado nas redes LTE, o CN5G introduz uma arquitetura mais flexível e modular, permitindo responder aos diferentes requisitos de desempenho definidos para os serviços 5G.

Uma das principais evoluções introduzidas pelo CN5G consiste na adoção da SBA, definida pelo 3GPP. Ao contrário das arquiteturas anteriores, baseadas em interfaces ponto-a-ponto entre entidades de rede, a SBA organiza o núcleo de rede como um conjunto de *Network Functions* (NFs) independentes, que disponibilizam os seus serviços através de interfaces normalizadas e baseadas em protocolos IP. Esta abordagem facilita a escalabilidade da rede, simplifica a introdução de novas funcionalidades e permite uma gestão mais flexível dos recursos.

A arquitetura SBA encontra-se igualmente alinhada com os princípios da virtualização e da computação em nuvem (*cloud-native*), permitindo que as diferentes funções do núcleo de rede sejam implementadas em máquinas virtuais ou contentores e distribuídas por diferentes infraestruturas computacionais, sem alterar o seu funcionamento lógico.

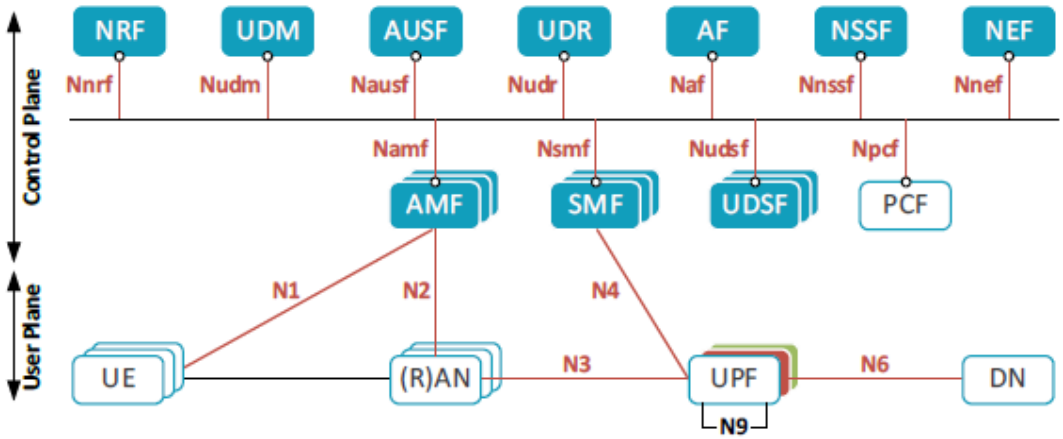


Figura 2-3: Arquitetura do Core da rede 5G (CN5G) [25]

Embora o 3GPP defina um conjunto alargado de funções para o CN5G, apenas algumas desempenham um papel central na arquitetura implementada neste trabalho. A Tabela 2:6 apresenta as principais funções de rede e a respetiva responsabilidade no funcionamento do sistema.

2.3.1 Principais funções do 5G Core

O 3GPP define, na norma TS 23.501[10], um conjunto alargado de funções de rede (*Network Functions* - NFs) para o 5G Core, cada uma responsável por um domínio funcional específico da arquitetura orientada a serviços (SBA). A Tabela 2:6 apresenta as principais funções de rede consideradas no âmbito do presente trabalho, bem como a respetiva responsabilidade no funcionamento do sistema.

Tabela 2:6 Principais funções de rede do 5G Core

Função	Designação	Principal responsabilidade
AMF	*Access and Mobility Management Function*	Gestão do acesso à rede, mobilidade, registo do UE e sinalização NAS.
SMF	*Session Management Function*	Gestão das sessões PDU, atribuição de endereços IP e controlo das ligações de dados.
UPF	*User Plane Function*	Encaminhamento do tráfego de utilizador entre a RAN e as redes de dados externas.
UDM	*Unified Data Management*	Gestão da informação de subscrição dos utilizadores.
AUSF	*Authentication Server Function*	Autenticação dos equipamentos e dos utilizadores.
NRF	*Network Repository Function*	Registo e descoberta das funções de rede disponíveis.
PCF	*Policy Control Function*	Definição das políticas de qualidade de serviço e controlo de recursos.
NSSF	*Network Slice Selection Function*	Seleção da *network slice* adequada ao UE, com base no S-NSSAI pedido

Para além do resumido na Tabela 2:6, acrescenta-se ainda a seguinte informação adicional sobre estas funções de rede:

- A AMF é responsável pelo estabelecimento do acesso à rede, pela gestão da mobilidade e pelos procedimentos de registo do UE. Todas as mensagens de sinalização provenientes do equipamento do utilizador são inicialmente processadas por esta função.
- A SMF gere as sessões de comunicação estabelecidas entre o utilizador e a rede, sendo responsável pela criação, modificação e libertação das sessões PDU (*Protocol Data Unit*), bem como pela seleção da UPF responsável pelo encaminhamento do tráfego.
- A UPF implementa o plano de utilizador do sistema, encaminhando os pacotes de dados entre a RAN e as redes de dados externas. Deste modo, constitui o elemento responsável pelo transporte efetivo da informação gerada pelas aplicações dos utilizadores.
- A NSSF é responsável por selecionar, para cada UE, as *networks slices* mais adequadas às suas necessidades, com base no S-NSSAI solicitado durante o registo.
- As restantes funções, nomeadamente a UDM, a AUSF, a NRF e a PCF, asseguram tarefas complementares relacionadas com a gestão da informação de subscrição, a autenticação dos utilizadores, a descoberta dinâmica de serviços e a definição das políticas de funcionamento da rede.

2.3.2 Network Slicing

O *network slicing* permite particionar logicamente uma única infraestrutura física de rede em múltiplas redes virtuais independentes, cada uma otimizada para um tipo de serviço com requisitos próprios de débito, latência ou fiabilidade [9], [10].

2.3.2.1 O S-NSSAI

O S-NSSAI (*Single Network Slice Selection Assistance Information*) identifica a que *slice* pertence uma sessão [10]. É composto por dois campos: o SST (*Slice/Service Type*),

que indica a categoria do serviço, e o SD (*Slice Differentiator*), opcional, usado quando existe mais do que uma instância do mesmo tipo de *slice*.

O 3GPP define três categorias principais de SST [10]:

- eMBB (SST 1), para débitos elevados;
- URLLC (SST 2), para baixa latência e alta fiabilidade;
- mMTC (SST 3), para um número elevado de dispositivos com baixo débito individual.

Durante o registo, o UE indica o S-NSSAI pretendido. A AMF, com o apoio da NSSF, seleciona então a SMF e a UPF correspondentes a essa *slice [11]*.

Este mecanismo é avaliado experimentalmente na secção 3.11, onde se configura uma *slice* URLLC adicional à *slice* eMBB por omissão, medindo o impacto da alocação de recursos rádio no desempenho de cada uma.

2.4 Arquitetura Protocolar do Sistema 5G NR

A arquitetura protocolar do sistema 5G NR define a organização dos protocolos responsáveis pela comunicação entre o UE, a RAN e o 5G Core. Especificada pelo 3GPP, esta arquitetura estabelece as funções atribuídas a cada protocolo e a forma como estes interagem para assegurar o transporte da sinalização de controlo e dos dados do utilizador.

Os protocolos encontram-se organizados segundo uma arquitetura em camadas (*Protocol Stack*), na qual cada protocolo desempenha funções específicas e disponibiliza serviços à camada superior, recorrendo simultaneamente aos serviços disponibilizados pela camada inferior. Esta organização funcional permite separar as diferentes responsabilidades associadas ao processamento da informação, garantindo a interoperabilidade entre equipamentos compatíveis com as especificações do 3GPP.

A Figura 2-4 apresenta a arquitetura protocolar do sistema 5G NR, evidenciando a distribuição dos diferentes protocolos entre o UE, o gNB e o 5G Core, bem como a sua organização segundo dois planos funcionais distintos:

- Plano de Controlo (*Control Plane* - CP), responsável pela sinalização necessária ao estabelecimento, configuração e gestão das comunicações;
- Plano de Utilizador (*User Plane* - UP), responsável pelo transporte do tráfego de dados entre o utilizador e a rede de dados.

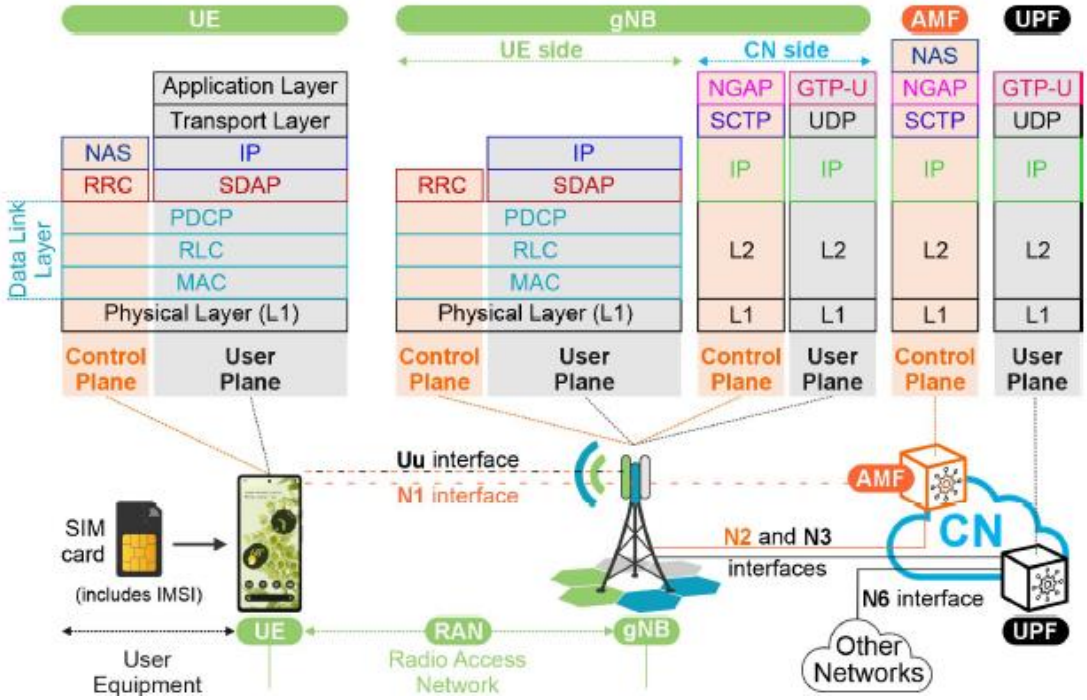


Figura 2-4: Arquitetura protocolar do sistema 5G NR [25]

Como ilustrado na Figura 2-4, a arquitetura protocolar do 5G NR organiza-se num conjunto de protocolos distribuídos entre o UE, o gNB e o 5G Core. A Tabela 2:7 descreve, de forma resumida, a especificação normativa e a função técnica principal de cada um destes protocolos.

Tabela 2:7 Classificação e especificações técnicas 3GPP da arquitetura protocolar

Protocolo	Especificação 3GPP	Função Técnica Principal
NAS (*Non-Access Stratum*)	TS 24.501[1]	Regula os protocolos de sinalização de estrato de não-acesso para a gestão de mobilidade (5GMM) e sessões (5GSM).
RRC (*Radio Resource Control*)	TS 38.331[2]	Define as funções do plano de controlo na interface Uu, incluindo difusão de SIBs, paginação e transições de estado do UE.
SDAP (*Service Data Adaptation*)	TS 37.324[15]	Responsável pelo mapeamento de QoS dinâmico entre os fluxos de QoS (QoS *Flows*) do Core e os suportes rádio (DRBs).
PDCP (*Packet Data Convergence*)	TS 38.323[4]	Executa a compressão de cabeçalhos (ROHC), a numeração de sequência, a cifragem e a proteção de integridade de dados e sinalização.
RLC (*Radio Link Control*)	TS 38.322[5]	Assegura a transferência de dados nos modos TM, UM e AM, realizando a segmentação, reassemblagem e deteção de duplicados.
MAC (*Medium Access Control*)	TS 38.321[6]	Efetua o mapeamento de canais lógicos em canais de transporte, o escalonamento (*scheduling*) de recursos e o controlo de erros via HARQ.
PHY (*Physical Layer*)	TS 38.211[7]	Define os canais físicos, as numerologias OFDM, a codificação de canal (LDPC/Polar) e as métricas rádio de medição.

2.5 Interfaces do 5G Core

A comunicação entre o UE, a RAN e o CN5G é realizada através de um conjunto de interfaces normalizadas pelo 3GPP, responsáveis pela troca de mensagens de controlo e pelo transporte do tráfego de utilizador.

A Tabela 2:8 apresenta as principais interfaces utilizadas na arquitetura 5G SA.

Tabela 2:8 Principais interfaces do sistema 5G

Interface	Entidades ligadas	Função
Uu	UE ↔ gNB	Interface rádio entre o equipamento do utilizador e a RAN.
N1	UE ↔ AMF	Transporte da sinalização NAS entre o UE e o CN5G.
N2	gNB ↔ AMF	Troca de mensagens de controlo entre a RAN e o CN5G.
N3	gNB ↔ UPF	Transporte do tráfego do plano de utilizador.
N4	SMF ↔ UPF	Gestão das sessões e configuração do plano de utilizador.
N6	UPF ↔ Data Network	Ligação entre o CN5G e as redes de dados externas.

Entre estas interfaces, assumem particular relevância as interfaces N2 e N3, uma vez que estabelecem a comunicação entre a RAN e o CN5G. A interface N2 transporta a sinalização necessária aos procedimentos de controlo, incluindo o registo do utilizador, gestão da mobilidade e estabelecimento das sessões de comunicação. Por sua vez, a interface N3 é responsável pelo encaminhamento do tráfego do plano de utilizador entre o gNB e a UPF, permitindo a transferência dos dados gerados pelas aplicações executadas no equipamento do utilizador.

A compreensão destas funções e interfaces é fundamental para interpretar os procedimentos de registo do UE, o estabelecimento das sessões de comunicação e o encaminhamento do tráfego observados durante os ensaios experimentais realizados no presente trabalho.

2.6 Procedimentos de acesso ao CN5G

O acesso de um equipamento do utilizador a uma rede 5G SA envolve um conjunto de procedimentos de sinalização normalizados pelo 3GPP, que permitem estabelecer a comunicação entre a RAN e o CN5G. Estes procedimentos asseguram que apenas equipamentos autorizados podem utilizar os recursos da rede e que a comunicação é estabelecida de forma segura.

De forma simplificada, o processo de acesso ao CN5G compreende três etapas principais:

- Numa primeira fase, o gNB estabelece ligação ao CN5G, tornando-se um elemento ativo da rede.
- Seguidamente, o UE executa o procedimento de registo e autenticação, permitindo ao CN5G validar a sua identidade e criar o respetivo contexto de mobilidade e segurança.
- Finalmente, é estabelecida uma sessão PDU, responsável pela criação do plano de utilizador e pelo encaminhamento do tráfego entre o UE e a rede de dados.

Os procedimentos descritos nesta secção serão posteriormente observados durante a implementação experimental da rede baseada na plataforma OAI, sendo analisadas as respetivas mensagens de sinalização através da ferramenta Wireshark.

2.6.1 Estabelecimento da ligação do gNB ao CN5G

Após a sua inicialização, o gNB deve estabelecer uma ligação de sinalização com o CN5G antes de poder disponibilizar serviços ao UE. Este procedimento é realizado através da interface N2, utilizando o NG *Application Protocol* (NGAP), responsável pela troca de mensagens de controlo entre a RAN e o núcleo de rede. O primeiro procedimento executado corresponde ao NG Setup, durante o qual o gNB envia à AMF uma mensagem NG *Setup Request*, contendo informações relativas à sua identificação, às células configuradas, às *Tracking Areas* (TAs) suportadas e às capacidades disponibilizadas pela estação base. Após a validação destas informações, a AMF responde com uma mensagem NG *Setup Response*, confirmando o estabelecimento da ligação N2 e disponibilizando os parâmetros necessários para a comunicação entre ambas as entidades.

A conclusão deste procedimento permite que o gNB seja reconhecido pelo CN5G, passando a integrar a infraestrutura da rede e ficando apto a suportar os procedimentos subsequentes de registo dos equipamentos do utilizador e de estabelecimento das sessões de comunicação.

A Figura 2-5 apresenta uma representação simplificada do procedimento NG *Setup*, ilustrando a troca das mensagens NG *Setup Request* e NG *Setup Response* entre o gNB e a AMF, através da interface N2.

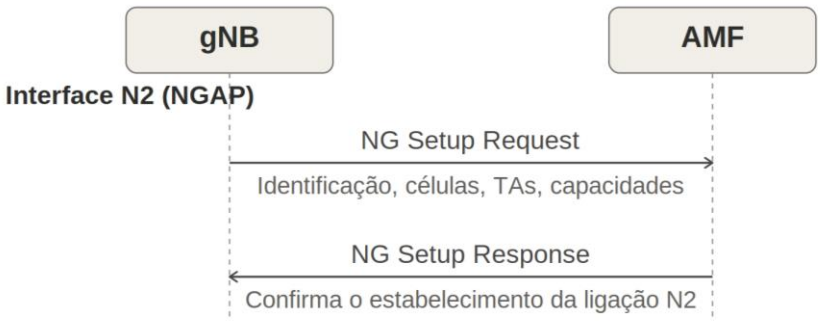


Figura 2-5: Diagrama simplificado do procedimento NG Setup entre o gNB e o CN5G

2.6.2 Procedimento de registo e autenticação do UE

O procedimento de registo do UE tem como principal objetivo permitir que o dispositivo seja reconhecido e autorizado a utilizar os serviços disponibilizados pela rede 5G. Após o envio da mensagem *Registration Request*, a AMF inicia o processo de autenticação do utilizador, recorrendo às informações de subscrição armazenadas no UDM e às funções de autenticação disponibilizadas pela AUSF.

Concluída a autenticação com sucesso, é executado o procedimento de estabelecimento do contexto de segurança, através da troca das mensagens *Security Mode Command* e *Security Mode Complete*, garantindo a ativação dos mecanismos de proteção da sinalização NAS entre o UE e o CN5G. Por fim, a AMF envia a mensagem *Registration Accept*, confirmando que o equipamento foi registado com sucesso na rede.

A conclusão deste procedimento permite a criação do contexto de mobilidade do utilizador no CN5G, constituindo um requisito fundamental para o estabelecimento posterior das sessões PDU e para a utilização dos serviços disponibilizados pela rede 5G SA.

A Figura 2-6 apresenta um diagrama simplificado do procedimento de registo e autenticação do UE, ilustrando a sequência das principais mensagens trocadas entre o UE, o gNB, a AMF e o UDM durante este processo.

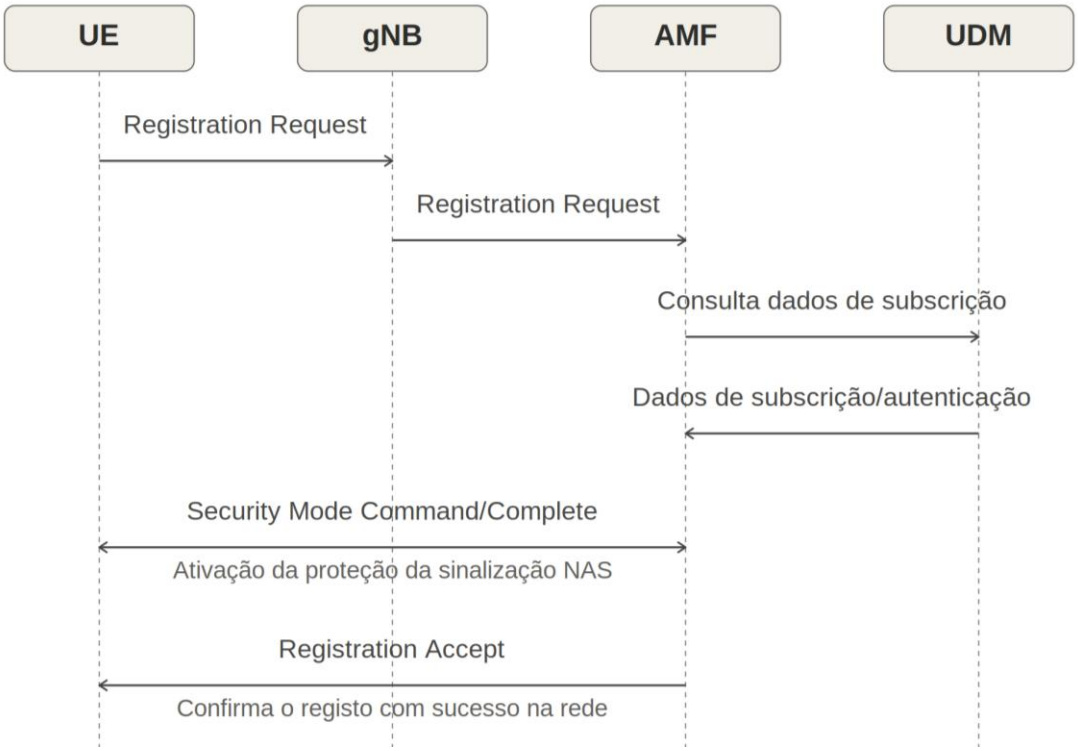


Figura 2-6: Diagrama simplificado do procedimento de registo e autenticação do UE

2.6.3 Procedimento de estabelecimento da sessão PDU

O procedimento de registo do UE permite o acesso à rede e a criação do contexto de mobilidade no CN5G. No entanto, este procedimento não estabelece, por si só, um caminho para o transporte de dados do utilizador. Para que a comunicação de dados possa ser efetuada, é necessário executar o procedimento de estabelecimento da sessão PDU (*PDU Session Establishment*).

Este procedimento é iniciado pelo UE através da mensagem *PDU Session Establishment Request*, transportada pela sinalização NAS até à SMF por intermédio da AMF. A SMF é responsável pela criação da sessão PDU, pela atribuição de um endereço IP ao equipamento e pela seleção da UPF que irá suportar o encaminhamento do tráfego do plano de utilizador. Após a configuração da sessão, a SMF coordena o estabelecimento do túnel GTP-U (GPRS *Tunnelling Protocol – User Plane*) entre o gNB e a UPF, através da interface N3. Este túnel constitui o mecanismo responsável pelo transporte do tráfego do plano de utilizador entre a RAN e a rede de dados externa. Concluído este procedimento,

a sessão PDU torna-se ativa, permitindo ao UE dispor de conectividade IP e estabelecer comunicações de dados através da rede 5G SA.

A Figura 2-7 apresenta um diagrama simplificado do procedimento de estabelecimento da sessão PDU, ilustrando a sequência das principais mensagens trocadas entre o UE, o gNB, a AMF, a SMF e a UPF, bem como o estabelecimento do túnel GTP-U através da interface N3.

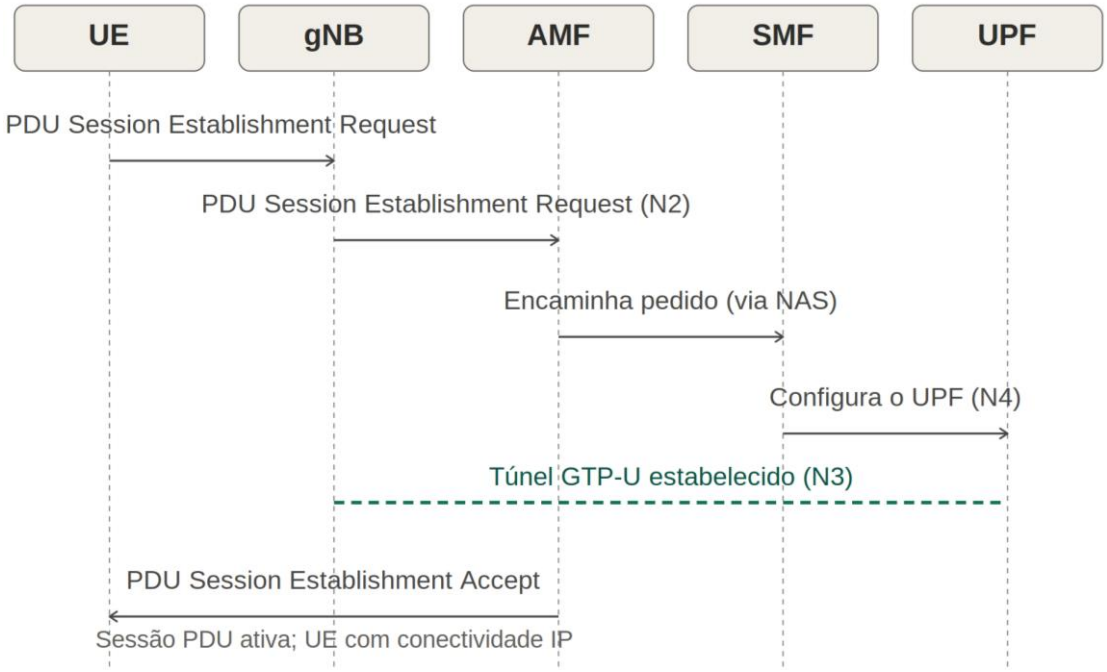


Figura 2-7: Diagrama simplificado do procedimento de estabelecimento da Sessão PDU

2.7 Segurança na Rede 5G NR

2.7.1 Arquitetura de Segurança

A arquitetura de segurança do sistema 5G NR é especificada pelo 3GPP na norma TS 33.501[13], que define os mecanismos de autenticação, os procedimentos de gestão de chaves e a proteção da sinalização e do tráfego de utilizador entre o UE, a RAN e o CN5G. Face ao 4G LTE, esta norma introduz mecanismos de ocultação da identidade permanente do subscritor e uma hierarquia de chaves mais robusta, aspetos detalhados, respetivamente, nas secções 2.7.4 e 2.7.6.

2.7.2 Funções de hash

Uma função de hash (h()) gera, a partir de uma mensagem de tamanho arbitrário, um resumo de tamanho fixo, sensível a qualquer alteração da mensagem original. Verifica a integridade dos dados, mas não a origem: é uma função pública, sem segredo, pelo que qualquer entidade, incluindo um atacante, a pode calcular.

2.7.3 MAC e assinatura digital

Um MAC (*Message Authentication Code*) resolve essa limitação, combinando a mensagem com uma chave secreta partilhada K, de forma que só quem possui essa chave consegue gerar ou verificar um MAC válido, garantindo simultaneamente integridade e autenticidade da origem. No 5G NR, os algoritmos de integridade (NIA1, NIA2, NIA3) usam

uma construção baseada em cifras de bloco, designada CMAC, e não uma construção baseada em *hash*, por vezes chamada HMAC; o princípio de segurança mantém-se: só quem detém a chave secreta gera ou verifica o código. É este mecanismo que sustenta o campo MAC-I observado nas mensagens de sinalização analisadas na secção 3.10.

Uma assinatura digital garante os mesmos dois objetivos através de criptografia assimétrica: o emissor assina com a chave privada, e qualquer recetor verifica com a chave pública correspondente. A vantagem face ao MAC é o não-repúdio, já que só o dono da chave privada podia ter produzido a assinatura. Em contrapartida, é bastante mais lenta, por assentar em exponenciação modular em vez de operações simétricas.

O 5G NR usa predominantemente MAC, não assinaturas digitais, por razões de desempenho: a integridade é verificada em tempo real a cada PDU, com latências na ordem dos microssegundos (secção 3.9.9). As assinaturas digitais ficam reservadas a cenários pontuais, como a autenticação de certificados nas interfaces do core (secção 2.3).

2.7.4 Privacidade

Comparativamente ao 4G LTE, o 5G introduz reforços significativos ao nível da privacidade do utilizador, dos quais se destaca, para efeitos do presente trabalho, a proteção da identidade permanente do subscritor durante o procedimento de registo inicial na rede. Esta proteção de identidade do subscritor assenta na utilização de três identificadores distintos, designadamente o SUPI, SUCI e o GUTI. Cada um destes identificadores corresponde a uma fase diferente do ciclo de vida da identificação do UE na rede, conforme se descreve detalhadamente nas subsecções seguintes. A Figura 2-8 ilustra de forma simplificada a relação entre estes três identificadores ao longo do ciclo de identificação do UE na rede, evidenciando a transição entre a identidade permanente, a sua forma cifrada e o identificador temporário atribuído após o registo. Uma explicação mais detalhada para cada um destes identificadores e a sua relação é providenciada nas próximas subsecções.

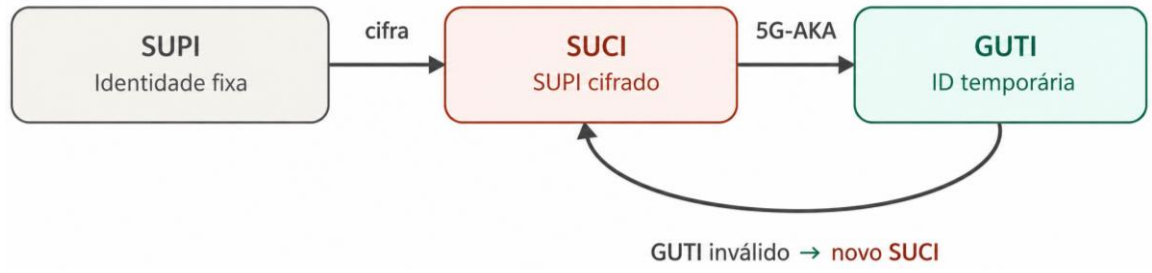


Figura 2-8: Diagrama simplificado da transição entre o SUPI, o SUCI e o GUTI durante o procedimento de registo do UE

2.7.4.1 SUPI

O SUPI constitui o identificador permanente e único do subscritor no sistema 5G, desempenhando uma função equivalente à do IMSI (*International Mobile Subscriber Identity*) utilizado nas gerações anteriores. Este identificador encontra-se armazenado de forma segura no USIM (*Universal Subscriber Identity Module*) do UE e na função UDM do CN5G, não devendo, em condições normais de funcionamento, ser transmitido em claro através da interface rádio.

Na sua forma mais comum, correspondente ao SUPI baseado em IMSI, o identificador é constituído pelos seguintes campos:

- MCC (*Mobile Country Code*), que identifica o país da rede de origem do subscritor;
- MNC (*Mobile Network Code*), que identifica o operador da rede de origem;
- MSIN (*Mobile Subscription Identification Number*), que identifica de forma única o subscritor dentro da rede do operador.

A título ilustrativo, considerando os valores fictícios MCC igual a 001, MNC igual a 01 e MSIN igual a 0000000001, obtém-se o SUPI 001010000000001.

A combinação do MCC com o MNC corresponde ao PLMN (*Public Land Mobile Network*), o identificador que designa de forma única a rede móvel de origem do subscritor, ficando este valor gravado no USIM através de campos como o *Home PLMN selector* e o *PLMN selector*, que definem os PLMNs prioritários para tentativa de registo [30]. É com base nestes valores que o UE decide em que redes pode tentar registar-se, pelo que a alteração do PLMN de uma rede exige a atualização correspondente destes campos no USIM, como se verifica experimentalmente na secção 3.12.

O 3GPP prevê ainda um formato alternativo, baseado em NAI (*Network Access Identifier*), tipicamente utilizado em cenários de acesso não 3GPP ou em redes privadas, o qual não é, contudo, utilizado no âmbito deste trabalho.

Dado que o SUPI identifica de forma inequívoca e permanente o subscritor, a sua transmissão em claro pela interface rádio constitui um risco de privacidade relevante. Um atacante equipado com uma estação base fraudulenta, comummente designada por *IMSI catcher*, poderia capturar este identificador e associar a identidade real de um utilizador à sua localização, vulnerabilidade amplamente documentada nas redes 2G, 3G e 4G. É precisamente para eliminar esta exposição que o 5G introduz o SUCI, descrito na subsecção seguinte.

2.7.4.2 SUCI

O SUCI corresponde à versão cifrada do SUPI, constituindo o identificador efetivamente transmitido pelo UE através da interface rádio durante o procedimento de registo inicial, sempre que este não possua ainda um GUTI válido atribuído pela rede.

O SUCI é gerado localmente pelo UE, mais concretamente pelo USIM, recorrendo ao esquema ECIES (*Elliptic Curve Integrated Encryption Scheme*). Este esquema utiliza a chave pública da rede de origem, previamente aprovisionada no USIM pelo operador. Importa referir que apenas a componente do identificador que individualiza o subscritor, o MSIN, é sujeita a cifra. A componente relativa à rede de origem, composta pelo MCC e pelo MNC, permanece em claro, uma vez que é necessária ao encaminhamento correto da mensagem até à rede de origem do subscritor.

O SUCI é estruturado nos seguintes campos, mantidos na sua designação original da norma:

- *SUPI Type*, que indica se o SUPI subjacente é baseado em IMSI ou em NAI;
- *Routing Indicator*, valor atribuído pelo operador para encaminhar o pedido até à instância correta da função de decifração;
- *Protection Scheme Identifier*, que identifica o esquema de cifra utilizado, podendo corresponder ao *Profile A*, ao *Profile B* ou ao *Null-scheme*;
- *Home Network Public Key Identifier*, que identifica qual a chave pública da rede de origem utilizada na cifra;

- *Scheme Output*, correspondente ao resultado da cifra ECIES aplicada ao MSIN.

A Tabela 2:9 compara os três esquemas de proteção do SUCI definidos pelo 3GPP, situando o *Null-scheme*, utilizado no presente trabalho, face às alternativas empregues em redes de produção.

Tabela 2:9 Esquemas de proteção do SUCI

Esquema	Descrição	Utilização típica
Null-scheme	O MSIN é transmitido sem qualquer cifra, ou seja, o SUCI corresponde, na prática, ao próprio SUPI em claro.	Cenários de teste e depuração; plataformas experimentais como a OAIBOX™.
Profile A	O MSIN é cifrado através de ECIES, utilizando a curva elíptica Curve25519.	Redes de produção, como esquema de proteção por omissão em muitas implementações comerciais.
Profile B	O MSIN é cifrado através de ECIES, utilizando a curva elíptica secp256r1 (NIST P-256).	Redes de produção, como alternativa ao *Profile* A, nomeadamente em implementações que sigam recomendações do NIST.

O 3GPP prevê ainda o *Null-scheme*, mecanismo no qual o MSIN é transmitido sem qualquer cifra. Este esquema encontra-se previsto exclusivamente para cenários de teste e depuração, não sendo recomendado em redes de produção. Este aspeto assume particular relevância no presente trabalho, uma vez que, em ambientes experimentais como o baseado na plataforma OAIBOX™, é frequente que o *Null-scheme* se encontre ativo por definição. Esta circunstância permitirá, na secção 3.10 do capítulo 3 dedicado à experimentação laboratorial, verificar diretamente, através da captura efetuada com o Wireshark, se o identificador presente na mensagem *Registration Request* corresponde a um SUCI genuinamente cifrado ou a um SUPI transmitido em claro sob este esquema.

Ao receber o SUCI, a AMF encaminha-o para a AUSF, que, por sua vez, solicita à função UDM, mais concretamente à sua subfunção SIDF (*Subscription Identifier De-concealing Function*), que decifre o identificador. A SIDF utiliza a chave privada correspondente da rede de origem para decifrar o SUCI através do algoritmo ECIES e recuperar o SUPI original. Este processo de decifração ocorre inteiramente no lado da rede, não sendo o SUPI, em circunstância alguma, reconstituído ou exposto na interface rádio.

2.7.4.3 GUTI

Após o processo de registo e o estabelecimento do contexto de segurança se concluírem com sucesso, conforme descrito na secção 2.6.2, a AMF atribui ao UE um identificador temporário, designado por 5G-GUTI, enviado através da mensagem *Registration Accept*. A partir deste momento, o UE passa a utilizar o GUTI, em vez do SUCI ou do SUPI, em todas as interações subsequentes de sinalização, nomeadamente nos procedimentos de atualização periódica de registo, nos pedidos de serviço (*Service Request*) e na paginação (*Paging*).

O 5G-GUTI é constituído por duas componentes principais:

- GUAMI (*Globally Unique AMF Identifier*), que identifica de forma única a instância de AMF que atribuiu o identificador, sendo composto pelo MCC, pelo MNC, pela AMF *Region ID*, pela AMF *Set ID* e pela AMF *Pointer*;

- 5G-TMSI (*5G Temporary Mobile Subscriber Identity*), identificador temporário, único no contexto da AMF que o atribuiu, que substitui, na prática, a necessidade de expor o SUPI ou o SUCI nas comunicações subsequentes.

O GUTI é periodicamente reatribuído pela rede através do procedimento de *GUTI Reallocation*, com o objetivo de limitar a possibilidade de um atacante correlacionar múltiplas sessões de sinalização com o mesmo utilizador ao longo do tempo. Caso o UE se desloque para uma área geográfica servida por uma AMF distinta, incapaz de resolver o GUTI anteriormente atribuído, ou caso o UE perca o contexto de segurança associado, por exemplo após um período prolongado de inatividade, a rede solicita novamente a identificação através do SUCI, reiniciando o ciclo descrito na subsecção seguinte.

A Tabela 2:10 sintetiza as principais diferenças entre os três identificadores apresentados nesta secção, quanto à sua natureza, ao momento de utilização e à proteção de privacidade que cada um assegura.

Tabela 2:10 Comparação entre SUPI, SUCI e GUTI

Identificador	Natureza	Momento de utilização	Proteção de privacidade associada
SUPI	Permanente	Armazenado no USIM e na UDM; nunca transmitido em claro pela interface rádio em condições normais.	Nenhuma por si só; depende inteiramente de nunca ser exposto diretamente.
SUCI	Temporário (gerado a cada nova tentativa de registo)	Transmitido pelo UE na mensagem *Registration Request*, sempre que não existe um GUTI válido.	Cifra do MSIN através de ECIES (exceto sob *Null-scheme*), impedindo a associação direta ao subscritor.
GUTI	Temporário (reatribuído periodicamente pela AMF)	Utilizado em todas as interações de sinalização subsequentes ao registo, incluindo atualizações periódicas, *Service Request* e *Paging*.	Substitui a necessidade de expor o SUPI ou o SUCI; limita a correlação de sessões ao longo do tempo.

2.7.5 Procedimento Integrado de Identificação e Autenticação do UE

Para consolidar a relação entre os três identificadores, descreve-se de seguida o fluxo típico de identificação de um UE que acede pela primeira vez à rede.

1. Numa primeira fase, o UE liga-se sem possuir um GUTI válido armazenado localmente, situação que ocorre, por exemplo, numa primeira ligação ou após o reinício do dispositivo com um contexto de segurança expirado. Não podendo transmitir o SUPI em claro, o UE cifra o MSIN localmente com a chave pública da rede de origem, através do esquema configurado, seja o *Profile A*, o *Profile B* ou o *Null-scheme*, obtendo o SUCI e enviando-o na mensagem *Registration Request*. Esta mensagem é transportada pela sinalização NAS através da interface Uu e, posteriormente, pelo protocolo NGAP através da interface N2, até à AMF.
2. Numa segunda fase, a AMF encaminha o SUCI para a AUSF, que solicita à UDM, através da função SIDF, que decifre o identificador, permitindo recuperar o SUPI original. Com base neste identificador, a AUSF e a UDM executam o procedimento de autenticação 5G-AKA (*5G Authentication and Key Agreement*),

derivando a hierarquia de chaves de segurança necessária à proteção da sinalização NAS e da sinalização AS (*Access Stratum*). Concluída a autenticação, é estabelecido o contexto de segurança, através da troca das mensagens *Security Mode Command* e *Security Mode Complete*, já descritas na secção 2.6.2.

3. Numa terceira e última fase, a AMF atribui um novo 5G-GUTI ao UE, enviado na mensagem *Registration Accept*. Enquanto este identificador permanecer válido e reconhecido pela mesma AMF, o UE passa a identificar-se exclusivamente através do GUTI nas interações subsequentes, evitando expor novamente o SUCI ou o SUPI.

A Figura 2-9 sintetiza estas três fases, ilustrando a sequência de mensagens trocadas entre o UE, o gNB, a AMF, a AUSF e a UDM ao longo de todo o procedimento.

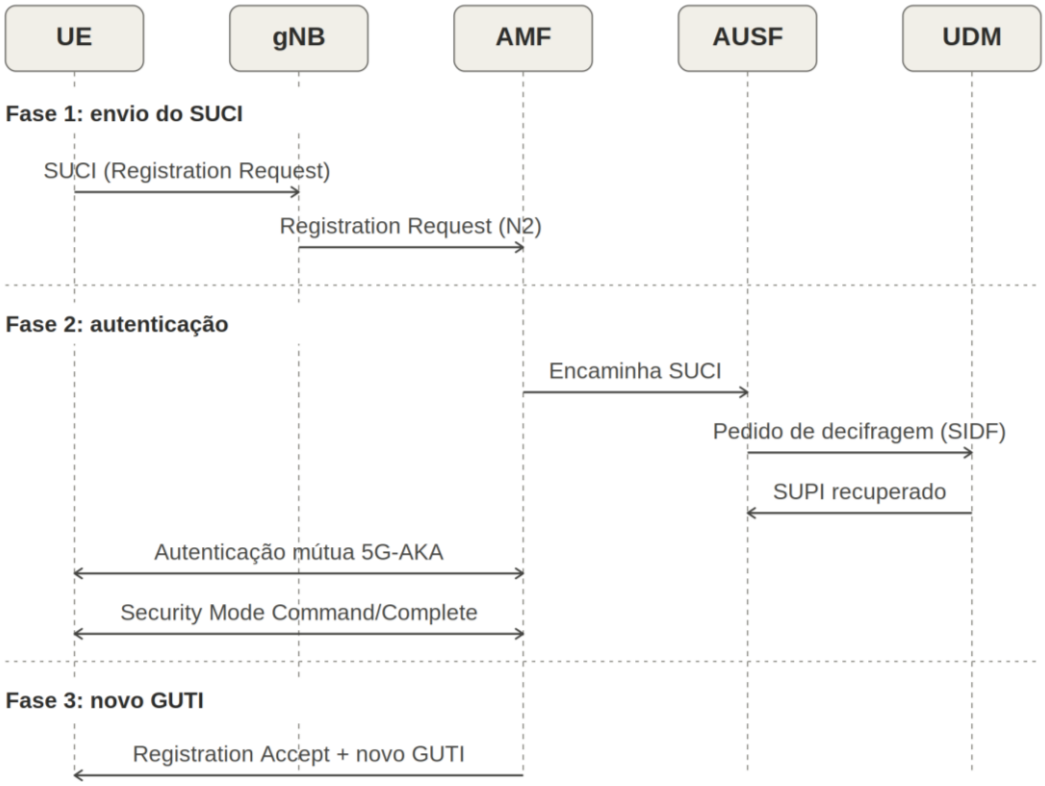


Figura 2-9: Diagrama simplificado do fluxo de identificação e autenticação do UE

Este fluxo evidencia o princípio central da privacidade do utilizador nas redes 5G. A identidade permanente do subscritor, representada pelo SUPI, só é exposta, e sempre sob forma cifrada através do SUCI, no momento estritamente necessário do primeiro contacto com a rede. Todas as interações subsequentes recorrem a um identificador temporário e substituível, o GUTI, minimizando a janela de exposição da identidade real do subscritor.

2.7.6 Gestão e Hierarquia de Chaves

A segurança do sistema 5G NR assenta numa hierarquia de chaves derivadas sucessivamente a partir de uma chave permanente e secreta, partilhada exclusivamente entre o USIM do UE e a função UDM da rede. Esta abordagem, especificada na norma TS 33.501[13], garante que cada entidade da rede recebe apenas as chaves estritamente

necessárias às suas funções, limitando o impacto de um eventual comprometimento a um único domínio de segurança.

2.7.6.1 Chaves de segurança e sua hierarquia

A chave permanente do subscritor, designada por **K**, encontra-se armazenada de forma segura no USIM e na base de dados de credenciais da UDM (*Authentication credential Repository and Processing Function* - ARPF), nunca sendo transmitida através da rede. A partir desta chave, e no âmbito do procedimento de autenticação 5G-AKA, já descrito na secção 2.7.5, deriva-se sucessivamente a seguinte hierarquia de chaves:

- CK, IK, (*Cipher Key*, *Integrity Key*) chaves de cifra e de integridade, derivadas de K através do algoritmo *Milenage*, constituindo a base de toda a hierarquia subsequente;
- K_AUSF, derivada tanto pelo UE como pela AUSF a partir de CK e IK, vinculada ao nome da rede servidora, impedindo a sua reutilização noutra rede;
- K_SEAF, (chave da função *Security Anchor Function* - SEAF) derivada pela AUSF a partir de K_AUSF, e entregue à SEAF, co-localizada com a AMF na rede servidora;
- K_AMF, derivada a partir de K_SEAF, constituindo a chave-raiz de todas as chaves de segurança do estrato de acesso (AS) e do estrato de não-acesso (NAS);
- K_NASint, K_NASenc derivadas de K_AMF, utilizadas para proteger, respetivamente, a integridade e a confidencialidade da sinalização NAS entre o UE e a AMF;
- K_gNB derivada de K_AMF, entregue ao gNB no momento do estabelecimento do contexto de segurança, constituindo a chave-raiz da segurança da interface rádio;
- K_RRCint, K_RRCenc, K_UPint, K_UPenc derivadas de K_gNB, utilizadas para proteger, respetivamente, a integridade e a confidencialidade da sinalização RRC e do tráfego do Plano de Utilizador.

Esta estrutura hierárquica assegura que um eventual comprometimento de uma chave de nível inferior (por exemplo, a K_gNB) não permite reconstituir as chaves de nível superior (K_AMF, K_SEAF ou K_AUSF), uma vez que a derivação de chaves é unidirecional.

2.7.6.2 Gestão de chaves

A gestão do ciclo de vida destas chaves inclui procedimentos de atualização e renovação, com destaque para dois mecanismos previstos pela norma TS 33.501:

- Derivação vertical de chaves, executada sempre que o UE efetua um novo procedimento de autenticação 5G-AKA (por exemplo, após um registo inicial), gerando uma nova hierarquia de chaves a partir de K_AMF;
- Derivação horizontal de chaves, executada durante procedimentos de mobilidade entre estações base (*handover*), na qual uma nova K_gNB é derivada a partir da K_gNB anterior, ou de K_AMF em determinados cenários, sem necessidade de reautenticação completa do UE, garantindo continuidade de serviço com segurança preservada. Esta derivação horizontal aplica-se especificamente a um *handover* intra-AMF; num handover inter-AMF, dado que a K_AMF está vinculada à instância específica da AMF, é necessário recalcular toda a cadeia a partir desta chave,

incluindo a K_NASenc, a K_NASint e a K_gNB, através de transferência de contexto pela interface N14 ou, em casos mais extremos, de reautenticação completa.

A gestão adequada desta hierarquia é particularmente relevante no contexto experimental do presente trabalho, uma vez que a correta derivação e ativação das chaves K_NASint, K_NASenc, K_RRCint e K_RRCenc pode ser verificada diretamente através da observação das mensagens *Security Mode Command* e *Security Mode Complete*, capturadas por Wireshark nos ensaios descritos na secção 3.10.

2.8 Indicadores de Desempenho (KPI) em Redes 5G NR

A avaliação experimental de uma rede 5G NR depende da recolha sistemática de indicadores-chave de desempenho (KPI) medidos ao nível rádio e reportados quer pelo gNB quer pelo UE. Estes indicadores são a base de leitura dos resultados obtidos nos ensaios laboratoriais descritos no capítulo 3, pelo que a sua definição precisa é indispensável antes de qualquer análise. As definições e a terminologia associada seguem a especificação de medições da camada física do 5G NR.

2.8.1 Definição dos Principais KPI Rádio

Tabela 2:11 Principais KPI rádio utilizados na avaliação experimental.

KPI	Designação	Descrição
RSSI	*Received Signal Strength Indicator*	Potência total recebida na banda de medição (sinal útil e interferência e ruído), utilizada internamente no cálculo do RSRQ.
RSRP	*Reference Signal Received Power*	Potência média recebida dos sinais de referência transmitidos pela estação base; principal indicador de cobertura.
RSRQ	*Reference Signal Received Quality*	Qualidade do sinal recebido, combinando a potência do sinal útil (RSRP) com o nível total de interferência e ruído no canal (RSSI).
SINR	*Signal-to-Interference-plus-Noise Ratio*	Relação entre a potência do sinal útil e a soma da interferência e do ruído; indicador determinante do débito alcançável.
CQI	*Channel Quality Indicator*	Indicador reportado pelo UE que reflete a qualidade instantânea do canal rádio, utilizado pelo gNB para a adaptação da modulação e codificação, ou adaptação de ligação.
MCS	*Modulation and Coding Scheme*	Combinação de esquema de modulação e taxa de codificação utilizada na transmissão, selecionada em função do CQI reportado.
BLER	*Block Error Rate*	Proporção de blocos de transporte recebidos com erro face ao total transmitido; reflete a fiabilidade da ligação e a eficácia da retransmissão automática híbrida.
RI	*Rank Indicator*	Número de camadas de transmissão (*streams*) que o UE recomenda para multiplexagem espacial, com base no *rank* instantâneo do canal MIMO.

Para além da definição conceptual apresentada na Tabela 2:11, apresenta-se de seguida a formulação matemática de cada indicador, com base nas definições técnicas documentadas na plataforma experimental utilizada, empregues no cálculo dos resultados apresentados no capítulo 3.

- O RSSI mede a potência média linear do sinal total recebido, por símbolo OFDM configurado e na largura de banda de medição, incluindo a potência da célula servidora, das células adjacentes, da interferência de canal e do ruído térmico:

$$RSSI = \frac{1}{N_{symb}} \sum_{l=1}^{N_{symb}} \sum_{r=1}^{N_{RB}} \sum_{k=1}^{N_{sc}^{RB}} | s_{l,r,k} |^2 \quad (2.1)$$

, onde N_{symb} é o número de símbolos OFDM usados na medição, $N_{sc}^{RB} = 12$ é o número de subportadoras por bloco de recursos (RB), e $s_{l,r,k}$ é o sinal recebido no símbolo OFDM l, bloco de recursos r e subportadora k. Em dBm:

$$RSSI_{dBm} = 10\log_{10}\left(\frac{RSSI\,[W]}{10^{-3}}\right) \quad (2.2)$$

- O RSRP mede a potência média linear recebida de um sinal de referência específico da célula, por elemento de recurso (RE):

$$RSRP = \frac{1}{N_{symb} N_{RB}} \sum_{l=1}^{N_{symb}} \sum_{k=1}^{N_{RE}} | s_{l,k} |^2 \quad (2.3)$$

, onde N_{RE} é o número total de elementos de recurso que efetivamente contêm o sinal de referência. Em dBm:

$$RSRP_{dBm} = 10\log_{10}\left(\frac{RSRP\,[W]}{10^{-3}}\right) \quad (2.4)$$

- O RSRQ combina o RSRP com o RSSI para refletir a qualidade do canal, incluindo o efeito da interferência:

$$RSRQ_{dB} = RSRP_{dBm} - RSSI_{dBm} + 10\log_{10}(N_{RB}) \quad (2.5)$$

- O SINR representa a razão entre a potência do sinal útil e a soma da interferência com o ruído:

$$SINR = \frac{S}{N + I} \quad (2.6)$$

onde S é a potência do sinal útil, N é a potência do ruído e I é a potência da interferência de outros sinais medidos.

- O CQI é reportado pelo UE numa escala de 0 a 15, permitindo ao gNB estimar a relação sinal-ruído alcançável e selecionar o MCS adequado. Os valores seguem tabelas normalizadas pelo 3GPP (64QAM, 256QAM e de baixa eficiência espectral), associando a cada índice uma modulação, uma taxa de codificação e uma eficiência espectral correspondente.

- O MCS é selecionado pelo gNB a partir de uma tabela normalizada, sinalizado ao UE através do PDCCH, definindo a combinação entre o esquema de modulação e a taxa de codificação a aplicar na transmissão, com base no CQI reportado.
- O BLER representa a proporção de blocos de transporte recebidos com erro:

$$BLER = \frac{N_{TB,err}}{N_{TB}} \tag{2.7}$$

onde $N_{TB,err}$ é o número de blocos de transporte recebidos com erro (deteção falhada pelo CRC) e N_{TB} é o número total de blocos transmitidos.

O RI é reportado pelo UE como parte do *Channel State Information* (CSI), indicando o número de camadas de transmissão que o canal rádio suporta com qualidade adequada nesse instante, com base no *rank* instantâneo do canal MIMO. O gNB usa este valor para decidir o número de camadas efetivamente transmitidas, não podendo exceder nem o RI reportado nem o número de antenas disponíveis em ambos os extremos da ligação [26].

- Embora não constitua um KPI rádio reportado diretamente pela interface, a taxa de transmissão (*throughput*) é calculada experimentalmente a partir do BLER e do *bitrate* configurado, sendo por isso apresentada como métrica complementar de análise.

$$Throughput = (1 - BLER) \times bitrate \tag{2.8}$$

- sendo o *bitrate* definido como o número total de bits transferidos por unidade de tempo:

$$bitrate = \frac{\sum_{i=1}^{N_{TB}} b_i}{\Delta T} \tag{2.9}$$

onde b_i é o número de bits de cada bloco de transporte i, transferidos num intervalo de tempo ΔT.

2.8.2 Modelos de propagação e cálculo teórico dos KPI

Apresentam-se os modelos analíticos utilizados para estimar teoricamente os KPI medidos nos ensaios laboratoriais, confrontando-os com os valores obtidos experimentalmente. O RSRP e o *bitrate* admitem um cálculo teórico direto; o SINR e o CQI admitem apenas uma aproximação, na forma de um limite teórico; o RSRQ e o BLER não são calculados, pelas limitações indicadas adiante.

2.8.2.1 RSRP teórico

O RSRP teórico resulta da perda de percurso em espaço livre entre o gNB e o UE, dada pela equação de Friis:

$$PathLoss_{Friis,dB} = 20\log_{10}(d) + 20\log_{10}\left(f_{c,GHz}\right) + 32{,}44 \tag{2.10}$$

$$RSRP_{teo,dBm} = EIRP_{RE,dBm} - PathLoss_{Friis,dB} + G_{UE,dB} \tag{2.11}$$

onde d é a distância entre o gNB e o UE, em metros, $f_{c,GHz}$ a frequência central da portadora, em GHz, $G_{UE,dB}$ o ganho de antena do UE, e $EIRP_{RE,dBm}$ a potência irradiada por elemento de recurso, calculada em cada laboratório a partir da largura de banda utilizada.

2.8.2.2 Bitrate teórico

O limite teórico de *bitrate* é dado pela capacidade de Shannon:

$$C = BW \times \log_2(1 + SINR) \tag{2.12}$$

onde BW é a largura de banda ocupada, em Hz, e $SINR$ o valor medido, em escala linear.

2.8.2.3 Bitrate teórico por alocação de slots TDD

Em complemento ao limite de Shannon (secção 2.8.2.2), o manual da OAIBOX™ [25] propõe um modelo mais específico, baseado na quantidade de dados transportada por bloco de recurso em cada *slot*, segundo o MCS assumido. A eficiência espectral de uma modulação resulta do produto entre o número de bits por símbolo (M) e a taxa de codificação (R):

$$SE = M \times R \tag{2.13}$$

Para o MCS 27 (256QAM, $M = 8$), com a taxa de codificação máxima normativa de $R = 0{,}925$, obtém-se:

$$\begin{aligned} SE &= 8 \times 0{,}925 = 7{,}4063 \text{ bits/símbolo} \\ D_{RB,slot} &= 12 \times 11 \times 7{,}4063 \approx 978 \text{ bits} \end{aligned} \tag{2.14}$$

, onde 12 é o número de subportadoras por bloco de recurso e 11 o número de símbolos OFDM disponíveis para dados por *slot* (dos 14 totais, descontando os símbolos reservados aos sinais de referência para demodulação, DMRS (*Demodulation Reference Signal*), e ao canal de controlo PDCCH). O *bitrate* teórico para uma direção (DL ou UL) resulta de:

$$\text{Bitrate}_{dir} = \frac{D_{RB,slot} \times N_{RB} \times N_{slots,dir}}{10^6} \text{ Mbps} \tag{2.15}$$

onde $N_{slots,dir}$ é o número de *slots* por segundo atribuídos a essa direção, segundo a configuração TDD. Para uma configuração com período de 5 *slots* (ex: DDDFU ou DDFUU), o total de 2000 *slots*/segundo (numerologia μ=1) reparte-se proporcionalmente pelo número de *slots* D e U de cada padrão, considerando o *slot* especial (F, estrutura 4:6:4 símbolos DL: guarda: UL) contabilizado integralmente do lado do *downlink*, dado o reduzido peso dos seus símbolos de *uplink* face à capacidade total.

2.8.2.4 Capacidade teórica MIMO

Para uma configuração MIMO com múltiplos fluxos espaciais independentes, o limite teórico de Shannon apresentado na secção 2.8.2.2 generaliza-se através do número de camadas espaciais (*rank*) transmitidas:

$$C_{MIMO,teo} = N_{layers} \times BW \times \log_2(1 + SINR) \tag{2.16}$$

onde N_{layers} é o número de camadas espaciais (*rank*) da transmissão, e BW e $SINR$ mantêm o significado já apresentado. Este modelo assume fluxos espaciais ortogonais e SINR idêntico em cada camada, uma simplificação que ignora a correlação entre antenas e a partilha de recursos de sinalização entre camadas, mas que permite estabelecer um limite de referência para o ganho de capacidade esperado com a multiplexagem espacial.

2.8.2.5 SINR e CQI

O SINR e o CQI não admitem uma previsão teórica exata, mas sim um limite de referência, útil para avaliar a margem entre o desempenho medido e o limite físico do sistema.

O SINR, se limitado apenas pelo ruído térmico, corresponde a um limite superior ideal, sem interferência nem degradação de implementação:

$$PN_{dBm} = -174 + 10\log_{10}(BW) + NF_{dB} \tag{2.17}$$

$$SINR_{teo,dB} = RSRP_{teo,dBm} - PN_{dBm} \tag{2.18}$$

Este valor não é diretamente comparável ao SINR medido, uma vez que o recetor real satura o valor reportado no valor máximo correspondente à modulação mais exigente suportada.

O CQI resulta de tabelas de correspondência entre o SINR e o CQI, calibradas pelo fabricante do *chipset*, e não de uma equação normativa. Ainda assim, quando o SINR (medido ou teórico) é suficientemente elevado para saturar essa correspondência no valor máximo, o CQI teórico pode ser inferido por esse efeito de saturação, sem necessidade de conhecer a tabela de calibração exata.

2.8.2.6 RSRQ e BLER

A ausência de cálculo teórico para estes dois indicadores decorre de limitações específicas de cada um. O RSRQ depende do RSSI, que incorpora o nível de interferência do ambiente, uma grandeza não determinável analiticamente sem instrumentação adicional. O BLER depende da realização específica do canal e do mecanismo HARQ (*Hybrid Automatic Repeat reQuest*), exigindo um simulador de nível de ligação, fora do âmbito deste trabalho.

2.8.2.7 Estimativa do raio de célula

O desempenho de uma ligação rádio pode ser estimado através do conceito de *link budget*, que relaciona a potência transmitida com a potência recebida, contabilizando os ganhos e as perdas do percurso. Seguindo a formulação adotada no manual de laboratório da OAIBOX™ [25], baseada no 3GPP TS 36.873[24], o nível de sinal recebido em *downlink* (RxSL) é dado por:

$$RxSL_{dBm} = P_{TX,dBm} - L_{cabo,dB} + G_{gNB,dB} - PathLoss_{UMa,dB} - PenetrationLoss_{dB} + G_{UE,dB} \tag{2.19}$$

onde $P_{TX,dBm}$ é a potência de transmissão do gNB, $L_{cabo,dB}$ as perdas de cabo, $G_{gNB,dB}$ e $G_{UE,dB}$ os ganhos de antena do gNB e do UE, e $PenetrationLoss_{dB}$ a perda adicional por obstrução (ex: paredes). Para efeitos deste trabalho, considera-se $PenetrationLoss_{dB} = 0$, sendo qualquer obstrução real refletida diretamente nos valores de perda de percurso estimados a partir das medições.

A perda de percurso, para o cenário *Urban Macro* (UMa) em condição de linha de vista, é modelada por:

$$PathLoss_{UMa,dB} = 28{,}0 + 22\log_{10}(d) + 20\log_{10}(f_{c,GHz}) \tag{2.20}$$

Para garantir a qualidade da ligação, o RxSL deve exceder a sensibilidade do recetor (RxS), definida em função do ruído térmico (PN), da figura de ruído do recetor (NF) e da

relação sinal-ruído alvo (SNR), que considera apenas o ruído térmico, sem interferência, ao contrário do SINR usado nos restantes indicadores:

$$RxS_{dBm} = PN_{dBm} + NF_{dB} + SNR_{dB} \quad (2.21)$$

Igualando o RxSL à RxS, obtém-se a perda de percurso máxima admissível pela ligação e, a partir desta e da equação do modelo UMa, o raio de célula suportado por uma dada configuração.

2.8.2.8 Eficiência espectral teórica por ordem de modulação

A eficiência espectral teórica de uma transmissão corresponde ao produto entre o número de bits por símbolo da modulação e a taxa de codificação:

$$SE_{teo} = M \times R \quad (2.22)$$

onde M é o número de bits por símbolo (2, 4, 6 ou 8, para QPSK, 16QAM, 64QAM e 256QAM, respetivamente) e R a taxa de codificação, cujo valor máximo normativo (secção 2.8.2.3) é de aproximadamente 0,925.

2.8.3 Classificação Qualitativa dos KPI

Para facilitar a leitura e a interpretação dos resultados obtidos nos ensaios laboratoriais, definiu-se uma escala qualitativa de classificação para os principais indicadores rádio (RSRP, RSRQ, SINR, CQI e BLER), organizada em quatro níveis: Excelente, Bom, Aceitável e Pobre, apresentada na Tabela 2:12. Os limiares adotados baseiam-se em valores de referência habitualmente utilizados na indústria e na literatura técnica para redes 4G/5G[16], servindo como referência de leitura transversal a todos os ensaios realizados, e não como limiares normativos do 3GPP.

Tabela 2:12 Escala qualitativa de classificação dos KPI rádio.

Classificação	RSRP (dBm)	RSRQ (dB)	SINR (dB)	CQI (0–15)	BLER (%)
Excelente	≥ -80	≥ -10	≥ 20	12 – 15	< 1
Bom	-90 a -80	-15 a -10	13 a 20	8 – 11	1 a 5
Aceitável	-100 a -90	-20 a -15	0 a 13	4 – 7	5 a 10
Pobre	< -100	< -20	< 0	0 – 3	> 10

3 Experimentação laboratorial

Os ensaios experimentais foram realizados no Laboratório C.7 da Escola Superior de Tecnologia (EST) da Universidade Politécnica de Castelo Branco (UPCB). Os ensaios focaram-se na variação controlada de parâmetros de configuração do gNB, permitindo avaliar o seu impacto nos indicadores de desempenho da rede, no uso da inspeção profunda de pacotes para melhor compreender o funcionamento de uma rede 5G, incluindo aspetos de segurança, e comandos de monitorização da rede core (CN5G). A lista de ensaios realizados foi a seguinte:

1. Análise do Impacto da Largura de Banda no Desempenho da Ligação 5G NR
2. Análise da alteração da Frequência Central da Portadora 5G NR
3. Alterar a Configuração de *Slots* TDD do 5G NR
4. Testar o Modo FDD
5. Alterar o Esquema de Modulação e Codificação (MCS) do 5G NR
6. Testar Configurações MIMO do 5G NR
7. Inspeção Profunda de Pacotes para melhor compreensão do 5G NR
8. Compreender a Segurança no 5G NR
9. Uso de *Network Slicing* em 5G Usando uma xApp
10. Configuração de PLMN e Programação de Cartões SIM 5G

3.1 Descrição do ambiente de experimentação utilizado

A Figura 3-1 apresenta o ambiente experimental adotado para a realização dos ensaios descritos neste trabalho. A plataforma de experimentação é constituída por uma OAIBOX™, na qual se encontra instalada a plataforma de software OAI, configurada para executar as funções do CN5G e do gNB.

A ligação da OAIBOX™ à rede da UPCB é efetuada através de uma interface Ethernet, enquanto a interface rádio é implementada por um *Universal Software Radio Peripheral* (USRP) B210, ligado à OAIBOX™ por intermédio de uma ligação USB 3.0. O USRP atua como *front-end* de rádio, realizando a conversão entre os sinais digitais processados pela plataforma OAI e os sinais de radiofrequência utilizados na comunicação sem fios.

O UE é constituído por um módulo *Quectel* RM520N-GL, ligado a um computador destinado à configuração do dispositivo e à execução dos ensaios experimentais.

Para efeitos de reprodutibilidade dos ensaios, a Tabela 3:1 sintetiza as principais especificações técnicas dos equipamentos utilizados na plataforma experimental.

Tabela 3:1 Especificações técnicas dos equipamentos utilizados

Equipamento	Função no ensaio	Especificações relevantes
OAIBOX™ MAX	Plataforma gNB + CN5G	Tecnologia 5G NR SA; bandas FR1 até 6 GHz (predefinição n41/n77/n78); largura de banda até 100 MHz; conforme 3GPP Release 15/16; EIRP (*Effective Isotropic Radiated Power*) máximo do gNB de 10 dBm; alcance até 150m em linha de vista (com antena direcional externa opcional)
USRP B210	*Front-end* de rádio (RF)	Placa SDR *National Instruments* USRP B210, externa, ligada à OAIBOX™ MAX por intermédio de uma ligação USB 3.0
Quectel RM520N-GL	Módulo UE 5G	*Chipset* Qualcomm; suporte 5G NR SA/NSA (sub-6 GHz), incluindo a banda n77; MIMO 4x4 em *downlink* e 2x2 em *uplink*; conforme 3GPP *Release* 16
PC1 e PC2	PC1: configuração e execução dos ensaios via módulo *Quectel*; PC2: acesso à *dashboard* de monitorização	Processador Intel Core i5-6300U @ 2,40 GHz; 8 GB RAM; sistema operativo de 64 bits

O cartão USIM utilizado é programável, suportando a configuração manual dos parâmetros de identificação e autenticação do subscritor exigidos pelos procedimentos de registo e segurança descritos na secção 2.7. Entre os parâmetros configuráveis incluem-se o IMSI, a chave secreta (*Key* - Ki) e os parâmetros de operador OP/OPC, utilizados no algoritmo de autenticação *Milenage*, conforme especificado pelo 3GPP para os sistemas GSM, WCDMA, LTE e NR. O cartão está disponível nos formatos destacáveis 2FF, 3FF e 4FF, e suporta tensões de alimentação de 5V, 3V e 1,8V. Por motivos de segurança, e em conformidade com os princípios de proteção da identidade do subscritor discutidos na secção 2.7, os valores reais de IMSI, Ki, OP e OPC utilizados nos ensaios não são reproduzidos neste documento.

A monitorização dos principais KPIs é efetuada através do *dashboard* disponibilizado pela OAIBOX™ [19], permitindo acompanhar a evolução dos indicadores de desempenho em tempo real durante a realização dos ensaios.

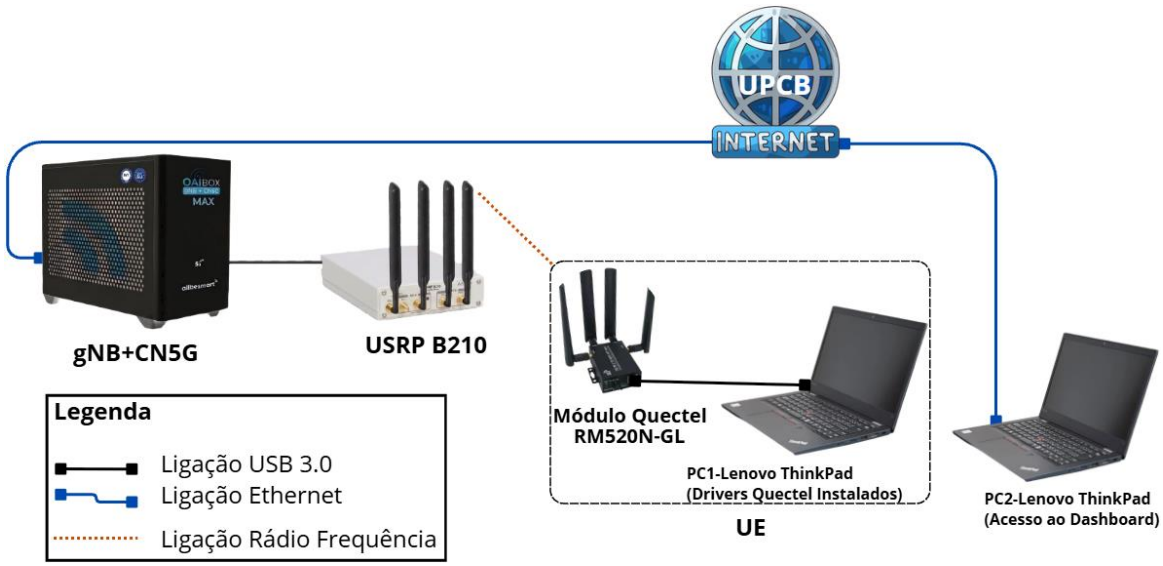


Figura 3-1: Ambiente experimental utilizado para a realização dos ensaios

3.2 Ferramentas de Medição e Análise

Para apoiar a realização dos ensaios experimentais, recorreu-se a um conjunto de ferramentas complementares de medição e análise, sintetizadas na Tabela 3:2.

Tabela 3:2 Ferramentas de medição e análise utilizadas

Ferramenta	Função no presente trabalho
Wireshark (DPI)	Captura e inspeção profunda de pacotes (*Deep Packet Inspection* - DPI) nas interfaces N2, N3 e Uu, permitindo observar os procedimentos de registo, de estabelecimento de sessão PDU e os mecanismos de segurança (secções 2.6 e 2.7).
OpenAirInterface (OAI) e plataforma OAIBOX™	Software de código aberto, conforme com as especificações do 3GPP, que implementa a RAN e o CN5G; a OAIBOX™ integra-o num sistema pré-configurado, servindo de base ao ambiente experimental (secção 3.1).

3.3 Análise do impacto da largura de banda no desempenho da ligação 5G NR

Com o objetivo de avaliar o impacto da largura de banda no desempenho da interface rádio, foram realizados dois testes experimentais em condições de linha de vista (*Line-of-Sight* - LoS), com uma distância aproximada de 2 m entre UE e o gNB. Foram avaliadas duas configurações de largura de banda, 20 MHz e 40 MHz, sendo a largura de banda o único parâmetro de configuração alterado entre os testes. Os resultados obtidos são apresentados na Figura 3-2 e na Figura 3-3.

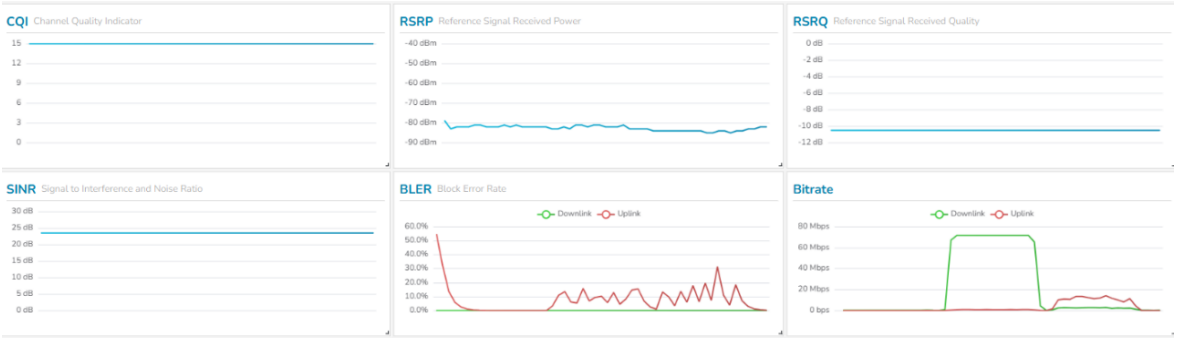


Figura 3-2: Evolução temporal dos KPIs (CQI, RSRP, RSRQ, SINR, BLER e taxa de transmissão) para uma largura de banda de 20 MHz

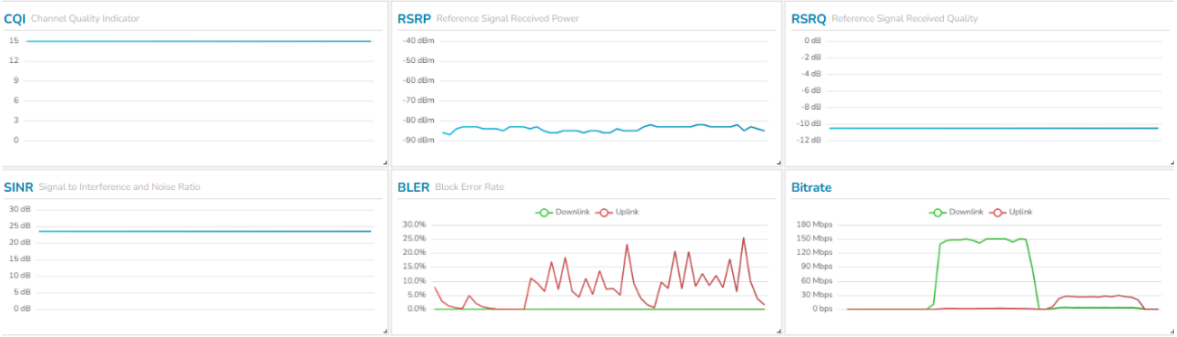


Figura 3-3: Evolução temporal dos KPIs (CQI, RSRP, RSRQ, SINR, BLER e taxa de transmissão) para uma largura de banda de 40 MHz

A análise qualitativa dos indicadores de desempenho da rede baseia-se nos limiares definidos na Tabela 2:12. Nesta base, o RSRP apresentou, por leitura aproximada dos gráficos, valores próximos de −80 dBm em ambos os testes ("Bom"), enquanto o RSRQ e o SINR se mantiveram em aproximadamente −10 dB e 24 dB, respetivamente, ambas classificadas como "Excelente". Esta estabilidade indica que nem a potência do sinal de referência recebida pelo UE, nem a qualidade da ligação face à interferência e ao ruído foram afetadas pela alteração da largura de banda.

O CQI manteve o valor máximo de 15 ao longo de todo o ensaio, confirmando que a qualidade do canal reportada pelo UE permaneceu constante independentemente da configuração. O BLER em DL situou-se próximo de 0%, também classificado como "Excelente"; em UL, registaram-se oscilações temporárias que atingiram, nalguns instantes, valores próximos de 20% a 30%.

Apesar desta estabilidade nos indicadores de qualidade da ligação, verificou-se um impacto substancial na taxa de transmissão. Na configuração de 20 MHz, o *throughput* em DL atingiu aproximadamente 70 Mbit/s, duplicando para cerca de 140 Mbit/s (aumento de 100%) na configuração de 40 MHz, em UL a taxa cresceu de forma semelhante.

Em suma, os resultados demonstram que o aumento da largura de banda permitiu aumentar a capacidade de transmissão da interface rádio, sem degradar o RSRP, o RSRQ, o SINR, o CQI ou o BLER. Para o cenário considerado, em linha de vista (LoS) e a cerca de 2 metros entre o UE e o gNB, a expansão do canal rádio otimiza a taxa de transferência de dados, mantendo inalterado o perfil de qualidade do sinal.

3.3.1 Cálculos teóricos

Aplicam-se aos dois cenários os modelos analíticos da secção 2.8.2, detalhados nas subsecções seguintes para cada KPI.

3.3.1.1 RSRP teórico

Aplicando a equação de Friis (secção 2.8.2.1) à distância aproximada de ≈2 m entre o UE e o gNB e à frequência central da banda n77 (4019,160 MHz), com um ganho de antena do UE de 1 dB, calcula-se o RSRP teórico para cada largura de banda, considerando o respetivo número de blocos de recursos (Tabela 2:3): 51 RB para 20 MHz e 106 RB para 40 MHz.

A Tabela 3:3 apresenta o RSRP teórico, o valor medido e o desvio entre ambos, para as duas larguras de banda.

Tabela 3:3 RSRP teórico e desvio face ao valor medido

Configuração	NRB	EIRPRE (dBm)	RSRP teórico (dBm)	RSRP medido (dBm)	Desvio (dB)
20 MHz	51	−17,9	−67,4	≈−80	≈13
40 MHz	106	−21,0	−70,5	≈−80	≈10

3.3.1.2 SINR teórico

O ruído térmico (secção 2.8.2.5), para uma figura de ruído de referência de 5 dB, é de −96,0 dBm (20 MHz) e −93,0 dBm (40 MHz).

Aplicando $SINR_{teo,dB} = RSRP_{teo,dBm} - PN_{dBm}$ aos valores de RSRP teórico da Tabela 3:3, obtém-se um SINR teórico de ≈28,6 dB (20 MHz) e ≈22,5 dB (40 MHz). Este último

valor é inferior ao SINR medido (≈24 dB), o que não é fisicamente possível para um limite superior teórico, indicando que a figura de ruído real do recetor da OAIBOX™ é mais favorável do que o valor de referência de 5 dB assumido. Por esta razão, o SINR teórico não é usado como termo de comparação direta, mas apenas como indicação de que o desempenho medido se aproxima do limite físico do sistema.

3.3.1.3 CQI teórico

Para ambas as configurações, o SINR medido (≈24 dB) satura o mapeamento SINR-CQI (secção 2.8.2.5) no valor máximo (15), coincidindo com o valor medido.

3.3.1.4 Bitrate teórico

O limite de Shannon (secção 2.8.2.2) assume toda a largura de banda disponível para dados, sem distinguir DL de UL nem descontar os *Resource Elements* usados por sinais de referência e controlo, pelo que sobrestima o *bitrate* real. Por esta razão, aplica-se o modelo de *bitrate* por alocação de *slots* TDD (secção 2.8.2.3), separado por direção e baseado no MCS observado em cada teste.

Na configuração TDD DDDFU (3:1:1), dos 2000 *slots*/segundo (μ=1), 1600 cabem ao DL e 400 ao UL. A Tabela 3:4 apresenta o MCS aproximado de cada teste, a eficiência espectral resultante a partir da equação na secção 2.8.2.8 e o *bitrate* teórico final a partir da equação na secção 2.8.2.3, comparado com o medido.

Tabela 3:4 Bitrate teórico (por alocação de slots TDD) e bitrate máximo medido, por direção

Configuração	Direção	MCS	Bitrate teórico (Mbps)	Bitrate medido (Mbps)
20 MHz (51 RB)	DL	≈21	≈61,3	≈70
20 MHz (51 RB)	UL	≈9,7	≈6,5	≈14
40 MHz (106 RB)	DL	≈20	≈122,1	≈150
40 MHz (106 RB)	UL	≈10	≈14,7	≈27

Em DL, o teórico fica 15 a 25% abaixo do medido, o que se explica pela margem de segurança habitual na seleção do MCS face ao limite de erro de bloco. Em UL, o medido é sensivelmente o dobro do teórico, sugerindo uma seleção mais conservadora do MCS face às condições reais do canal.

O RSRP teórico apresenta um desvio de 10 a 13 dB face ao valor medido, explicado por três fatores. Primeiro, o ambiente de ensaio não é uma câmara anecoica, pelo que as reflexões e o multipercurso reduzem, em média, a potência recebida face ao modelo de espaço livre da equação de Friis. Segundo, o cálculo assume o EIRP máximo declarado (10 dBm), mas os equipamentos de rádio operam tipicamente com uma margem de recuo face a esse valor, pelo que a potência efetivamente transmitida pode ser inferior à assumida. Terceiro, a equação de Friis assume a potência distribuída uniformemente por todos os elementos de recurso, quando o RSRP é medido apenas sobre os do sinal de referência, que podem ter um nível de potência diferente do dos dados.

Quanto ao SINR, em 20 MHz o valor teórico é superior ao medido, como seria de esperar de um limite ideal, calculado sem interferência nem perdas de implementação. Em 40 MHz, o valor teórico fica abaixo do medido, o que só é fisicamente possível se a figura de ruído real do recetor da OAIBOX™ for inferior aos 5 dB assumidos como referência no cálculo (secção 3.3.1.2). O SINR teórico serve, por isso, como indicação da ordem de grandeza do limite físico do sistema, não como previsão exata do valor medido.

O CQI teórico coincide com o valor medido nas duas larguras de banda, uma vez que o SINR, medido ou teórico, é em ambos os casos suficientemente elevados para saturar o mapeamento SINR-CQI no valor máximo (15).

O BLER não admite uma expressão fechada que permita a sua estimativa direta a partir do SINR, dependendo antes de curvas de simulação ao nível de ligação, específicas da implementação de cada fabricante. O valor próximo de 0% observado nos ensaios é, ainda assim, consistente com os níveis de SINR e CQI elevados verificados em ambas as configurações.

3.4 Análise do impacto da banda de frequência e do cenário de propagação no desempenho da ligação 5G NR

Com o objetivo de avaliar o impacto da banda de frequência e do cenário de propagação no desempenho da interface rádio, foram realizados quatro testes experimentais, combinando as bandas n77 (4019,160 MHz) e n78 (3319,320 MHz) com condições de linha de vista (LoS) e sem linha de vista (NLoS). Os restantes parâmetros de configuração mantiveram-se fixos em todos os ensaios: largura de banda de 40 MHz, numerologia μ=1 e configuração SISO 1x1.

Na Figura 3-4 e na Figura 3-5 apresentam-se os resultados obtidos em condição de linha de vista (LoS), para as bandas n77 e n78, respetivamente.

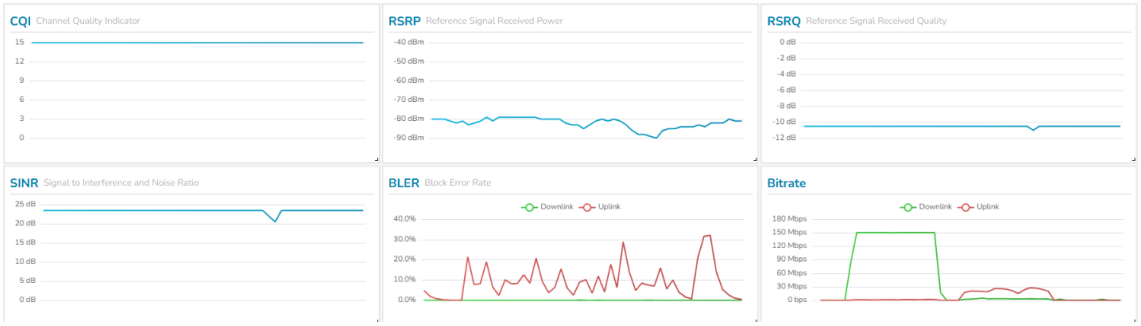


Figura 3-4: Evolução temporal dos KPIs para a banda n77 LoS

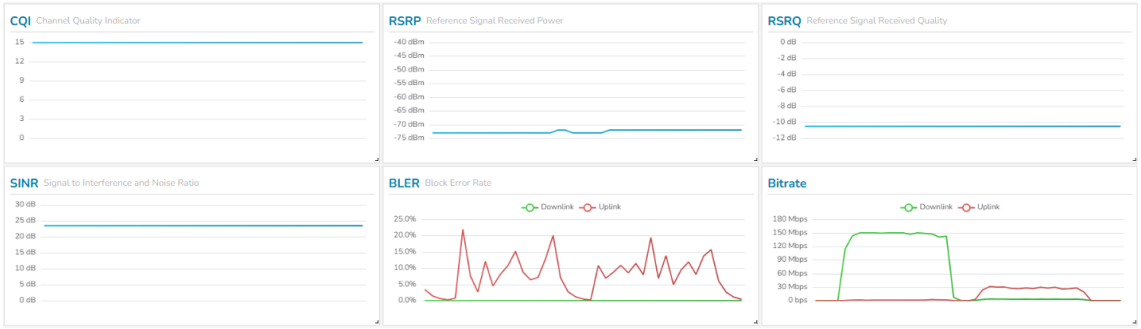


Figura 3-5: Evolução temporal dos KPIs para a banda n78 LoS

A análise qualitativa segue os limiares da Tabela 2:12. No RSRP, a n77 registou −82,4 dBm, na categoria "Bom", enquanto a n78 atingiu −72,1 dBm, já "Excelente". No RSRQ, ambas as bandas registaram −10,5 dB, classificado como "Bom". No SINR, ambas atingiram 23,5 dB, "Excelente", e o CQI manteve-se no valor máximo (15) em ambas, também "Excelente". No BLER, a n77 apresentou 0% em *downlink* ("Excelente") e 8,1%

em *uplink* ("Aceitável"); a n78 registou também 0% em *downlink*, mas 5% em *uplink*, já "Bom".

Esta diferença de cerca de 10 dB no RSRP é explicada pela maior atenuação em espaço livre associada à frequência mais elevada da n77, conforme a equação de Friis (secção 2.8.2). O ligeiro alívio do BLER em *uplink* na n78 acompanha esta melhoria de sinal, mas os restantes indicadores não se alteram entre bandas, e o *bitrate* também não é afetado, com 150 Mbit/s em *downlink* em ambos os casos e valores semelhantes em *uplink* (28 e 26 Mbit/s, respetivamente). Conclui-se que, nesta distância reduzida e em condição de linha de vista, a mudança de banda tem impacto reduzido no desempenho real da ligação.

Na Figura 3-6 e na Figura 3-7 apresentam-se os resultados obtidos para as mesmas bandas, em condição sem linha de vista (NLoS).

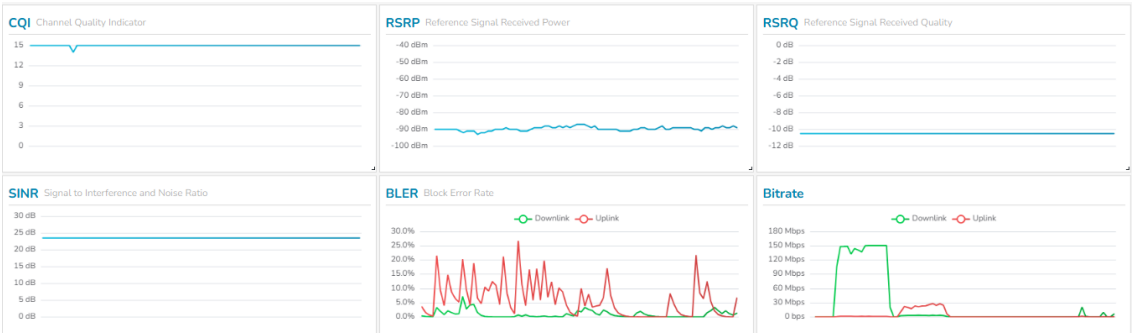


Figura 3-6: Evolução temporal dos KPIs para a banda n77 NLoS

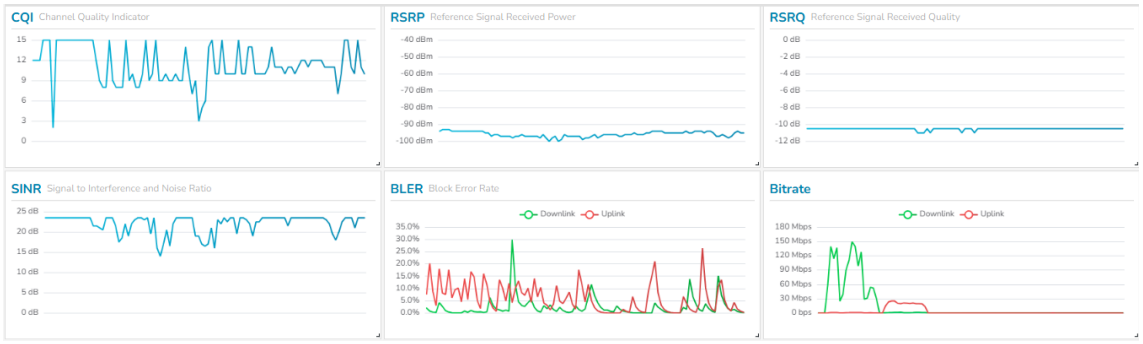


Figura 3-7: Evolução temporal dos KPIs para a banda n78 NLoS

Em NLoS, e segundo os mesmos limiares, o RSRP da n77 desceu para −89,3 dBm, mantendo-se "Bom", enquanto o da n78 caiu para −95,5 dBm, já "Aceitável". O RSRQ manteve-se em −10,5 dB em ambas as bandas, "Bom". O SINR manteve-se "Excelente" na n77 (23,5 dB), mas desceu para 21,8 dB na n78, ainda "Excelente". O CQI manteve-se no valor máximo (15, "Excelente") na n77, e desceu para 11 na n78, já "Bom". No BLER, a n77 registou 1% em *downlink* ("Bom") e 5,8% em *uplink* ("Aceitável"); a n78 registou 2% em *downlink* e 5% em *uplink*, ambos "Bom".

Esta maior sensibilidade da n78 é coerente com o facto de frequências mais elevadas sofrerem mais com obstáculos e multipercurso, efeitos que a equação de Friis, por assumir espaço livre, não contempla. Ainda assim, o *bitrate* manteve-se semelhante ao do cenário LoS em ambas as bandas, o que mostra que esta degradação do sinal não chegou a comprometer o desempenho real da ligação.

A Tabela 3:5 resume os valores medidos nos quatro cenários.

Tabela 3:5 Resumo dos KPIs medidos por banda e cenário de propagação

Cenário	RSRP (dBm)	RSRQ (dB)	SINR (dB)	CQI	BLER DL/UL (%)	*Throughput* DL/UL máx. (Mbps)
n77 LoS	−82,4	−10,5	23,5	15	0 / 8,1	150 / 28
n78 LoS	−72,1	−10,5	23,5	15	0 / 5	150 / 26
n77 NLoS	−89,3	−10,5	23,5	15	1 / 5,8	150 / 28
n78 NLoS	−95,5	−10,5	21,8	11	2 / 5	150 / 25

3.4.1 Cálculos teóricos

Aplicam-se aos quatro cenários os modelos analíticos da secção 2.8.2, detalhados nas subsecções seguintes para cada KPI.

3.4.1.1 RSRP teórico

O RSRP corresponde à potência recebida num único elemento de recurso, não à potência total transmitida. Partindo do EIRP máximo do gNB (10 dBm, Tabela 3:1) e da largura de banda de 40 MHz, correspondente a 106 blocos de recursos (Tabela 2:3), com 12 subportadoras cada:

$$N_{RE} = N_{RB} \times 12 = 106 \times 12 = 1272 \tag{3.1}$$

$$EIRP_{RE,dBm} = EIRP_{total,dBm} - 10\log_{10}(N_{RE}) = 10 - 10\log_{10}(1272) \approx -21{,}0\ dBm \tag{3.2}$$

Este valor é comum aos quatro cenários, uma vez que todos usam a mesma largura de banda.

Aplicando a equação de Friis (secção 2.8.2.1) à distância aproximada de cada ensaio (≈2 m em LoS, ≈5 m em NLoS), à frequência central de cada banda e a um ganho de antena do UE de 1 dB.

A Tabela 3:6 apresenta o RSRP teórico, o valor medido e o desvio entre ambos, para os quatro cenários.

Tabela 3:6 RSRP teórico e desvio face ao valor medido

Cenário	**d (m)**	**f_c (GHz)**	**PathLoss (dB)**	**RSRP teórico (dBm)**	**RSRP medido (dBm)**	**Desvio (dB)**
n77 LoS	2	4,019	50,5	−70,5	−82,4	11,9
n78 LoS	2	3,319	48,9	−68,9	−72,1	3,2
n77 NLoS	5	4,019	58,5	−78,5	−89,3	10,8
n78 NLoS	5	3,319	56,8	−76,8	−95,5	18,7

O desvio, definido como $RSRP_{teo} - RSRP_{medido}$, quantifica o afastamento entre o valor previsto pelo modelo e o valor medido, e serve de indicador da adequação do modelo ao ambiente de ensaio. O seu valor é positivo nos quatro cenários, o que é esperado: a equação de Friis assume espaço livre, enquanto a sala continha obstáculos (bancadas, computadores, cadeiras) mesmo em condição LoS.

A grandeza do desvio distingue claramente as duas bandas. Na n77, mantém-se estável entre LoS e NLoS (11,9 e 10,8 dB), indicando um efeito limitado do aumento da

distância, de ≈2 m para ≈5 m. Na n78, aumenta cerca de seis vezes, de 3,2 para 18,7 dB, confirmando, por via teórica, a maior degradação desta banda em NLoS já identificada na análise qualitativa anterior, onde o RSRP da n78 desceu de "Excelente" para "Aceitável".

3.4.1.2 SINR teórico

O ruído térmico para 40 MHz (secção 2.8.2.3) é de −93,0 dBm. Aplicando $SINR_{teo,dB} = RSRP_{teo,dBm} - PN_{dBm}$ aos valores de RSRP teórico da Tabela 3:7, obtém-se:

Tabela 3:7 SINR teórico e comparação com o valor medido

Cenário	SINR teórico (dB)	SINR medido (dB)
n77 LoS	23,5	23,5
n78 LoS	25,1	23,5
n77 NLoS	15,5	23,5
n78 NLoS	17,2	21,8

Em LoS, o SINR teórico iguala o valor medido na banda n77 (23,5 dB) e excede-o ligeiramente na banda n78 (25,1 dB vs. 23,5 dB), como seria de esperar de um limite superior. Em NLoS, o valor teórico fica abaixo do medido em ambas as bandas, repetindo o padrão já identificado na análise da largura de banda: o nível de ruído do recetor assumido como referência no cálculo (5 dB) subestima a qualidade real do recetor da OAIBOX™.

3.4.1.3 CQI teórico

Em três dos quatro cenários (n77 LoS, n78 LoS e n77 NLoS), o SINR medido (23,5 dB) é suficientemente elevado para saturar o mapeamento SINR-CQI no valor máximo, pelo que o CQI teórico coincide com o CQI medido, ambos no valor 15. Já no cenário n78 NLoS, o SINR desce para 21,8 dB, um valor inferior ao dos restantes três cenários e insuficiente para saturar esse mapeamento; o CQI teórico aproxima-se, por isso, do valor efetivamente medido (11), confirmando a coerência entre a queda de SINR e a descida de CQI observadas.

3.4.1.4 Bitrate teórico

O limite teórico de *bitrate*, dado pela capacidade de Shannon (secção 2.8.2.2), foi calculado a partir da largura de banda utilizada (40 MHz) e do SINR medido em cada cenário, convertido de dB para escala linear.

A Tabela 3:8 compara este limite com o *bitrate* máximo efetivamente medido.

Tabela 3:8 Capacidade de Shannon e bitrate máximo medido

Cenário	SINR medido (dB)	Capacidade de Shannon (Mbit/s)	*Bitrate* máx. medido (Mbit/s)
n77 LoS	23,5	312,6	150
n78 LoS	23,5	312,6	150
n77 NLoS	23,5	312,6	150
n78 NLoS	21,8	289,8	150

O *bitrate* medido mantém-se sempre bastante abaixo do limite de Shannon, devido à configuração experimental: antena única (SISO 1x1), ordem de modulação máxima

suportada, e repartição TDD (padrão DDDFU), que reserva apenas parte dos *slots* ao *downlink*.

3.4.1.5 Raio de célula (aplicação auxiliar)

Aplicando o modelo UMa e o *link budget* da secção 2.8.2.7, com o mesmo EIRP total (10 dBm), obtém-se um raio de célula estimado de 348 m para a n77 e 414 m para a n78.

3.5 Análise do impacto da configuração TDD no desempenho da ligação 5G NR

Com o objetivo de avaliar o impacto da configuração de *slots* TDD no desempenho da interface rádio, foram realizados quatro testes experimentais, combinando duas configurações TDD, DDDFU (3:1:1, orientada ao *downlink*) e DDFUU (2:1:2, equilibrada), com duas larguras de banda, 20 MHz e 40 MHz, em condição de linha de vista (LoS). Os restantes parâmetros de configuração mantiveram-se fixos: banda n77, numerologia μ=1, configuração SISO 1x1.

Na Figura 3-8 e na Figura 3-9 apresentam-se os resultados para a configuração DDDFU, nas larguras de banda de 20 MHz e 40 MHz, respetivamente.

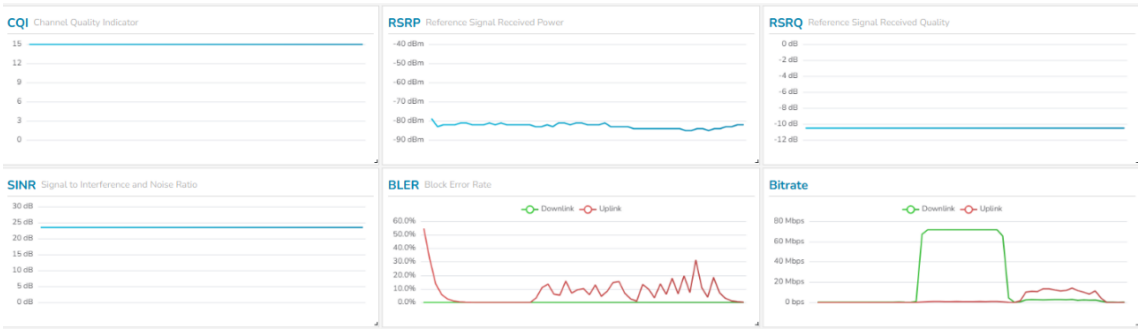


Figura 3-8: KPIs medidos para a configuração DDDFU (20 MHz)

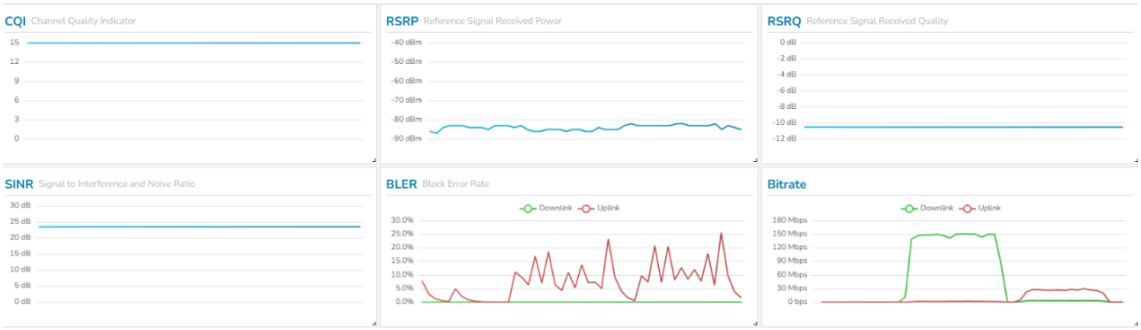


Figura 3-9: KPIs medidos para a configuração DDDFU (40 MHz)

Em ambas as larguras de banda, o RSRP manteve-se próximo de −82 dBm ("Bom") e o RSRQ em −10,5 dB ("Bom"), enquanto o SINR (≈23,5 dB) e o CQI (valor máximo, 15) foram classificados como "Excelente", segundo a Tabela 2:12. O *bitrate* em *downlink* acompanhou o aumento da largura de banda, subindo de ≈70 Mbit/s (20 MHz) para ≈150 Mbit/s (40 MHz), replicando o comportamento já observado na secção 3.3. O BLER em *uplink* manteve-se instável, com picos entre 20% e 30% ("Bom" a "Aceitável"), refletindo a reduzida fração de *slots* atribuída a esta direção.

Na Figura 3-10 e na Figura 3-11 apresentam-se os resultados para a configuração DDFUU, em 20 MHz e 40 MHz, respetivamente.

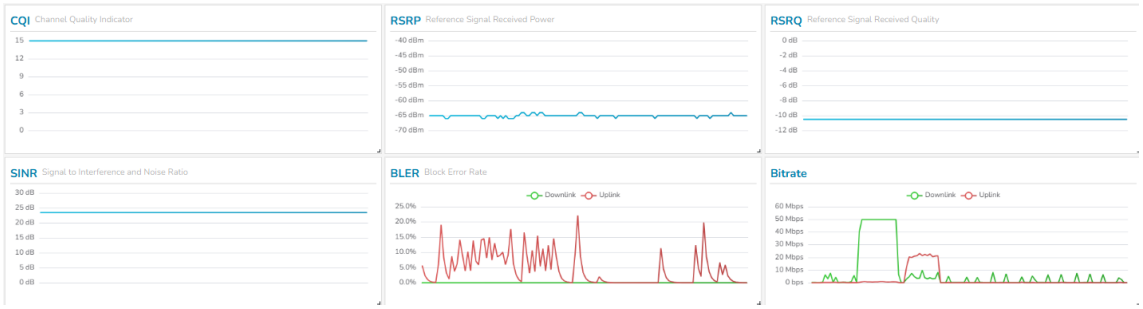


Figura 3-10: KPIs medidos para a configuração DDFUU (20 MHz)

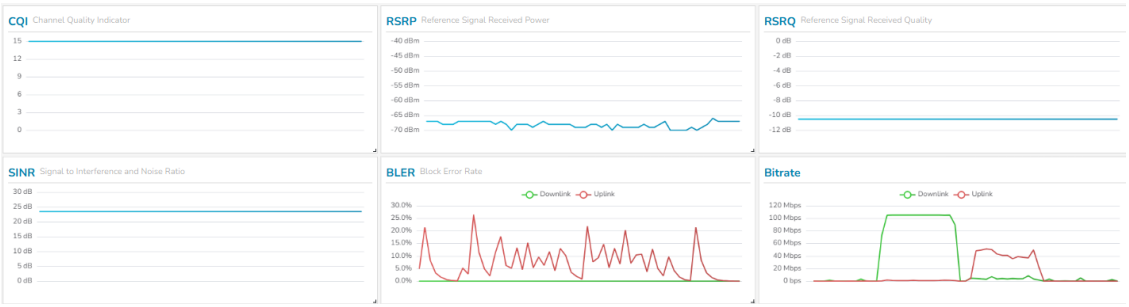


Figura 3-11: KPIs medidos para a configuração DDFUU (40 MHz)

Ao contrário da configuração anterior, o RSRP melhorou para ≈−65 dBm em ambas as larguras de banda, já "Excelente" segundo a Tabela 2:12; o RSRQ manteve-se "Bom" (−10,5 dB), e o SINR e o CQI continuaram "Excelente" (≈23,5 dB/ 15). A diferença mais relevante está na repartição do *bitrate*: o *downlink* máximo desceu para ≈50 Mbit/s (20 MHz) e ≈100 Mbit/s (40 MHz), enquanto o *uplink* subiu de forma expressiva, atingindo valores próximos aos do *downlink* (≈23 e ≈50 Mbit/s, respetivamente), resultado esperado, dado que esta configuração atribui mais *slots* ao *uplink* em detrimento do *downlink*.

Comparando as duas configurações, conclui-se que a configuração de *slots* TDD não afeta a qualidade do sinal recebido nem a estabilidade da ligação (RSRQ, SINR e CQI mantêm-se equivalentes), mas redistribui diretamente a capacidade de transmissão entre *downlink* e *uplink*, conforme o número de *slots* atribuído a cada direção.

A Tabela 3:9 resume os valores medidos, para as duas configurações e larguras de banda ensaiadas.

Tabela 3:9 Resumo de bitrate medido por configuração TDD

Configuração	Largura de banda	Bitrate DL medido (Mbit/s)	Bitrate UL medido (Mbit/s)
DDDFU (3:1:1)	20 MHz	≈70	≈15
DDDFU (3:1:1)	40 MHz	≈150	≈27
DDFUU (2:1:2)	20 MHz	≈50	≈23
DDFUU (2:1:2)	40 MHz	≈100	≈50

3.5.1 Cálculos teóricos

3.5.1.1 Modelo de alocação de *slots* TDD

Os valores teóricos de *bitrate* foram calculados através do modelo de alocação de *slots* TDD (secção 2.8.2.3).

Onde 978 bits é o volume de dados por bloco de recurso por *slot* (secção 2.8.2.3), N_{RB} o número de blocos de recursos da largura de banda utilizada (51 para 20 MHz, 106 para 40 MHz, Tabela 2:3), e $N_{slots,dir}$ o número de *slots* por segundo atribuídos a cada direção, segundo a configuração TDD:

Configuração	Nslots, DL/s	Nslots, UL/s
DDDFU (3:1:1)	1600	400
DDFUU (2:1:2)	1200	800

A título de exemplo, para a configuração DDDFU a 40 MHz:

$$\text{Bitrate}_{DL} = \frac{978 \times 106 \times 1600}{10^6} \approx 166 \text{ Mbps} \quad (3.3)$$

$$\text{Bitrate}_{UL} = \frac{978 \times 106 \times 400}{10^6} \approx 41 \text{ Mbps} \quad (3.4)$$

3.5.1.2 Comparação com os valores medidos

Aplicando a mesma expressão aos restantes cenários, obtêm-se os valores apresentados na Tabela 3:10, que compara os valores teóricos obtidos com os valores medidos.

Tabela 3:10 Bitrate teórico e desvio face ao valor medido, por configuração TDD

Configuração	Largura de banda	Bitrate DL teórico (Mbit/s)	Bitrate UL teórico (Mbit/s)
DDDFU (3:1:1)	20 MHz	80	20
DDDFU (3:1:1)	40 MHz	166	41
DDFUU (2:1:2)	20 MHz	60	40
DDFUU (2:1:2)	40 MHz	124	83

O *bitrate* medido aproxima-se do valor teórico em todos os cenários, sendo consistentemente inferior, tal como já discutido (3.3, 3.4), devido à sobrecarga de sinalização, ao mecanismo HARQ e às condições reais de propagação, não contempladas no modelo. A diferença relativa mantém-se semelhante entre configurações, indicando que o modelo de alocação de *slots* descreve adequadamente o efeito da configuração TDD na capacidade de transmissão, independentemente da direção ou da largura de banda.

3.6 Análise do desempenho da ligação 5G NR em modo FDD

Com o objetivo de avaliar o desempenho da interface rádio em modo *Frequency Division Duplex* (FDD), foram realizados dois testes experimentais, com larguras de banda de 20 MHz e 40 MHz, em condição de linha de vista (LoS). Os restantes parâmetros de configuração mantiveram-se fixos: banda n77, numerologia μ=1, configuração SISO 1x1.

Na Figura 3-12 e na Figura 3-13 apresentam-se os resultados para 20 MHz e 40 MHz, respetivamente.

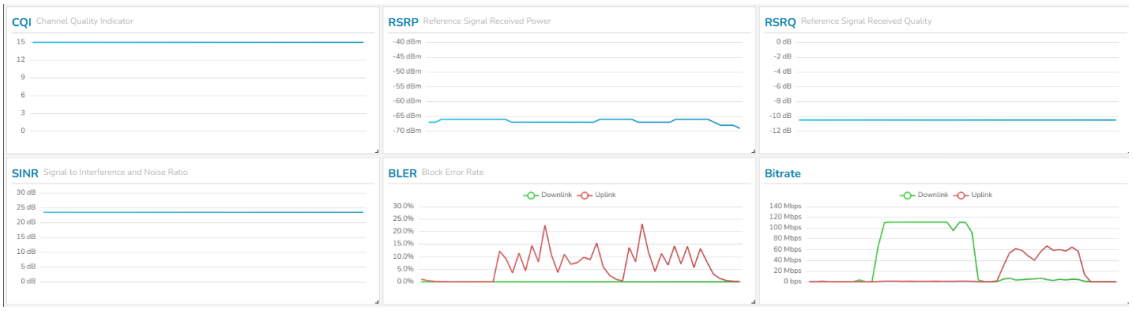


Figura 3-12: KPIs medidos em modo FDD (20 MHz)

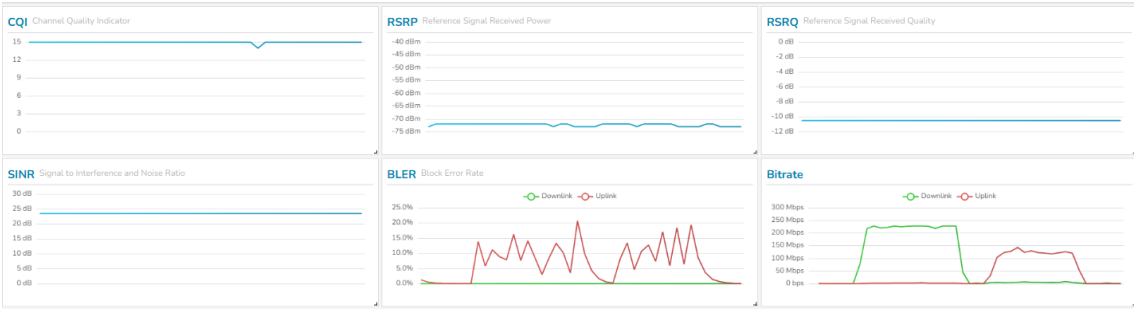


Figura 3-13: KPIs medidos em modo FDD (40 MHz)

Segundo os limiares da Tabela 2:12, o RSRP situou-se em ≈−68 dBm a 20 MHz e ≈−72,5 dBm a 40 MHz, ambos "Excelente"; o RSRQ, o SINR e o CQI mantiveram-se "Bom" e "Excelente", respetivamente, em ambas as larguras de banda, tal como nos restantes laboratórios. O BLER manteve-se próximo de 0% em *downlink*, mas subiu para 5,4% (20 MHz) e 5,6% (40 MHz) em *uplink*, ainda assim "Aceitável" segundo a mesma tabela.

A diferença mais relevante do modo FDD face ao TDD está no *bitrate*. Em vez de o *downlink* e o *uplink* partilharem o tempo de transmissão por *slots*, como nas secções 3.3 e 3.5, cada direção dispõe da totalidade da largura de banda numa portadora própria, em simultâneo.

Esta separação eleva o *bitrate* máximo muito acima do observado em TDD. A 20 MHz, atinge ≈110 Mbit/s em *downlink* e ≈67 Mbit/s em *uplink*; a 40 MHz, ≈227 e ≈143 Mbit/s, respetivamente. Em ambos os casos, o *uplink* mais do que duplica o valor conseguido em TDD para a mesma largura de banda (3.3, 3.5).

O FDD é, por isso, a configuração mais vantajosa para aplicações que exijam elevado débito simultâneo nas duas direções.

A Tabela 3:11 resume os valores medidos nas duas configurações.

Tabela 3:11 Resumo dos KPIs e do bitrate medidos em modo FDD

Largura de banda	RSRP (dBm)	RSRQ (dB)	SINR (dB)	CQI	BLER DL/UL (%)	Bitrate DL/UL máx. (Mbit/s)
20 MHz	−68,8	−10,5	23,5	15	0 / 5,4	110 / 67
40 MHz	−72,5	−10,5	23,5	15	0 / 5,6	227 / 143

3.6.1 Cálculos teóricos

3.6.1.1 Capacidade de Shannon

Ao contrário da secção 3.3 e da 3.5, o modelo de alocação de *slots* TDD (secção 2.8.2.3) não se aplica ao modo FDD, uma vez que o *downlink* e o *uplink* não partilham *slots* no tempo, dispondo cada um da totalidade da largura de banda configurada. Aplica-se, por isso, apenas o limite de Shannon (secção 2.8.2.2). A título de exemplo, para 40 MHz:

$$C = 4 \times 10^7 \times \log_2\left(1 + 10^{23{,}5/10}\right) \approx 312{,}6 \text{ Mbps} \quad (3.5)$$

3.6.1.2 Comparação com os valores medidos

A Tabela 3:12 compara este limite com o *bitrate* máximo medido em cada largura de banda.

Tabela 3:12 Capacidade de Shannon e bitrate máximo medido, modo FDD

Largura de banda	SINR medido (dB)	Capacidade de Shannon (Mbit/s)	Bitrate DL medido (Mbit/s)	Bitrate UL medido (Mbit/s)
20 MHz	23,5	156,3	110	67
40 MHz	23,5	312,6	227	143

O *downlink* aproxima-se mais do limite de Shannon (a ≈46 e ≈86 Mbit/s de distância) do que o *uplink* (a ≈89 e ≈170 Mbit/s de distância), a 20 e 40 MHz, respetivamente. Esta diferença explica-se pela ordem de modulação: o MCS em *downlink* (≈24 a 20 MHz, ≈26 a 40 MHz) é muito superior ao de *uplink* (≈9,4 e ≈10,2, respetivamente), pelo que o *uplink* transmite menos bits por símbolo e fica, por isso, mais longe do limite teórico.

3.7 Análise do impacto do esquema de modulação e codificação no desempenho da ligação 5G NR

Com o objetivo de avaliar o impacto da ordem de modulação no desempenho da interface rádio, foram realizados oito testes experimentais, combinando quatro ordens de modulação (QPSK, 16QAM, 64QAM e 256QAM) com duas condições de propagação, LoS e NLoS. Os restantes parâmetros de configuração mantiveram-se fixos: banda n77, largura de banda de 40 MHz, numerologia μ=1, configuração SISO 1x1.

3.7.1 QPSK

Na Figura 3-14 e na Figura 3-15 apresentam-se os resultados para a modulação QPSK em condição LoS, seguidos, na Figura 3-16 e na Figura 3-17, dos resultados para a mesma modulação em condição NLoS.

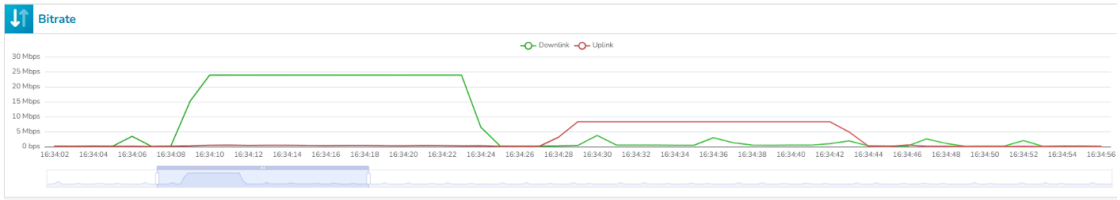


Figura 3-14: Evolução do bitrate para modulação QPSK em condição LoS

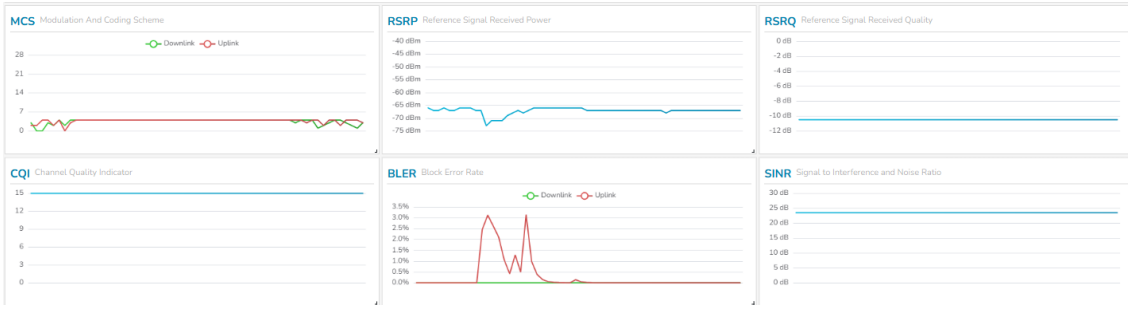


Figura 3-15: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação QPSK em condição LoS

Em condição LoS, os cinco indicadores de qualidade da ligação, RSRP, RSRQ, SINR, CQI e BLER, situam-se todos entre "Bom" e "Excelente" segundo a Tabela 2:12 (RSRP ≈−67 dBm; BLER de 0% e 0,3% em DL e UL, respetivamente). O MCS mantém-se baixo, ≈4 em DL e ≈3,7 em UL, refletindo o teto imposto pela própria modulação QPSK, independentemente da qualidade real do canal.

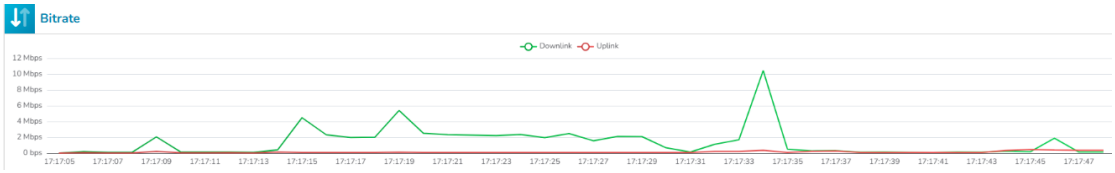


Figura 3-16: Evolução do bitrate para modulação QPSK em condição NLoS

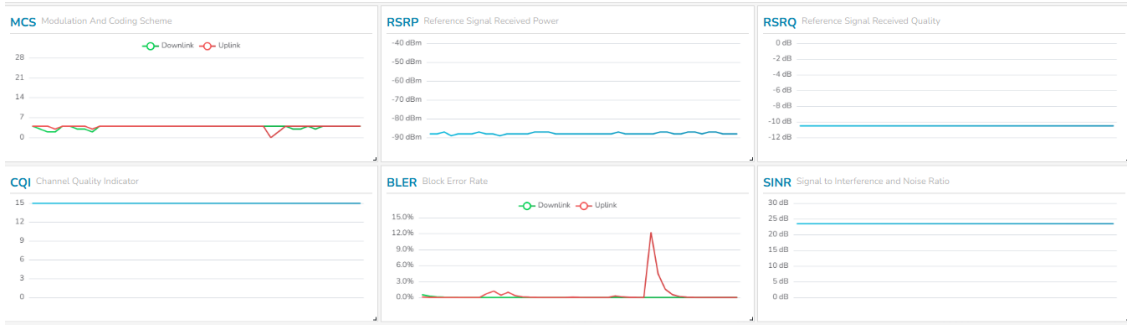


Figura 3-17: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação QPSK em condição NLoS

A transição para NLoS penaliza o RSRP em cerca de 20 dB (para ≈−87,7 dBm), sem que isso se traduza em qualquer alteração no MCS ou numa subida relevante do BLER (0,5% em UL, ainda "Excelente"). O impacto real desta transição só se manifesta no *bitrate*: o *downlink* cai de ≈24 para ≈10 Mbit/s, e o *uplink* praticamente desaparece, de ≈8 para ≈0,46 Mbit/s. A modulação QPSK revela-se, assim, robusta em termos de qualidade de ligação reportada, mas incapaz de sustentar o débito em *uplink* face à perda de linha de vista.

3.7.2 16QAM

Na Figura 3-18 e na Figura 3-19 apresentam-se os resultados para a modulação 16QAM em condição LoS, seguidos, na Figura 3-20 e na Figura 3-21, dos resultados para a mesma modulação em condição NLoS.

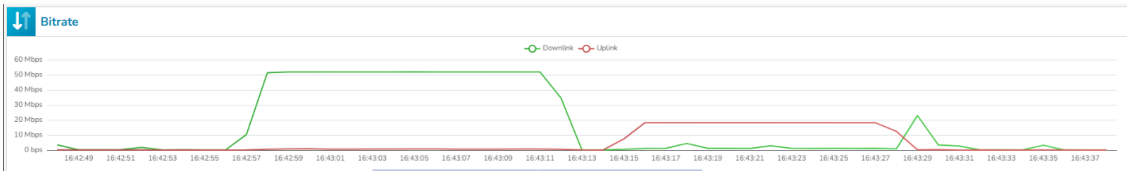


Figura 3-18: Evolução do bitrate para modulação 16QAM em condição LoS

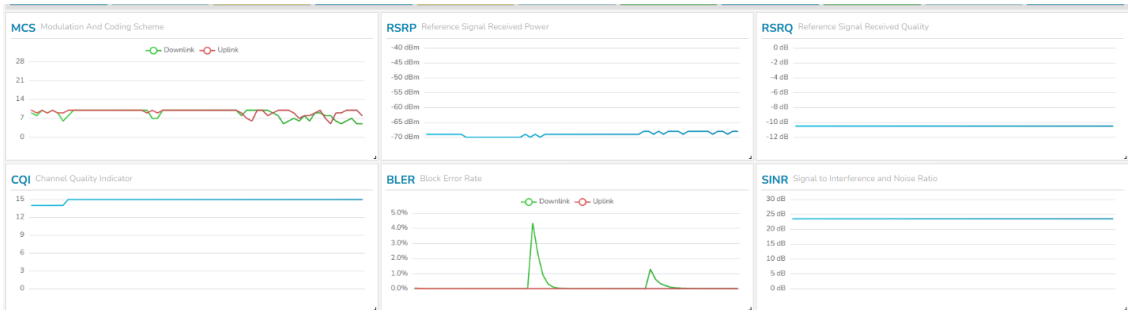


Figura 3-19: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação 16QAM em condição LoS

Subindo para 16QAM, o MCS acompanha o aumento esperado (≈9 em DL e UL), sem qualquer custo em fiabilidade: o BLER em *uplink* mantém-se em 0,7%, ainda "Excelente" segundo a Tabela 2:12, e o RSRP em LoS situa-se em ≈−69 dBm, também "Bom".

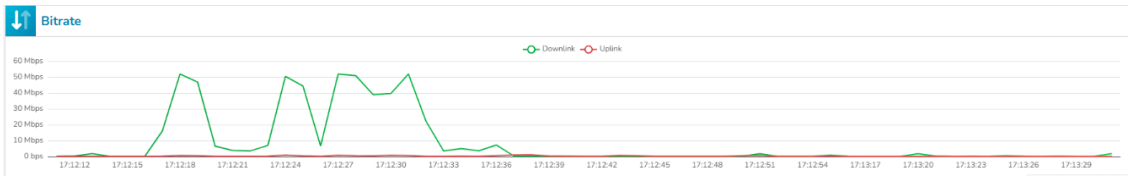


Figura 3-20: Evolução do bitrate para modulação 16QAM em condição NLoS

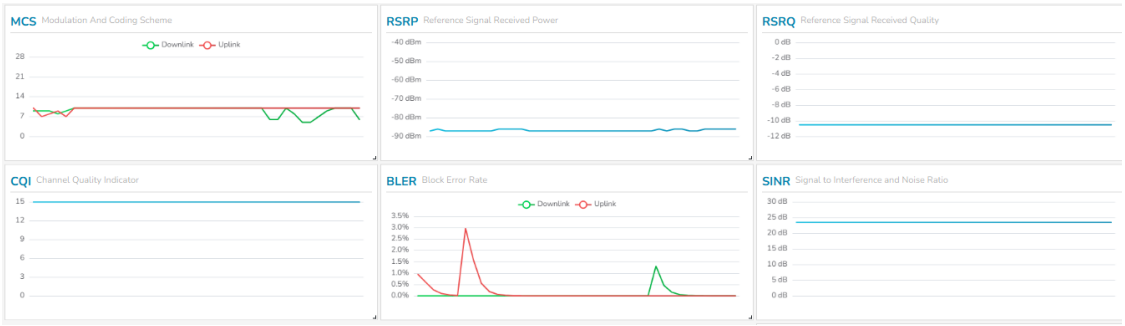


Figura 3-21: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação 16QAM em condição NLoS

Já em NLoS, ocorre algo digno de nota: apesar de o RSRP cair para ≈−86,7 dBm, o MCS em *uplink* sobe ligeiramente (≈9,8) e o BLER desce para 0,2%, um resultado melhor do que em LoS. No entanto, esta aparente melhoria de qualidade não se reflete no débito: o *uplink* colapsa de ≈18 para ≈1,1 Mbit/s, enquanto o *downlink* se mantém praticamente inalterado (≈52 para ≈51 Mbit/s). A contradição entre indicadores de qualidade estáveis (ou melhores) e um *bitrate* muito inferior sugere que a queda não tem origem na qualidade do canal, mas antes numa redução dos recursos rádio atribuídos ao *uplink* durante este ensaio específico.

3.7.3 64QAM

Na Figura 3-22 e na Figura 3-23 apresentam-se os resultados para a modulação 64QAM em condição LoS, seguidos, na Figura 3-24 e na Figura 3-25, dos resultados para a mesma modulação em condição NLoS.

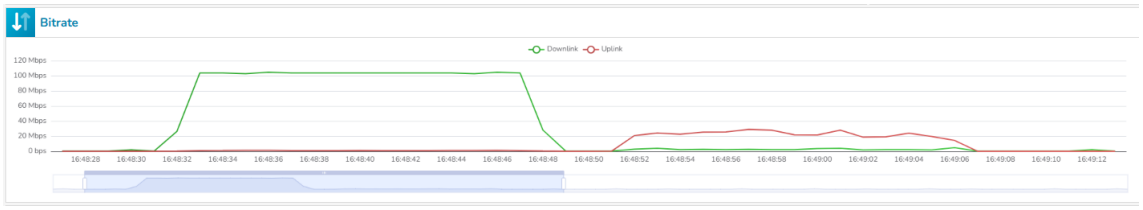


Figura 3-22: Evolução do bitrate para modulação 64QAM em condição LoS

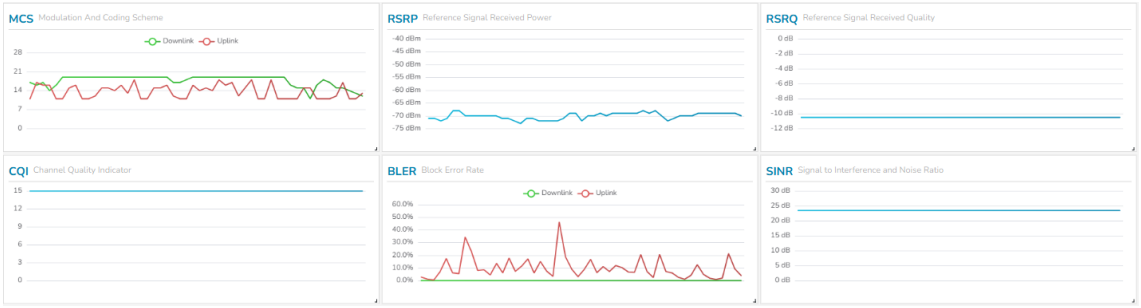


Figura 3-23: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação 64QAM em condição LoS

O 64QAM marca a primeira fronteira relevante deste laboratório: o BLER em *uplink*, até aqui inferior a 1%, salta para 10% em LoS, já na categoria "Aceitável" da Tabela 2:12, com o RSRP em ≈−69,9 dBm e o MCS a atingir ≈18 em DL e ≈13,6 em UL.

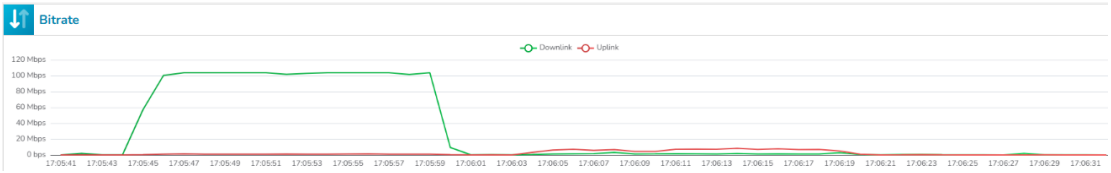


Figura 3-24: Evolução do bitrate para modulação 64QAM em condição NLoS

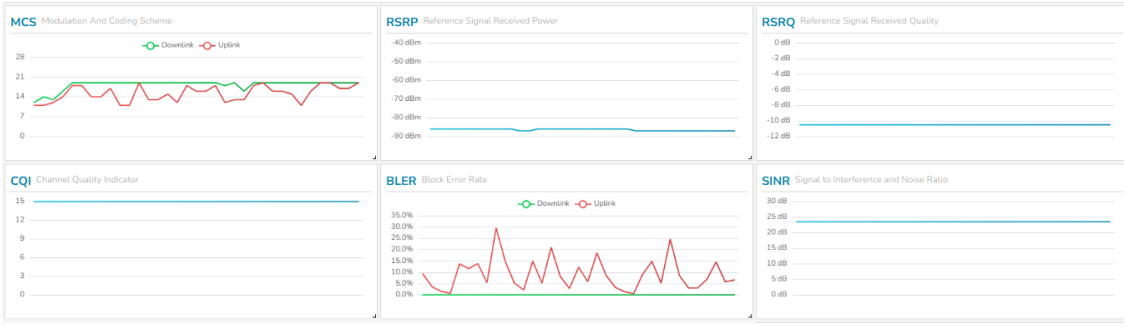


Figura 3-25: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação 64QAM em condição NLoS

O mesmo padrão contraintuitivo do 16QAM repete-se em NLoS: o RSRP desce para ≈−86,4 dBm, mas o MCS em *uplink* sobe para ≈15,2 e o BLER melhora ligeiramente para 9,2%. Novamente, esta estabilidade (ou ligeira melhoria) dos indicadores de qualidade não impede uma queda acentuada do *bitrate* em *uplink*, de ≈29 para ≈8 Mbit/s, enquanto o

downlink se mantém em ≈104 Mbit/s. Consolida-se, com este segundo caso, a hipótese de que a causa da degradação do débito em NLoS está ligada à gestão de recursos rádio pelo escalonador, e não a uma efetiva perda de qualidade de sinal em *uplink*.

3.7.4 256QAM

Na Figura 3-26 e na Figura 3-27 apresentam-se os resultados para a modulação 256QAM em condição LoS, seguidos, na Figura 3-28 e na Figura 3-29, dos resultados para a mesma modulação em condição NLoS.

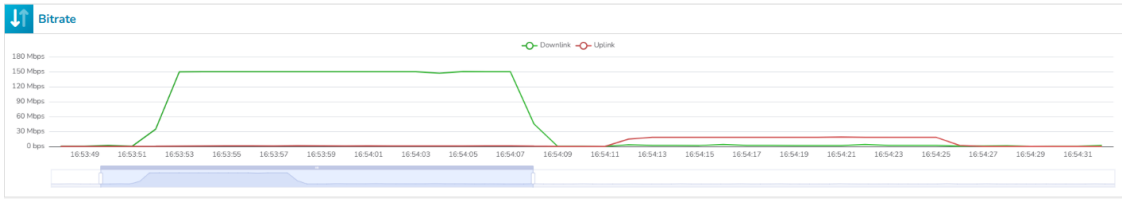


Figura 3-26: Evolução do bitrate para modulação 256QAM em condição LoS

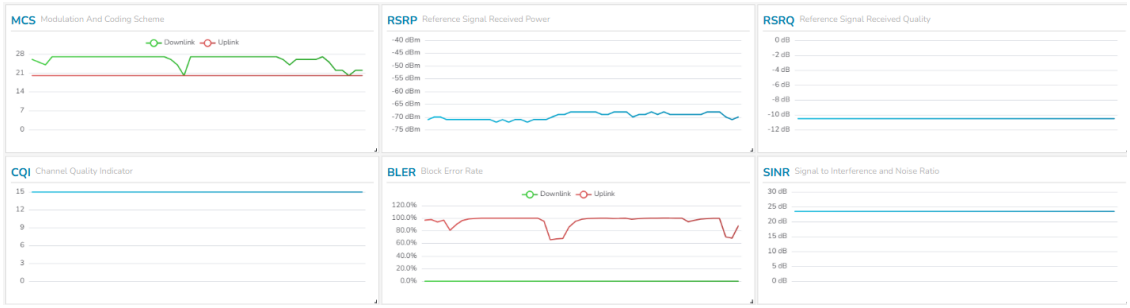


Figura 3-27: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação 256QAM em condição LoS

No cenário LoS, o *downlink* mantém um BLER próximo de 0% ("Excelente", Tabela 2:12), mas o *uplink* apresenta um BLER médio de 88,7%, muito acima do limiar "Pobre" da mesma tabela. Este resultado indica que a ligação em *uplink* não consegue sustentar de forma fiável a modulação 256QAM, mesmo em condição de linha de vista, apesar de o *downlink* a sustentar sem dificuldade.

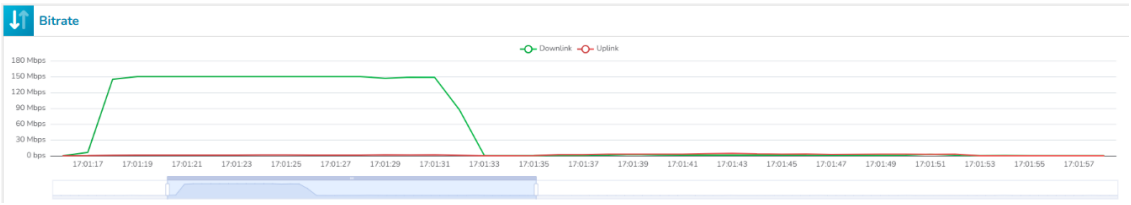


Figura 3-28: Evolução do bitrate para modulação 256QAM em condição NLoS

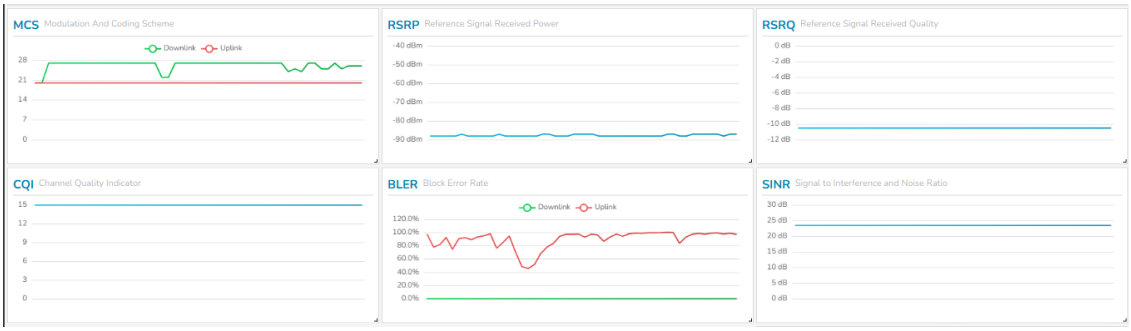


Figura 3-29: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para modulação 256QAM em condição NLoS

A Tabela 3:13 resume os valores medidos nos oito cenários.

Tabela 3:13 RSRP, RSRQ, SINR, CQI, BLER, MCS e bitrate medidos, por ordem de modulação e cenário de propagação

Modulação	Cenário	RSRP (dBm)	RSRQ (dB)	SINR (dB)	CQI	BLER DL (%)	BLER UL (%)	MCS DL	MCS UL	Bitrate DL (Mbit/s)	Bitrate UL (Mbit/s)
QPSK	LoS	−67	−10,5	23,5	15	0	0,3	4	3,7	≈24	≈8
QPSK	NLoS	−87,7	−10,5	23,5	15	0	0,5	4	3,8	≈10	≈0,458
16QAM	LoS	−69	−10,5	23,5	14,9	0	0,7	9	9,1	≈52	≈18
16QAM	NLoS	−86,7	−10,5	23,5	15	0	0,2	9	9,8	≈51	≈1,1
64QAM	LoS	−69,9	−10,5	23,5	15	0	10	18	13,6	≈104	≈29
64QAM	NLoS	−86,4	−10,5	23,5	15	0	9,2	18	15,2	≈104	≈8
256QAM	LoS	−69,4	−10,5	23,5	15	0	88,7	25	20	≈150	≈18
256QAM	NLoS	−87,2	−10,5	23,5	15	0	88,2	25	20	≈150	≈5

Em suma, o *downlink* beneficia de forma consistente do aumento da ordem de modulação, com ganhos de *bitrate* semelhantes em LoS e em NLoS, e mantém-se estável entre os dois cenários a partir do 16QAM. O *uplink*, pelo contrário, degrada-se à medida que a modulação exige mais do canal, culminando na inviabilidade prática do 256QAM, independentemente da condição de propagação.

No QPSK e no 64QAM, a queda de *bitrate* em *uplink* entre LoS e NLoS é acompanhada por uma redução acentuada do PHR (*Power Headroom Report*, a margem de potência disponível no UE para transmissão em *uplink*), de 24 para 9,5 dB e de 23 para 15,6 dB, respetivamente, indicando que o UE ficou com menos margem de potência disponível para compensar a maior perda de percurso em NLoS, condicionando os recursos que o escalonador lhe atribuiu. No 16QAM, contudo, o PHR mantém-se inalterado (24 dB em ambos os cenários), pelo que a causa desta queda específica de *bitrate* não é identificável a partir dos indicadores recolhidos neste ensaio.

3.7.5 Cálculos teóricos

3.7.5.1 Eficiência espectral teórica

A eficiência espectral teórica de cada ordem de modulação foi calculada segundo o modelo da secção 2.8.2.3, assumindo a taxa de codificação máxima normativa (≈0,925):

$$SE_{teo,QPSK} = 2 \times 0{,}925 \approx 1{,}85\ b/s/Hz \quad (3.6)$$

Aplicando a mesma expressão às restantes ordens de modulação, obtêm-se os valores da Tabela 3:14.

Tabela 3:14 Eficiência espectral teórica e medida, por ordem de modulação e cenário de propagação

Modulação	Efic. espectral teórica (b/s/Hz)	Efic. espectral DL medida, LoS/NLoS (b/s/Hz)	Efic. espectral UL medida, LoS/NLoS (b/s/Hz)
QPSK	1,85	0,60 / 0,25	0,20 / 0,011
16QAM	3,70	1,30 / 1,28	0,45 / 0,028
64QAM	5,55	2,60 / 2,60	0,73 / 0,20
256QAM	7,40	3,75 / 3,75	0,45 / 0,13

Em *downlink*, a eficiência espectral medida aproxima-se do valor teórico de forma crescente com a ordem de modulação, mas mantém-se sempre abaixo dele, uma vez que o modelo teórico assume a taxa de codificação máxima de forma permanente, enquanto a transmissão real intercala períodos de tráfego com períodos de inatividade e está sujeita à repartição TDD (secção 2.8.2.3).

Em *uplink*, o desvio é substancialmente maior em todas as ordens de modulação, agravando-se de forma acentuada no 256QAM, onde a eficiência medida (0,45 e 0,13 b/s/Hz) fica muito aquém do valor teórico (7,40 b/s/Hz), consequência direta do elevado BLER já discutido nesta secção (3.7.4).

3.8 Testar configurações MIMO do 5G NR

Com o objetivo de avaliar o impacto da configuração de antenas MIMO no desempenho da ligação 5G NR, foram realizados quatro testes experimentais, combinando duas configurações de antena, *Single-Input Single-Output* (SISO, 1x1) e *Multiple-Input Multiple-Output* (MIMO, 2x2), com duas condições de propagação, LoS e NLoS. Os restantes parâmetros de configuração mantiveram-se fixos: banda n77, largura de banda de 20 MHz, numerologia μ=1.

3.8.1 SISO 1x1

Na Figura 3-30 e na Figura 3-31 apresentam-se, respetivamente, a evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR, e a evolução do *bitrate*, para a configuração SISO (1x1) em condição LoS.



Figura 3-30: Evolução do bitrate para SISO (1x1) em condição LoS

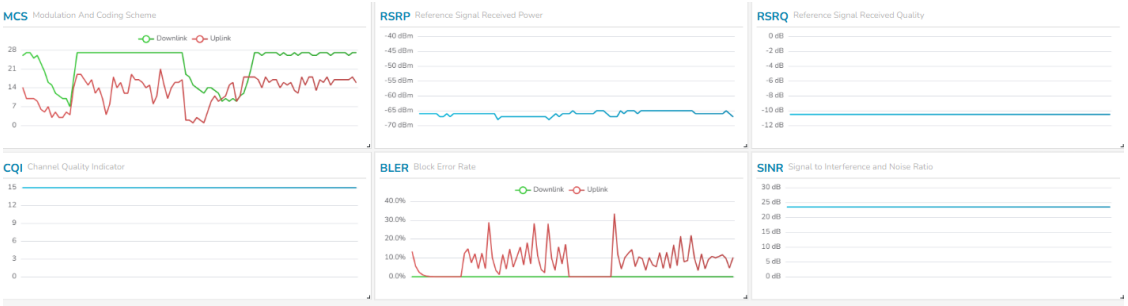


Figura 3-31: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para SISO (1x1) em condição LoS

Durante o teste de *downlink*, o RSRP e o RSRQ situam-se em ≈−67 dBm e ≈−10,5 dB, o SINR ronda os ≈23,5 dB e o CQI mantém-se no valor máximo (15) ao longo de todo o ensaio, valores que correspondem às categorias "Bom" e "Excelente" da Tabela 2:12. O MCS acompanha esta boa qualidade de canal, subindo para valores próximos de 28, enquanto o BLER se mantém perto de 0%.

No teste de *uplink*, os restantes indicadores mantêm-se inalterados, mas o MCS sobe apenas para valores próximos de 14 a 21, e o BLER passa a oscilar entre ≈5% e 30%, com picos pontuais próximos de 40%, ainda assim compatível com um desempenho "Bom" na maior parte do ensaio. Conforme visível na Figura 3-30, o *bitrate* estabiliza em ≈72 Mbit/s em *downlink* e ≈14 Mbit/s em *uplink*.

Repetindo o mesmo procedimento em condição NLoS, obtiveram-se os resultados apresentados na Figura 3-32 e na Figura 3-33.



Figura 3-32: Evolução do bitrate para SISO (1x1) em condição NLoS

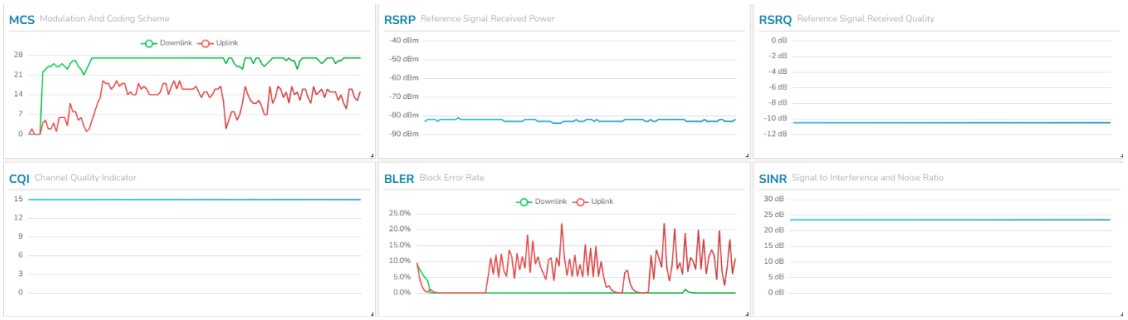


Figura 3-33: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para SISO (1x1) em condição NLoS

Com a perda de linha de vista, o RSRP desce para ≈−82 dBm, mantendo-se ainda assim na categoria "Bom", enquanto o RSRQ, o SINR e o CQI permanecem praticamente inalterados face ao cenário LoS. Durante o teste de *downlink*, o MCS continua elevado (≈21 a 28) e o BLER mantém-se perto de 0%, o que evidencia a compensação da maior atenuação de percurso através da seleção do MCS pelo gNB. No teste de *uplink*, o MCS oscila de forma mais acentuada, com quedas ocasionais a valores próximos de 0, e o BLER

mostra maior volatilidade, entre ≈5% e 25%. Como mostra a Figura 3-32, o *bitrate* mantém-se próximo do observado em LoS em *downlink* (≈72 Mbit/s), com uma ligeira redução em *uplink* (≈13 Mbit/s).

Em suma, na configuração SISO a transição de LoS para NLoS penaliza fortemente o RSRP (≈15 dB), sem que isso se reflita no RSRQ, no SINR ou no CQI, nem no débito de *downlink*. O *uplink* revela maior sensibilidade à perda de linha de vista, com o BLER mais instável e uma ligeira quebra no *bitrate*.

3.8.2 MIMO 2x2

Na Figura 3-34 e na Figura 3-35 apresentam-se, respetivamente, a evolução do *bitrate* e a evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR, para a configuração MIMO (2x2) em condição LoS.

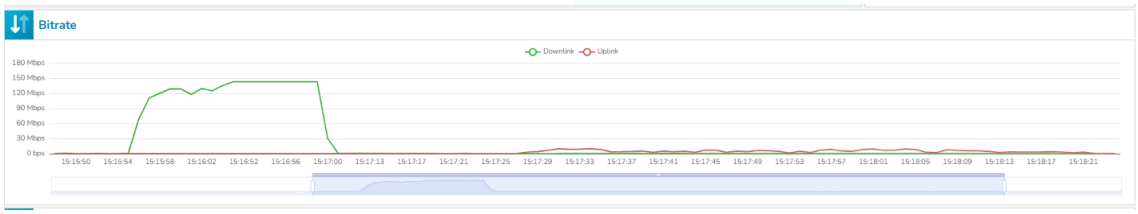


Figura 3-34: Evolução do bitrate para MIMO (2x2) em condição LoS

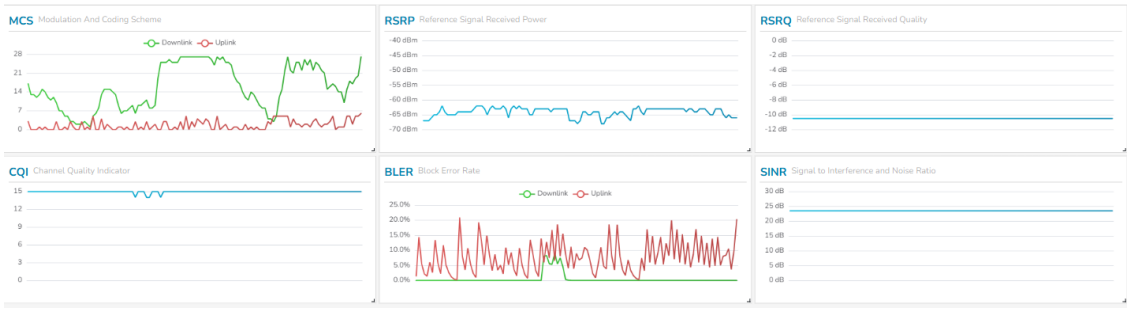


Figura 3-35: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para MIMO (2x2) em condição LoS

Com a configuração MIMO 2x2, o RSRP situa-se em ≈−66 dBm e o RSRQ em ≈−10,5 dB, correspondendo às categorias "Bom" e "Excelente" da Tabela 2:12, com SINR próximo de ≈25 dB. O CQI mantém-se, na generalidade, no valor máximo (15), com quebras pontuais até ≈9. Durante o teste de *downlink*, o MCS oscila entre ≈7 e 28, refletindo a repartição da capacidade pelos dois fluxos espaciais, e o BLER mantém-se perto de 0%. No teste de *uplink*, o MCS mantém-se mais moderado, entre ≈0 e 14, e o BLER passa a oscilar entre ≈0% e 25%. Conforme visível na Figura 3-34, o *bitrate* estabiliza em ≈143 Mbit/s em *downlink*, praticamente o dobro do valor obtido em SISO, e de ≈9 Mbit/s em *uplink*.

Repetindo o mesmo procedimento em condição NLoS, obtiveram-se os resultados apresentados na Figura 3-36 e na Figura 3-37.



Figura 3-36: Evolução do bitrate para MIMO (2x2) em condição NLoS

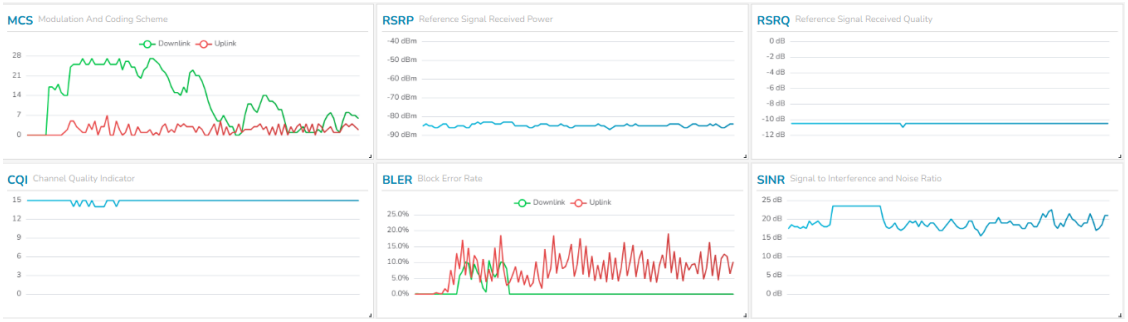


Figura 3-37: Evolução temporal do MCS, RSRP, RSRQ, CQI, BLER e SINR para MIMO (2x2) em condição NLoS

Com a perda de linha de vista, o RSRP desce para ≈−80 dBm, mantendo-se na categoria "Bom", enquanto o RSRQ permanece em ≈−10,5 dB e o SINR desce ligeiramente para uma gama entre ≈15 e 25 dB. O CQI mantém-se, na generalidade, no valor máximo, com as mesmas quebras pontuais já observadas em LoS. Durante o teste de *downlink*, o MCS desce de forma mais acentuada ao longo do ensaio, de valores próximos de 28 para ≈7 a 14, e o BLER sobe para uma gama entre ≈0% e 10%.

No teste de *uplink*, o BLER mostra maior volatilidade, entre ≈0% e 25%. Como mostra a Figura 3-36, o *bitrate* de *downlink* mantém-se praticamente inalterado face ao cenário LoS (≈143 Mbit/s), enquanto o de *uplink* desce para ≈7 Mbit/s.

3.8.3 Resultados e discussão

A Tabela 3:15 resume os valores medidos de *bitrate* de *downlink* e *uplink* nos quatro cenários testados.

Tabela 3:15 Bitrate DL e UL medido e Rank Indicator, por configuração de antena e cenário de propagação

Configuração	RI	Bitrate DL LoS (Mbit/s)	Bitrate DL NLoS (Mbit/s)	Bitrate UL LoS (Mbit/s)	Bitrate UL NLoS (Mbit/s)
SISO (1x1)	1	≈72	≈72	≈14	≈13
MIMO (2x2)	2	≈143	≈143	≈9	≈7

A configuração MIMO 2x2 duplica o *bitrate* de *downlink* face ao SISO, de ≈72 para ≈143 Mbit/s, um ganho consistente com a multiplexagem espacial descrita na secção 2.2.3. O *bitrate* de *uplink*, pelo contrário, diminui com o MIMO (≈14 para ≈9 Mbit/s em LoS; ≈13 para ≈7 Mbit/s em NLoS), resultado do maior custo de sinalização de referência (SRS) exigido para a estimação de canal em ambas as antenas, segundo o mecanismo de PMI da norma 3GPP TS 38.214 [26].

O cenário de propagação tem pouco impacto no *bitrate* de *downlink*: mantém-se em ≈72 Mbit/s em SISO e ≈143 Mbit/s em MIMO, tanto em LoS como em NLoS, apesar de o RSRP descer de ≈−67 para ≈−82 dBm em SISO e de ≈−66 para ≈−80 dBm em MIMO. Em SISO, o MCS mantém-se em ≈21 a 28 em ambos os cenários, o que explica o *bitrate* constante. Em MIMO, o MCS oscila entre ≈7 e 28 em LoS, mas passa a oscilar apenas entre ≈7 e 14 em NLoS, um valor claramente inferior. Ainda assim o *bitrate* mantém-se em ≈143 Mbit/s; este comportamento sugere uma maior alocação de blocos de recursos (PRBs) ao *downlink* nesse cenário, compensando o MCS mais baixo. O *uplink* sofre uma

ligeira degradação adicional em NLoS (≈14 para ≈13 Mbit/s em SISO; ≈9 para ≈7 Mbit/s em MIMO).

O *Rank Indicator* (RI) reportado pelo *dashboard* da OAIBOX™ foi consistentemente 1 em SISO e 2 em MIMO, em ambos os cenários, coincidindo com o rank máximo esperado para cada configuração segundo a Tabela 8-1 [25] do manual da OAIBOX™.

3.8.4 Cálculos teóricos

3.8.4.1 Capacidade teórica MIMO

O limite teórico de *bitrate* em SISO, pela capacidade de Shannon (secção 2.8.2.2), foi calculado a partir da largura de banda (20 MHz) e do SINR medido (≈23,5 dB):

$$C_{SISO,teo} = 2 \times 10^7 \times \log_2\left(1 + 10^{23,5/10}\right) \approx 156{,}3 \text{ Mbps}$$

Para a configuração MIMO 2x2, aplicando a generalização apresentada na secção 2.8.2.4, com rank 2 (consistente com o *Rank Indicator* medido):

$$C_{MIMO,teo} = 2 \times C_{SISO,teo} \approx 312{,}5 \text{ Mbps}$$

3.8.4.2 Comparação com os valores medidos

A Tabela 3:16 compara estes limites teóricos com o *bitrate* de *downlink* efetivamente medido em cada configuração de antena.

Tabela 3:16 Capacidade de Shannon e bitrate de downlink medido, por configuração de antena

Configuração	SINR medido (dB)	Capacidade de Shannon (Mbit/s)	Bitrate DL medido (Mbit/s)
SISO (1x1)	≈23,5	≈156	≈72
MIMO (2x2)	≈23,5	≈312	≈143

Em ambas as configurações, o *bitrate* medido atinge cerca de 46% do limite de Shannon, a mesma proporção observada na secção 3.3 para a mesma largura de banda. A diferença deve-se ao facto de o modelo de Shannon não descontar a sinalização de referência (DMRS), o canal de controlo (PDCCH) nem a repartição temporal entre *downlink* e *uplink*. Esta proporção manter-se igual entre SISO e MIMO confirma, de forma quantitativa, que o ganho medido corresponde à duplicação de capacidade esperada para rank 2.

3.9 Inspeção Profunda de Pacotes para melhor compreensão do 5G NR

Com o objetivo de compreender a arquitetura em camadas da interface rádio 5G NR e o modo como os dados são encapsulados ao longo das interfaces Uu, N3 e N6, recorreu-se à técnica de *Deep Packet Inspection* (DPI), utilizando o Wireshark configurado com os dissectores específicos para NGAP, NAS-5GS, RRC-NR, PDCP-NR, RLC-NR e MAC-NR, conforme descrito na secção 10.2 do manual da OAIBOX™ [25]. Mantiveram-se os parâmetros de configuração de omissão da plataforma: banda n77, largura de banda de 20 MHz, duplex TDD (configuração de *slots* DDDFU) e MIMO SISO (1x1). A análise dividiu-se em duas partes: o procedimento de registo do gNB junto da AMF (*NG Setup*) e o encapsulamento de um pacote ICMP ao longo das interfaces Uu, N3 e N6.

3.9.1 Procedimento NG Setup

Conforme descrito na secção 2.6.1, o procedimento NG *Setup* estabelece a interface N2 entre o gNB e a AMF através da troca das mensagens *NGSetupRequest* e *NGSetupResponse* [27]. Nesta secção, esse procedimento é observado experimentalmente através de captura de pacotes com o Wireshark.

Após ativar o registo de pacotes (PCAP *Enabled*) na página do gNB e reiniciar o CN5G e o gNB a partir do *dashboard* da OAIBOX™ [19], capturou-se o tráfego na interface oai-cn5g com o filtro “ngap”, tendo-se observado as duas mensagens esperadas com um intervalo de 0,126 ms entre si. A Figura 3-38 apresenta a lista de pacotes capturados, bem como o detalhe dos campos do *NGSetupRequest*, confirmando os parâmetros de identificação do gNB.

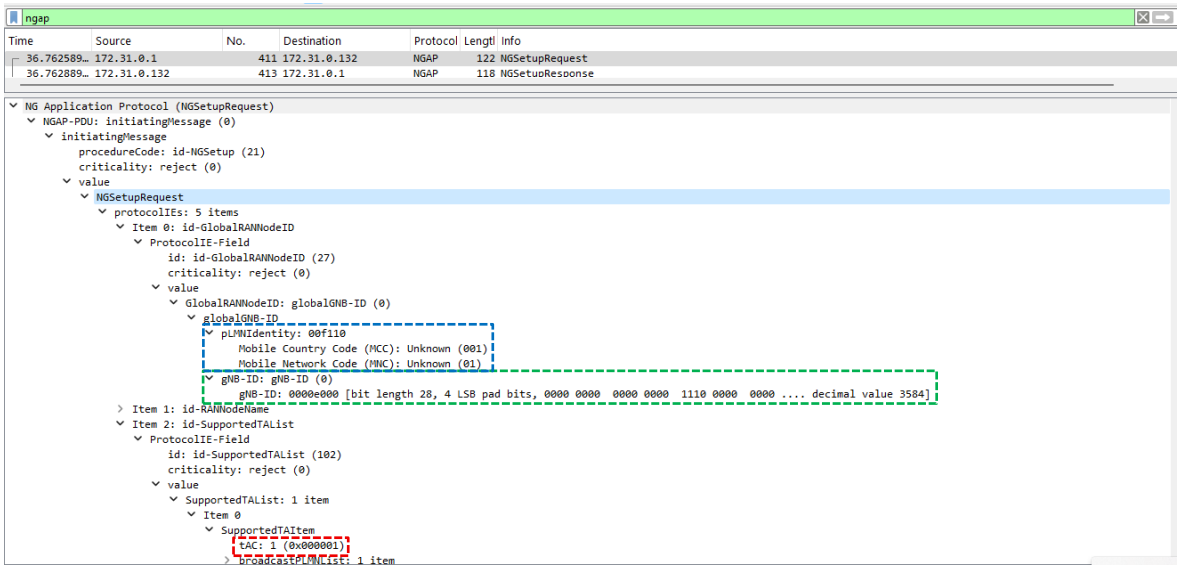


Figura 3-38: Pacotes do procedimento NG Setup (NGSetupRequest e NGSetupResponse) e detalhe dos campos do NGSetupRequest

3.9.2 Encapsulamento de pacotes ICMP entre interfaces 5G NR

Para observar o encapsulamento de dados de utilizador ao longo do sistema 5G, iniciou-se uma nova captura simultaneamente nas interfaces oai-cn5g e Loopback: lo, com o filtro de exibição icmp. A partir do Host PC, executou-se um pedido ICMP de teste (ping -c 1 172.31.0.1) dirigido ao servidor da rede externa (OAI-EXT-DN, endereço 172.31.0.1 neste ambiente de testes).

A Figura 3-39 e a Figura 3-40 apresentam, em conjunto, o pacote correspondente ao *Echo Request* capturado na interface Uu, já com os dissectores MAC-NR/RLC-NR/PDCP-NR corretamente configurados.

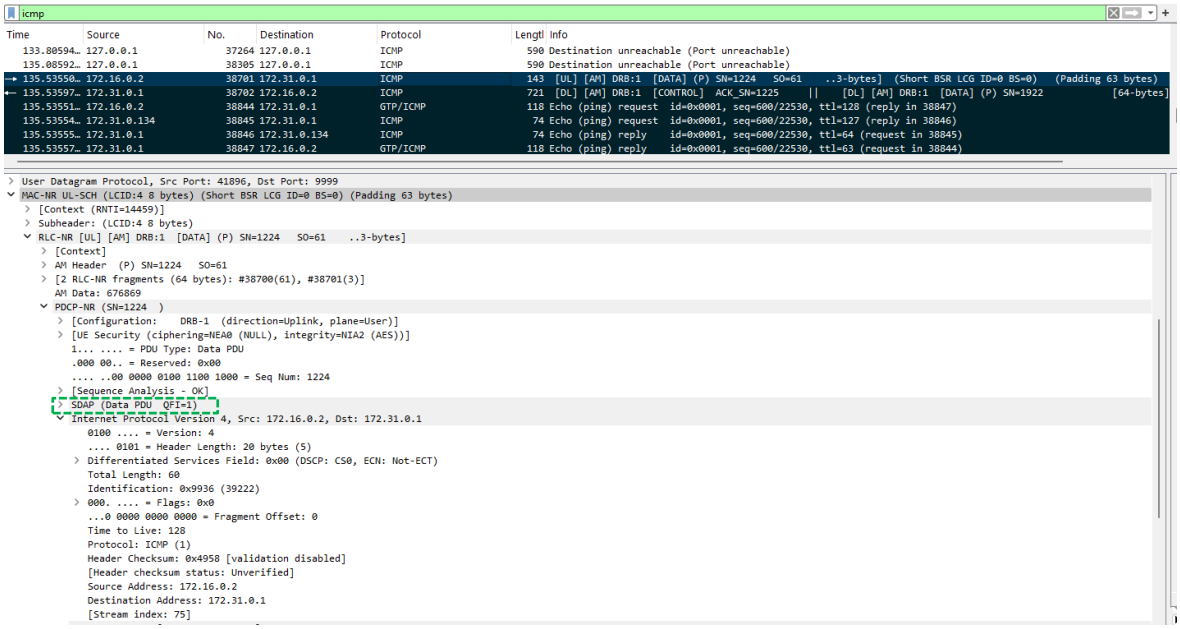


Figura 3-39: Pacotes na interface Uu e camadas MAC-NR/RLC-NR/PDCP-NR/SDAP do pacote ICMP *Echo Request*

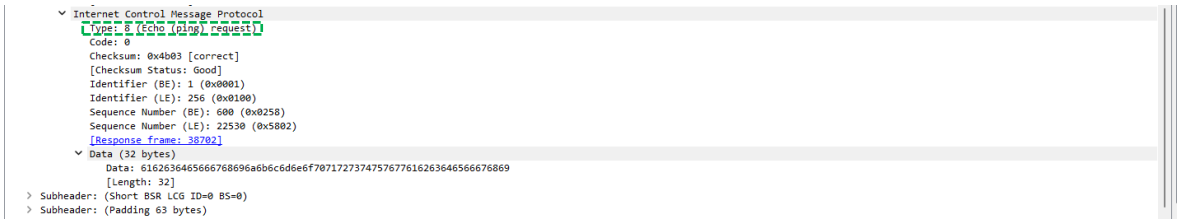


Figura 3-40: Pacote ICMP *Echo Request* na interface Uu

O pacote é segmentado pela camada RLC-NR em dois fragmentos (SN=1224), sendo depois reagrupado e processado pela camada PDCP-NR, que aplica os algoritmos de segurança configurados na rede (ciphering=NEA0, integrity=NIA2). Ao contrário do observado nas interfaces N3 e N6, esta camada apresenta ainda um cabeçalho *SDAP* (QFI=1), confirmando que o mapeamento de QoS *Flow* para a DRB ocorre precisamente nesta fronteira, entre a camada SDAP e a PDCP-NR, ao nível do rádio.

Nas interfaces N3 e N6, capturadas na interface oai-cn5g, observa-se o mesmo pacote em duas formas sucessivas: primeiro encapsulado num túnel GTP-U entre o gNB (172.31.0.1) e o UPF (172.31.0.134), com *TEID* = 0xed805671, e depois, já sem qualquer cabeçalho de túnel, como um datagrama IP/ICMP normal entre o UPF e o destino, após tradução do endereço de origem (NAT) pelo UPF.

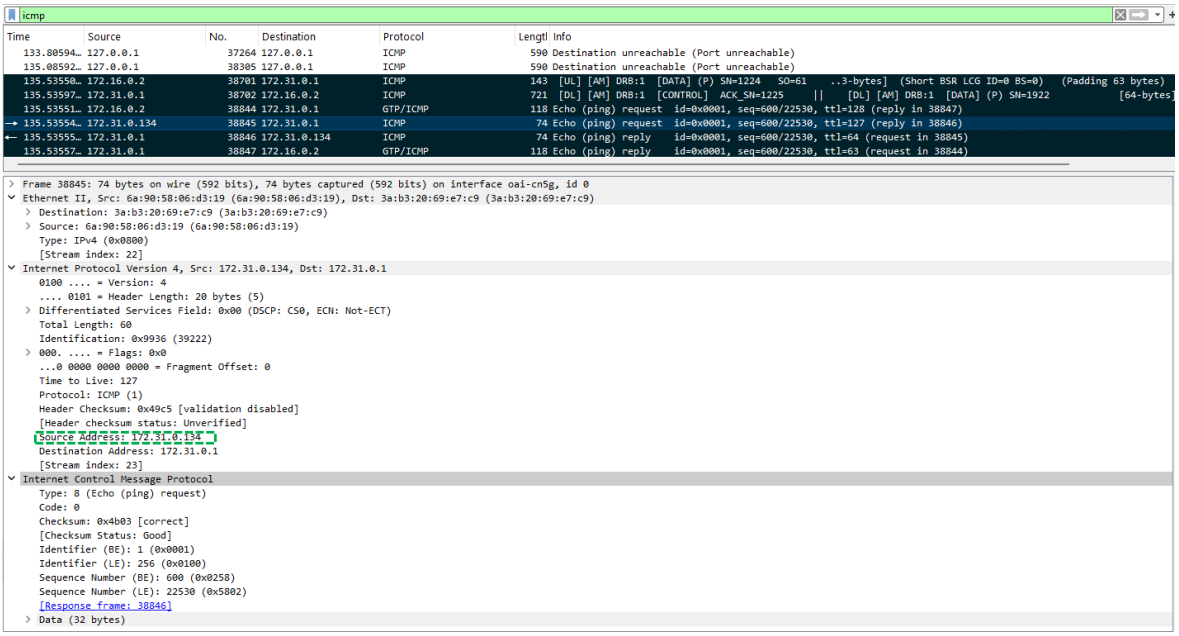


Figura 3-41: Pacotes ICMP nas interfaces N3 e N6, evidenciando a tradução do endereço de origem (NAT) pelo UPF

A Tabela 3:17 resume as três interfaces observadas, incluindo a evolução do valor de *Time-To-Live* (TTL) ao longo do percurso:

Tabela 3:17 Interfaces observadas no encapsulamento do *Echo Request* e evolução do TTL

Interface	Protocolo observado	TTL (request)
Uu (UE → gNB)	ICMP (dentro de MAC-NR/RLC-NR/PDCP-NR/SDAP)	128
N3 (gNB ↔ UPF)	GTP/ICMP (túnel GTP-U)	128
N6 (UPF ↔ destino)	ICMP puro (sem GTP-U, com NAT)	127

O TTL mantém-se constante entre as interfaces Uu e N3 (128), confirmando que o encapsulamento GTP-U é transparente ao pacote original; só ao ser efetivamente encaminhado pelo UPF, na interface N6, o TTL é decrementado em uma unidade (128-127), como esperado de um salto IP normal.

3.9.3 Registo do gNB na AMF

- O gNB regista-se junto da AMF.
- O procedimento normalizado designa-se NG *Setup procedure*.
- Os parâmetros PLMN (MCC/MNC) e o Tracking Area Code (TAC) devem coincidir entre o gNB (plmn_list, tracking_area_code em *OAIBOX™.yaml*) e a AMF (plmn_support_list em config.yaml); caso contrário, a AMF rejeita o *NGSetupRequest* por não reconhecer o PLMN/TAC anunciado.
- A sinalização NGAP é transportada sobre SCTP sobre IP, na interface N2 (NG-C), conforme confirmado na captura (frames 411/413, portas 56137/38412).

3.9.4 Interfaces atravessadas pelo tráfego de utilizador

Conforme descrito na secção 2.5, o tráfego de utilizador atravessa as interfaces Uu (UE ↔ gNB, via rádio), N3 (gNB ↔ UPF, túnel GTP-U sobre UDP) e N6 (UPF ↔ rede externa). Isto acontece porque, como apresentado na arquitetura protocolar da secção 2.4, o

SDAP/PDCP/RLC/MAC do gNB trata o pacote apenas ao nível do rádio; a partir daí, o UPF assume o encaminhamento IP para fora do sistema 5G, sendo necessário o túnel GTP-U (N3) para transportar o pacote entre o gNB e o núcleo, e o N6 para o reencaminhar ao destino final.

3.9.5 Relação entre a topologia e os pacotes observados

A topologia apresentada na Figura 10-2 do manual [25], consistente com as interfaces já descritas na secção 2.5, identifica os pontos de captura correspondentes às interfaces Uu, N3 e N6. Os pacotes observados na Figura 3-39 e na Figura 3-41 confirmam exatamente esse percurso: o pacote é gerado pelo UE e enviado pelo rádio (Uu), reencaminhado pelo gNB através de um túnel GTP-U até ao UPF (N3), e finalmente entregue ao destino já sem encapsulamento, após tradução de endereço (N6). A correspondência entre a arquitetura teórica e os dados capturados confirma que cada interface foi corretamente identificada e associada ao respetivo troço da rede.

3.9.6 TTL constante entre Uu e N3

O TTL do pacote IP interno permanece inalterado entre Uu e N3 porque o GTP-U é um mecanismo de tunelamento transparente [28]: o gNB e o UPF acrescentam um cabeçalho externo (Ethernet/IP/UDP/GTP-U) sem desencapsular nem alterar o pacote original; só o UPF, na saída para a rede externa (N6), remove esse cabeçalho. Como o TTL pertence ao cabeçalho IP interno, e este não sofre encaminhamento enquanto viaja dentro do túnel, o valor mantém-se inalterado até ser efetivamente encaminhado como pacote IP normal na interface N6, tal como confirmado experimentalmente na Tabela 3:17.

3.9.7 Diagrama de encapsulamento do Echo Request

A Figura 3-42 ilustra o encapsulamento do pacote ICMP *Echo Request* ao longo das três interfaces observadas neste trabalho. Na interface *Uu*, o pacote é processado pela pilha de protocolos do rádio (MAC-NR, RLC-NR, PDCP-NR e SDAP). Na interface *N3*, o gNB encapsula o mesmo pacote IP/ICMP num túnel GTP-U, sem o alterar. Na interface *N6*, o UPF remove o túnel e traduz o endereço de origem (NAT), mantendo o *payload* ICMP inalterado em todas as interfaces.

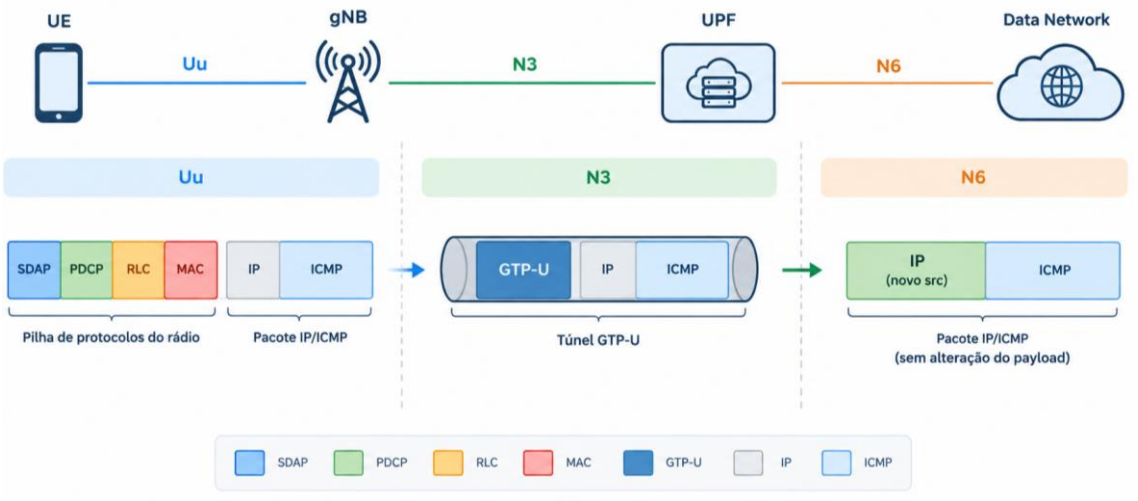


Figura 3-42: Diagrama do encapsulamento do pacote ICMP nas interfaces Uu, N3 e N6

3.9.8 Presença do cabeçalho SDAP

Ao contrário do que o enunciado desta pergunta assume por omissão, a captura efetuada neste trabalho (Figura 3-39) revela a presença do cabeçalho SDAP no pacote ICMP capturado na interface Uu, com um QFI=1.

Como descrito na secção 2.4, o SDAP é responsável pelo mapeamento dinâmico de QoS *Flows* para DRBs [15], sendo o seu cabeçalho incluído sempre que a configuração da rede o define explicitamente (*sdap-HeaderUL: present, sdap-HeaderDL: present*), independentemente de existir ou não mapeamento de múltiplos QoS *Flows*. A presença observada neste trabalho revela, portanto, que a configuração desta rede opta por incluir explicitamente a identificação do QoS *Flow* em cada PDU, mesmo com um único fluxo por omissão, o que facilita a inspeção e a depuração do tráfego, em detrimento de uma ligeira redução de eficiência.

Em suma, este laboratório confirmou experimentalmente o percurso completo de um pacote entre o UE e uma rede externa: o registo prévio do gNB junto da AMF (NG *Setup*), o encapsulamento em GTP-U na interface N3 e a sua remoção com tradução de endereço na interface N6, mantendo o TTL constante ao longo do túnel. Ao contrário do esperado pelo enunciado, a interface Uu revelou a presença do cabeçalho SDAP, facto explicado no ponto 3.9.8 com base na especificação 3GPP.

3.9.9 Medição da latência entre interfaces

Para complementar a análise anterior, mediu-se a latência introduzida por cada interface no percurso do pacote ICMP *Echo Request*/*Reply*, aproveitando a captura simultânea já efetuada nas interfaces oai-cn5g e Loopback: lo. A Figura 3-43 apresenta a lista de pacotes correspondente, identificando o mesmo pacote (id=0x0001, seq=600/22530) nas seis passagens sucessivas: Uu (*request)*, N3 (*request*), N6 (*request*), N6 (*reply*), N3 (*reply)* e Uu (*reply*), através da coluna *Time*.

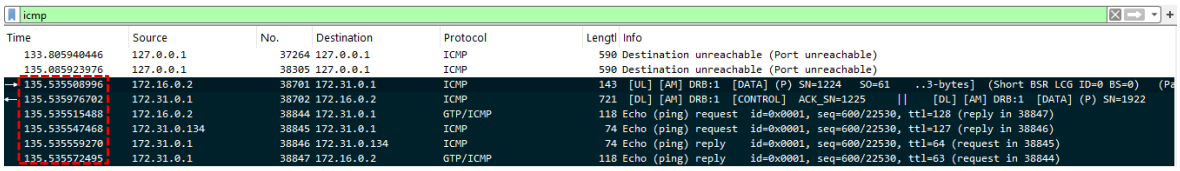


Figura 3-43: Lista de pacotes ICMP nas interfaces Uu, N3 e N6, evidenciando o campo Time para cálculo da latência

A partir dos valores da coluna *Time* de cada *frame* identificado na Figura 3-43, calculou-se a latência acumulada em cada troço do percurso, subtraindo sucessivamente os *timestamps* correspondentes. A Tabela 3:18 resume os resultados obtidos.

Tabela 3:18 Latência acumulada entre interfaces (Echo Request/Reply)

Troço	Cálculo (s)	Latência
Uu → N3 (request)	135,535515488 − 135,535508996	6,49 µs
N3 → N6 (request)	135,535547468 − 135,535515488	31,98 µs
N6 (processamento no servidor)	135,535559270 − 135,535547468	11,80 µs
N6 → N3 (reply)	135,535572495 − 135,535559270	13,23 µs
N3 → Uu (reply)	135,535976702 − 135,535572495	404,21 µs
RTT total (Uu → Uu)	135,535976702 − 135,535508996	467,71 µs

Os resultados evidenciam uma disparidade de ordens de grandeza entre os troços internos (N3/N6), na ordem das dezenas de microssegundos (6,49 a 31,98 µs), e o troço final de rádio (N3→Uu, reply), responsável isoladamente por cerca de 404 µs, mais de 85% da latência total medida (467,71 µs). Esta diferença resulta do escalonamento TDD da interface rádio (secção 2.8.2.3): enquanto o encaminhamento IP interno é imediato, a transmissão em *downlink* depende da disponibilidade do próximo *slot* atribuído a essa direção, ao contrário da comutação no núcleo de rede, que não está sujeita a este tipo de espera.

O *Round-Trip Time* (RTT) obtido (467,71 µs) situa-se abaixo do limiar de 1 ms definido pela IMT-2020 para serviços URLLC (Tabela 1:3) ainda que este resultado deva ser interpretado com reserva: o ensaio decorreu com um único UE, sem contenção de recursos rádio nem retransmissões HARQ, condições que não se verificam necessariamente em cenários de utilização comercial. Ainda assim, confirma-se experimentalmente que o núcleo de rede não constitui, por si só, um fator limitativo para os requisitos de baixa latência do 5G NR, cabendo à interface rádio o papel determinante no desempenho *end-to-end*.

3.10 Compreender a Segurança no 5G NR

Recorreu-se à técnica de DPI para observar experimentalmente os mecanismos de segurança do 5G NR descritos teoricamente na secção 2.7, nomeadamente a ocultação do SUPI através do SUCI, a negociação de algoritmos de segurança NAS e AS, e a proteção (cifra e integridade) aplicada às *Data Radio Bearers* (DRBs). Mantiveram-se os parâmetros de configuração de omissão da plataforma: banda n77, largura de banda de 20 MHz, duplex TDD (configuração de *slots* DDDFU) e MIMO SISO (1x1), com cifra NEA0 e integridade desativada, conforme detalhado na subsecção seguinte.

3.10.1 Algoritmos de segurança configurados

O ficheiro *config.yaml* da AMF define os algoritmos de segurança suportados pela rede, por ordem de prioridade: NIA2 > NIA1 > NIA0 para integridade, e NEA0 > NEA2 > NEA1 para cifra como mostra a Figura 3-44.

```
supported_integrity_algorithms:
- NIA2
- NIA1
- NIA0
supported_encryption_algorithms:
- NEA0
- NEA2
- NEA1
```

Figura 3-44: config.yaml, algoritmos de integridade e cifra suportados pela AMF

Ao nível de acesso (AS), a página do gNB no *dashboard* da OAIBOX™ (Figura 3-45) confirma a mesma ordem de prioridade, com o toggle *Ciphering Algorithms* ativado e o toggle *Integrity Algorithms* desativado por omissão, significando que as DRBs não têm, por omissão, proteção de integridade ativa, embora a cifra esteja habilitada.

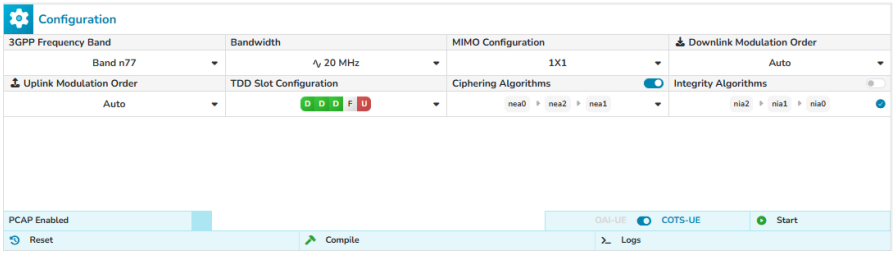


Figura 3-45: dashboard do gNB, configuração por omissão

3.10.2 Procedimento de segurança NAS

Após ativar o registo de pacotes (PCAP Enabled) e iniciar uma captura simultânea nas interfaces oai-cn5g e Loopback: lo com o filtro de exibição ngap, conforme descrito na secção 2.6.2, o registo do UE inicia-se com o envio de uma mensagem *Registration Request*, na qual o UE reporta as suas capacidades de segurança e a sua identidade.

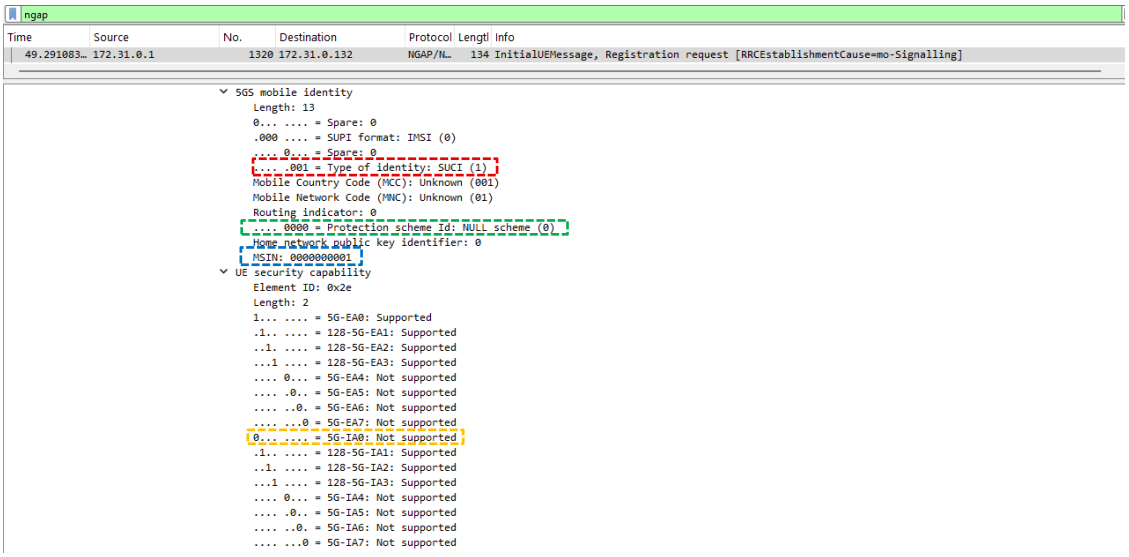


Figura 3-46: InitialUEMessage/Registration Request, campos 5GS mobile identity e UE Security Capability

No mesmo pacote, o campo *5GS mobile identity* confirma que a identidade é transmitida como SUCI consistente com o descrito na secção 2.7.4.2, uma vez que se trata do primeiro registo do UE na rede. O esquema de proteção utilizado é o *NULL scheme*, ou seja, sem ocultação criptográfica do IMSI/SUPI subjacente, pelo que o identificador do assinante (MSIN: 0000000001) permanece visível em texto claro. No campo *UE security capability*, destaca-se ainda a ausência de suporte ao algoritmo 5G-IA0, confirmando que o UE nunca aceitaria uma ligação totalmente sem proteção de integridade. A norma TS 33.501 [13] exige a proteção de integridade do NAS como obrigatória em condições normais de registo, contrariamente à cifra, cuja ativação é opcional.

3.10.3 Procedimento de autenticação (5G-AKA)

Entre o *Registration Request* e o *NAS Security Mode Command*, observa-se o procedimento de autenticação mútua 5G-AKA, através da troca das mensagens *Authentication Request* e *Authentication Response*.

Na mensagem *Authentication Request* (Figura 3-47), a rede envia ao UE o parâmetro RAND, um valor aleatório gerado pela AUSF, e o AUTN, um *token* de autenticação que

inclui o campo MAC, calculado a partir da chave permanente K partilhada entre o USIM e a UDM (secção 2.7.6). O UE recalcula este MAC localmente a partir do mesmo K e do RAND recebido, e só aceita a rede como legítima se o valor coincidir, uma vez que só uma rede com acesso à chave K correta poderia tê-lo gerado.

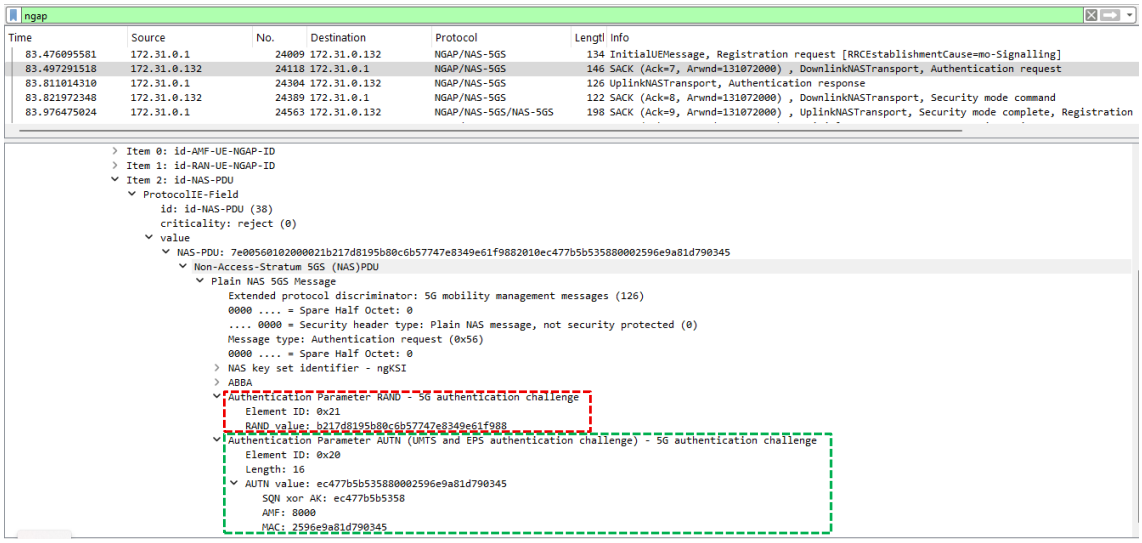


Figura 3-47: Authentication request, campos RAND e AUTN

Na mensagem *Authentication Response* (Figura 3-48), o UE devolve o RES*, calculado a partir do RAND recebido e da própria chave K. A rede compara este valor com o XRES* calculado localmente pela AUSF a partir dos mesmos parâmetros e, em caso de coincidência, autentica o UE como legítima.

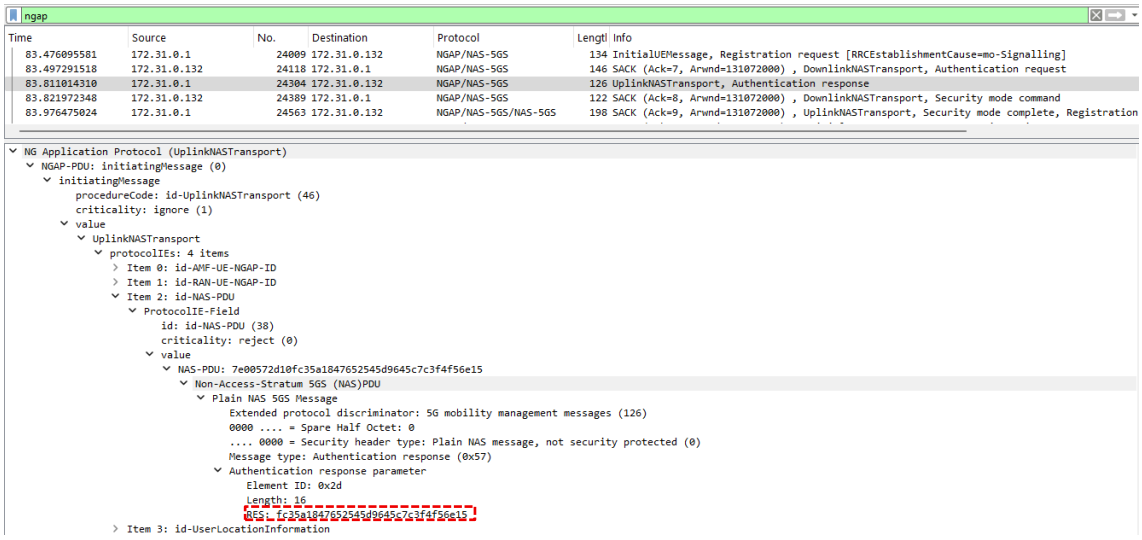


Figura 3-48: Authentication response, campo RES*

Este mecanismo bidirecional, o UE valida a rede através do MAC embutido no AUTN, e a rede valida o UE através do RES*, sustenta o caráter mútuo da autenticação 5G-AKA.

Após receber as capacidades do UE, a rede seleciona os algoritmos de segurança NAS através da mensagem *NAS Security Mode Command* (Figura 3-49): 5G-EA0 (cifra nula) e 128-5G-IA2 (AES-CMAC), correspondendo à prioridade máxima definida no *config.yaml* que o UE também suporta. A mensagem inclui um *Message Authentication Code* (0xe207d958), calculado pela rede a partir da chave de integridade NAS (K_NASint)

através do algoritmo selecionado, confirmando a proteção de integridade mesmo sem cifra ativa. A mesma mensagem reenvia ainda ao UE as capacidades de segurança por esta reportadas inicialmente (Figura 3-50), permitindo confirmar que não foram alteradas em trânsito por um eventual atacante que tentasse forçar a seleção de algoritmos mais fracos.

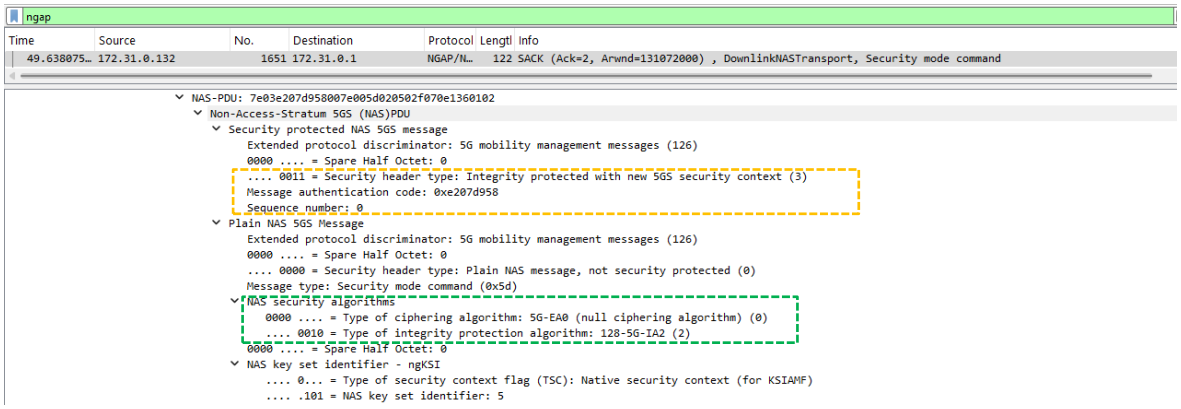


Figura 3-49: NAS Security Mode Command, algoritmos selecionados e Message Authentication Code

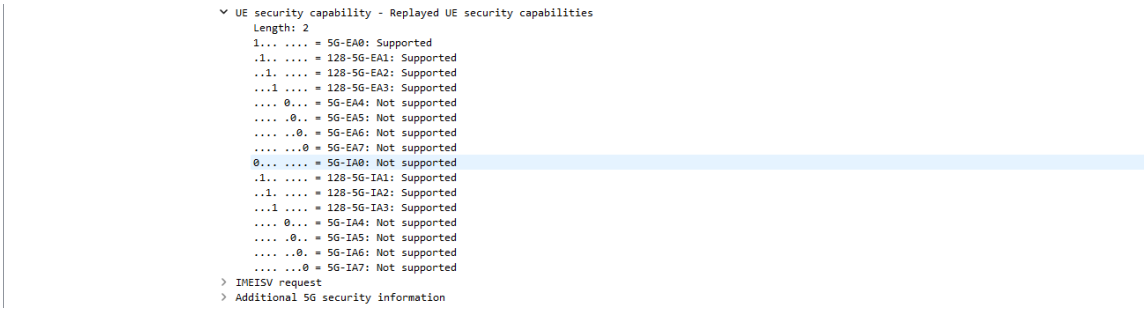


Figura 3-50: NAS Security Mode Command, capacidades de segurança do UE reenviadas pela rede (Replayed UE security capabilities)

A resposta do UE, mensagem *NAS Security Mode Complete* (Figura 3-51), confirma a ativação da cifra e da integridade através do *Security header type* "*Integrity protected and ciphered with new 5GS security context*", com um MAC (0x36f84eab). Nesta mensagem, o UE reporta ainda a sua identidade IMEISV e reencaminha, embutida num *NAS message container*, a mensagem *Registration Request* original enviada em claro no início do procedimento, mecanismo que permite à rede validar retroativamente essa mensagem inicial, agora sob proteção de integridade.

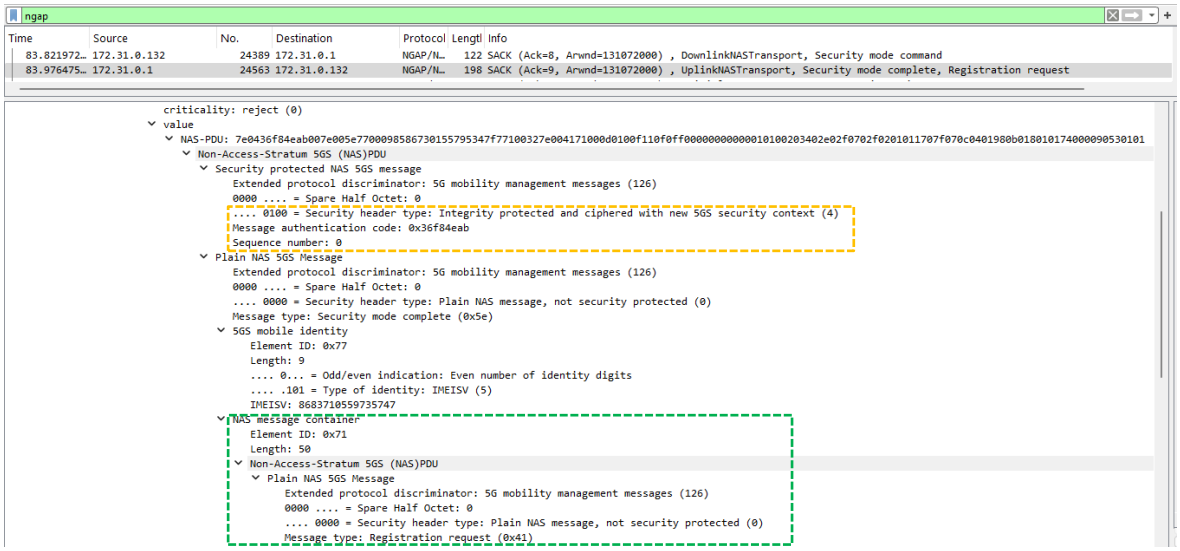


Figura 3-51: NAS Security Mode Complete, confirmação de cifra e integridade

3.10.4 Procedimento de segurança AS

A proteção ao nível de acesso (AS), entre o UE e o gNB, só é ativada depois de estabelecido o contexto de segurança NAS descrito na subsecção anterior. Este processo é iniciado pelo envio, da AMF para o gNB, da mensagem *InitialContextSetupRequest* (Figura 3-52), que transporta os elementos necessários para o gNB estabelecer a sua própria proteção de segurança.

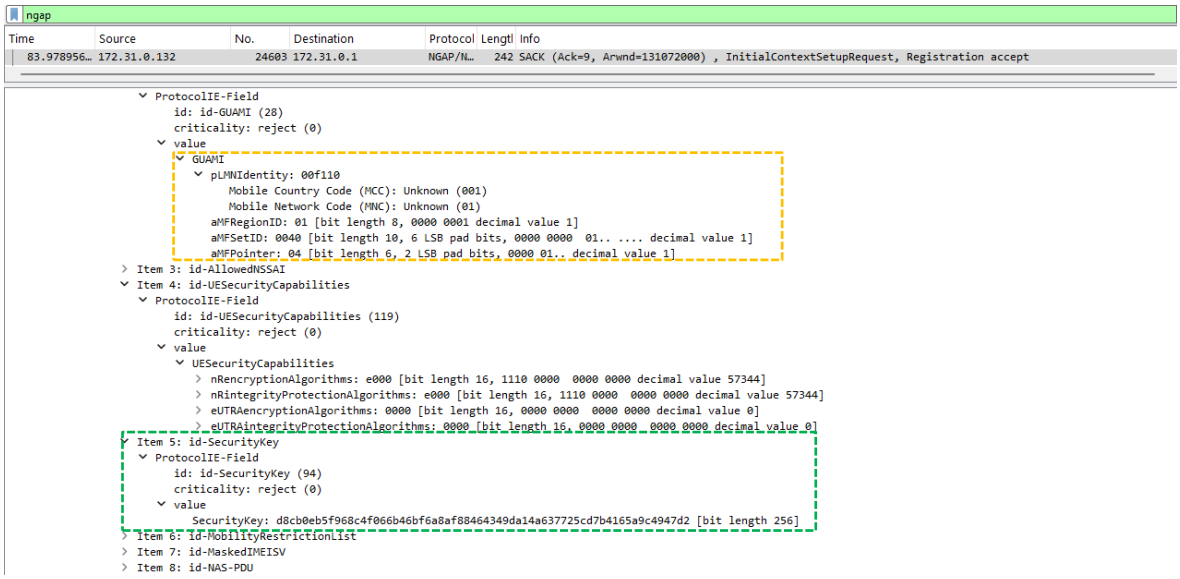


Figura 3-52: InitialContextSetupRequest, campos GUAMI e SecurityKey

Os valores observados nestes três campos estão resumidos na Tabela 3:19.

Tabela 3:19 InitialContextSetupRequest, campos GUAMI e SecurityKey

Campo	Valor observado	Significado
GUAMI (PLMN)	001/01	Identifica a rede móvel doméstica, coincidindo com o PLMN já confirmado no NG *Setup*
GUAMI (AMF Region/Set/Pointer)	1 / 1 / 1	Identifica de forma única a instância da AMF que serve este UE
UESecurityCapabilities	e000 (cifra e integridade)	Reencaminhamento, sem alteração, das capacidades reportadas pelo UE na *Registration Request*
SecurityKey (K_gNB)	256 bits	Chave-base a partir da qual o gNB deriva as chaves de cifra e integridade para RRC e para o plano de utilizador

A partir da chave K_gNB, o gNB deriva localmente as chaves de cifra (K_RRCenc, K_UPenc) e de integridade (K_RRCint, K_UPint) que serão utilizadas nas mensagens RRC e no tráfego de utilizador, sem que estas chaves derivadas necessitem de ser transmitidas pela rede.

Ao nível de acesso (AS), a mensagem *AS Security Mode Command* (Figura 3-53) confirma, no campo *securityAlgorithmConfig*, a seleção dos algoritmos nea0 (cifra nula) e nia2 (AES-CMAC), coincidindo com os algoritmos já selecionados ao nível NAS. A camada PDCP-NR anota ainda estes mesmos algoritmos automaticamente (*ciphering*=NEA0, *integrity*=NIA2), e o campo *MAC* (0x61d8131b) confirma a proteção de integridade desta mensagem RRC. Alterou-se o filtro de exibição do Wireshark para nr-rrc, permitindo observar as mensagens RRC subsequentes.

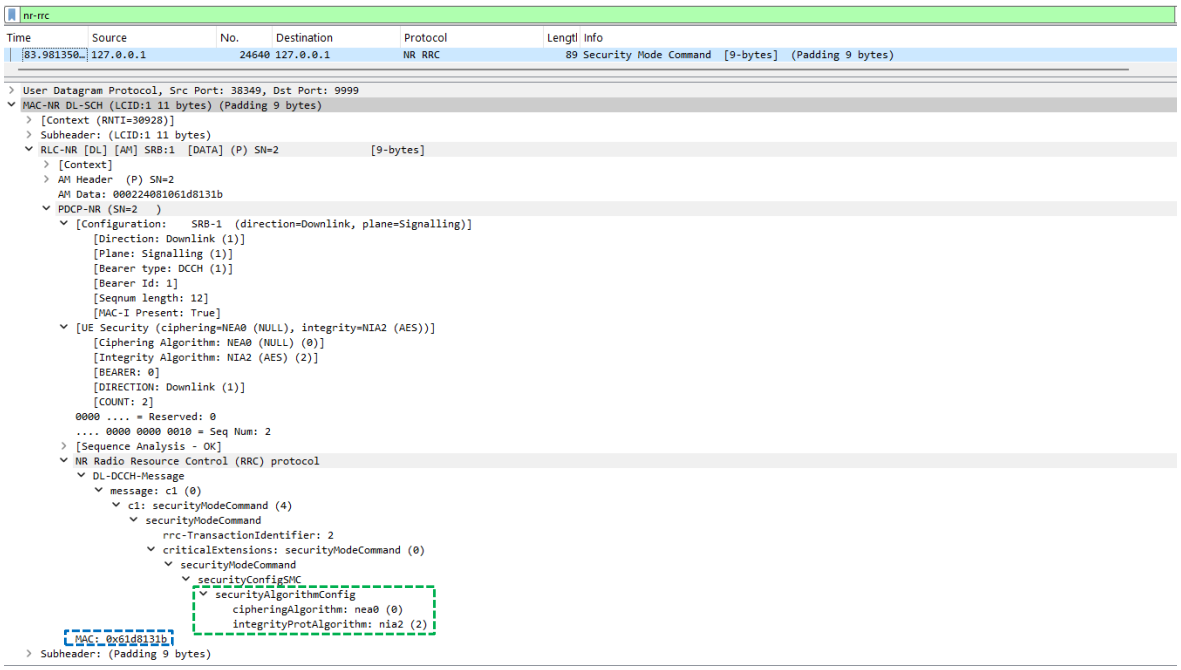


Figura 3-53: AS Security Mode Command, securityAlgorithmConfig e MAC

A mensagem *RRC Reconfiguration* (Figura 3-54) estabelece a configuração da DRB (drb-*Identity*: 1), incluindo o bloco pdcp-Config. Não são transmitidos os campos *cipheringDisabled* nem *integrityProtection*: segundo a especificação 3GPP TS 38.331 [2], estes campos só são incluídos quando o respetivo mecanismo se desvia do valor por

omissão (cifra ativa, integridade desativada), situação que corresponde exatamente à configuração observada no *dashboard* (Figura 3-45). A sua ausência confirma, portanto, indiretamente, que a DRB mantém a configuração por omissão.

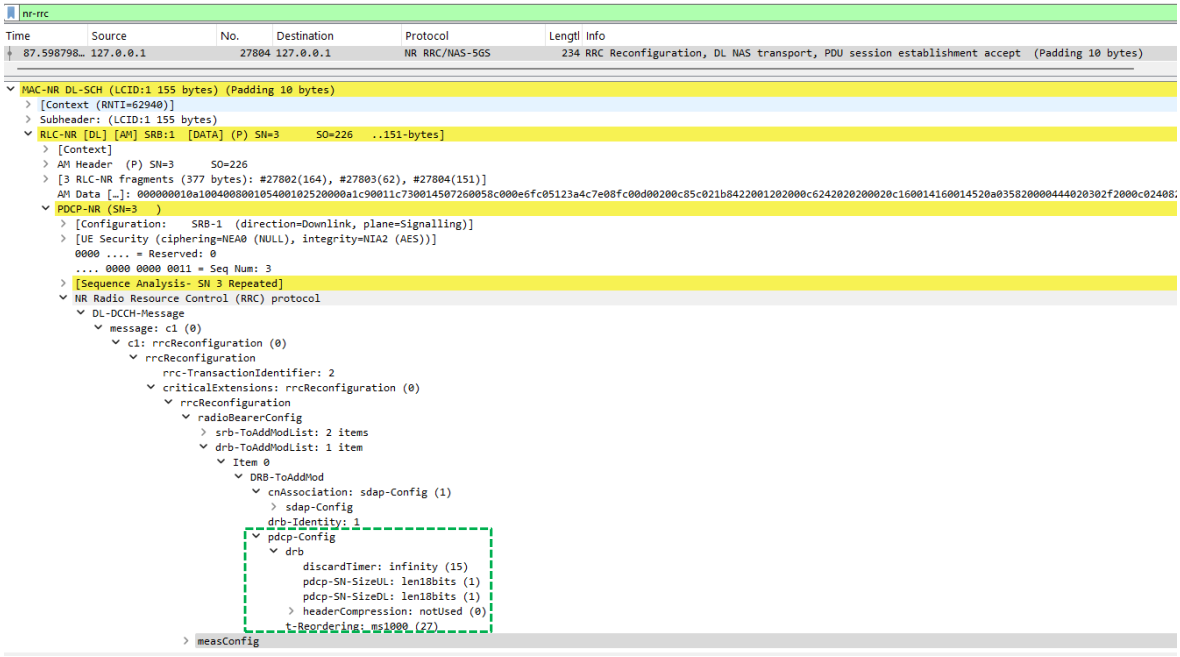


Figura 3-54: RRC Reconfiguration, pdcp-Config da DRB (ausência de cipheringDisabled/integrityProtection)

3.10.5 Proteção da mensagem NAS do UE até à SMF

A mensagem *PDU Session Establishment Request*, do tipo NAS-SM, percorre três troços até chegar à SMF. Cada um tem o seu próprio mecanismo de proteção.

No primeiro troço, entre o UE e o gNB, a mensagem viaja dentro de um contentor RRC, protegido pelas chaves K_RRCenc e K_RRCint. O conteúdo NAS-SM não tem contexto de segurança próprio. É antes transportado embutido como *payload container*, dentro de uma mensagem NAS-MM *UL NAS Transport*, capturada na interface N2 (Figura 3-55), com o *Security header type* assinalado como *Integrity protected and ciphered*, acompanhado do respetivo código de autenticação.

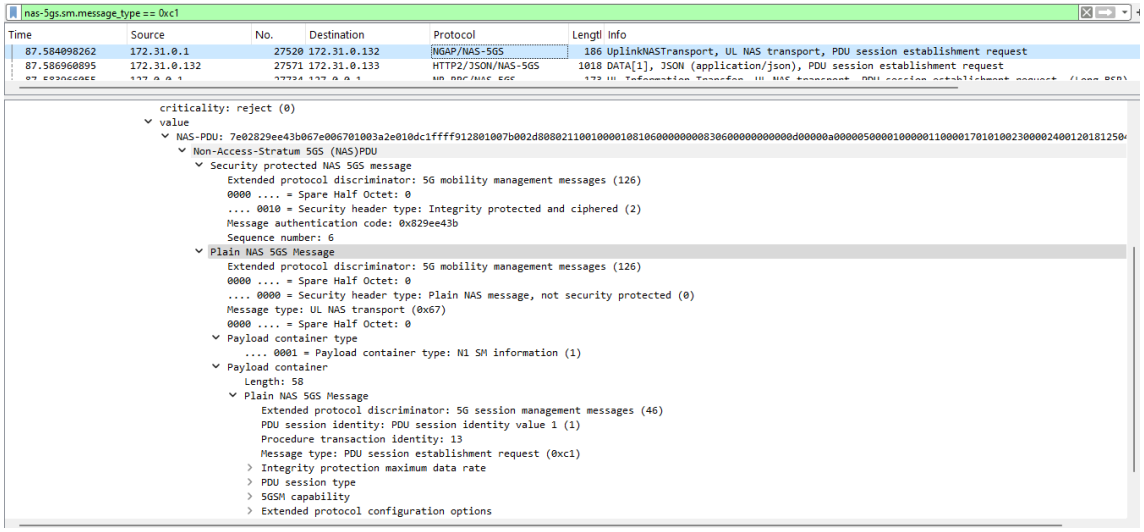


Figura 3-55: Security header type e payload container da mensagem UL NAS Transport, interface N2

A mensagem chega à AMF ainda cifrada, através da interface N2. É aí que é decifrada. O PDU NAS-SM é então extraído e reencaminhado à SMF, através da interface N11, em HTTP/2, num corpo *multipart/related* com duas partes: a primeira, em JSON, com os metadados do pedido, entre os quais os campos *supi*, *guami*, *pduSessionId* e *n1SmMsg* (Figura 3-56).

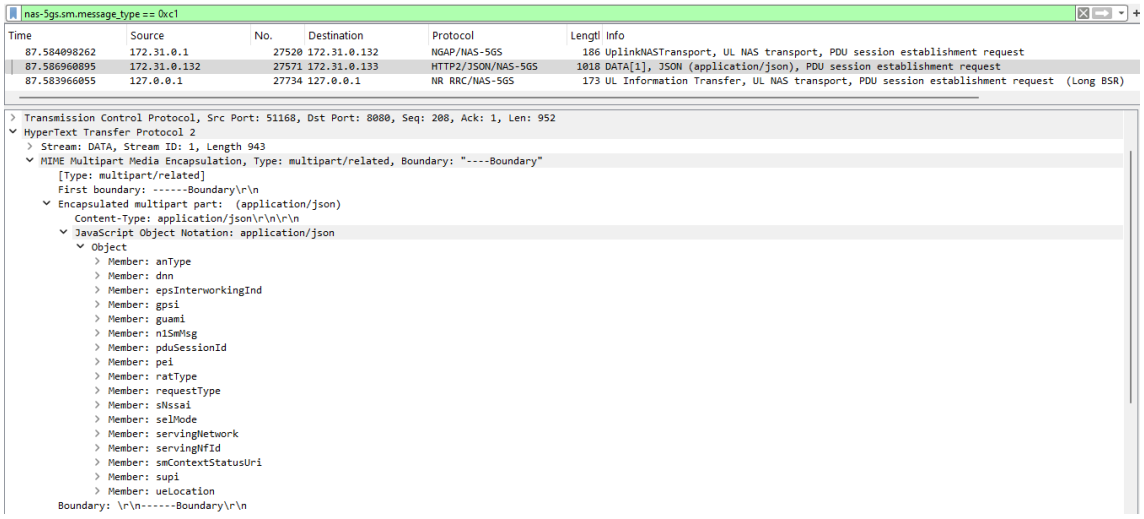


Figura 3-56: Parâmetros JSON do reencaminhamento à SMF, interface N11

A segunda parte, identificada pelo *Content-Id: n1SmMsg* (Figura 3-57), corresponde ao PDU NAS-SM já em claro, confirmando a mensagem *PDU session establishment request*, associada à *PDU session identity* 1.

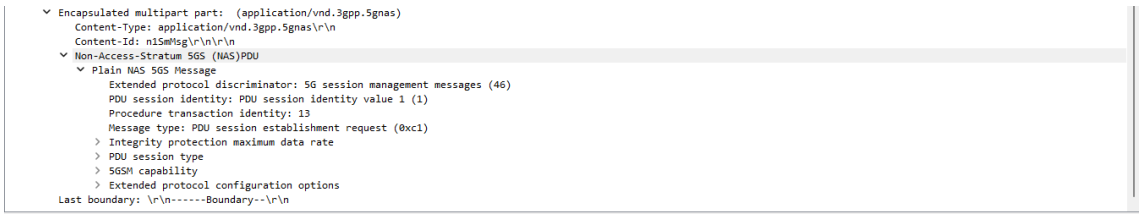


Figura 3-57: Conteúdo NAS-SM em claro reencaminhado à SMF

O campo SUPI circula sem cifra entre a AMF e a SMF, ao contrário da interface rádio, onde o SUPI nunca é exposto (secção 2.7.4.2). A proteção de privacidade do 5G aplica-se, assim, especificamente à interface rádio; entre funções do core já autenticadas mutuamente, a identidade resolvida circula em claro, salvaguardada apenas pela proteção de transporte da interface N11.

Ao contrário do previsto na TS 33.501 [13] para a N11 (secção 2.3), a captura não revela nenhuma camada TLS entre o TCP e o HTTP/2. Neste ambiente experimental, a comunicação entre a AMF e a SMF ocorre em texto claro, à semelhança do *Null-scheme* já observado na cifra do SUCI.

Pressuposto assumido: o contexto de segurança NAS já estava ativo antes deste pedido, por já ter ocorrido o procedimento de registo e autenticação descrito anteriormente.

3.10.6 Proteção do plano de utilizador

Para observar o efeito prático da cifra e da integridade sobre o tráfego de utilizador, testou-se, a partir do Host PC, um pedido ping dirigido ao servidor da rede externa (OAI-EXT-DN, endereço 172.31.0.1 neste ambiente de testes). Capturou-se o tráfego simultaneamente nas interfaces oai-cn5g e Loopback: lo, identificando primeiro o instante temporal do pedido ICMP através do filtro icmp na interface oai-cn5g, e aplicando depois, na interface Loopback: lo, o filtro pdcp-nr restringido a esse intervalo temporal, para isolar os pacotes PDCP-NR correspondentes.

Este teste foi repetido em três configurações do gNB:

- com cifra NEA0 e sem integridade (configuração por omissão);
- com a integridade ativada;
- com a cifra restrita a NEA2.

3.10.6.1 Com cifra NEA0 e sem integridade (configuração por omissão)

Enviou-se um pedido ping do Host PC para o OAI-EXT-DN (172.31.0.1), capturando-se simultaneamente as interfaces oai-cn5g e Loopback: lo com o filtro pdcp-nr, restringido ao intervalo temporal do pedido ICMP. Identificaram-se assim os dois pacotes PDCP-NR correspondentes, um em *Downlink* (SN=150951) e outro em *Uplink* (SN=50864), ambos na DRB-1 (Figura 3-58 e Figura 3-59).

Em ambos, o cabeçalho PDCP-NR limita-se aos campos PDU *Type*, *Reserved* e *Sequence Number*, seguidos diretamente do campo Data, sem qualquer campo MAC-I. Esta observação é consistente com a configuração por omissão já identificada (Figura 3-45).

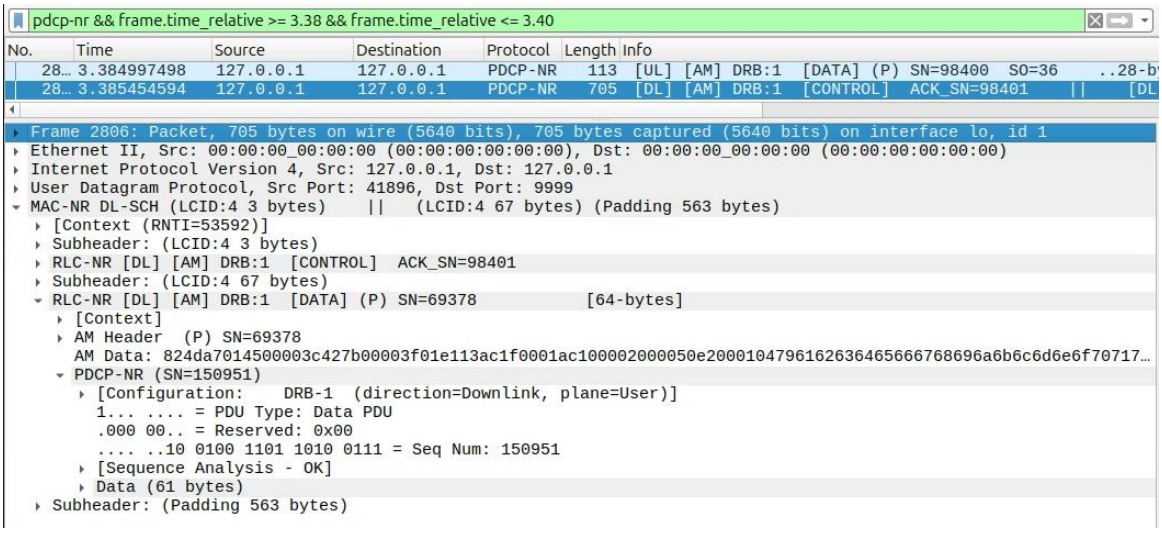


Figura 3-58: PDCP-NR, pacote Downlink (SN=150951)

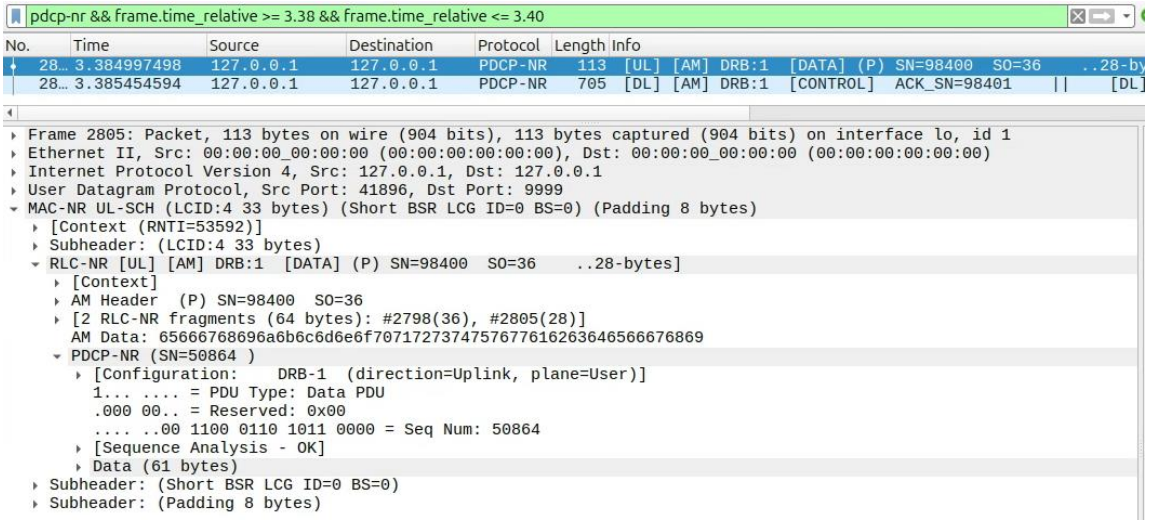


Figura 3-59: PDCP-NR, pacote Uplink (SN=50864)

3.10.6.2 Com a integridade ativada

A Figura 3-60 apresenta a configuração do *dashboard* com o *toggle Integrity Algorithms* ativado.

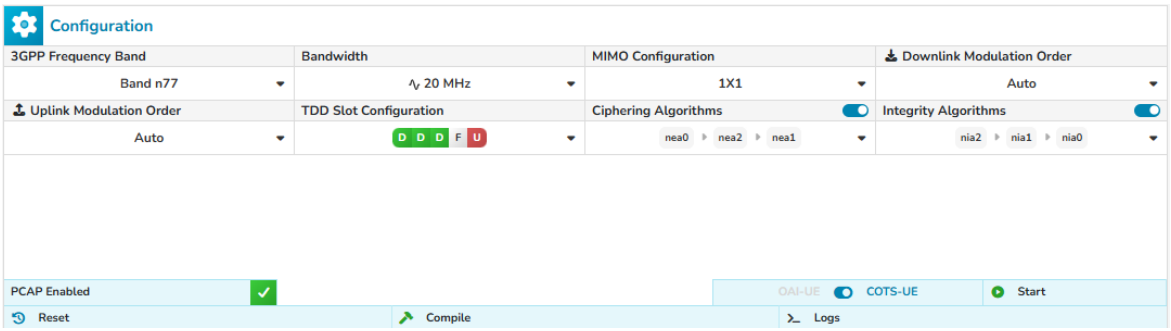


Figura 3-60: dashboard do gNB, integridade ativada

Identificaram-se os pacotes PDCP-NR correspondentes ao novo pedido ping, em *Downlink* (SN=2314) e *Uplink* (SN=2022), ambos na DRB-1 (Figura 3-61 e Figura 3-62).

Em ambos os pacotes, o campo Data apresenta 65 bytes, mais 4 bytes do que na configuração anterior sem integridade (61 bytes). Esta diferença corresponde ao tamanho do campo MAC-I (32 bits), especificado pela norma 3GPP TS 38.323 [4], confirmando a ativação da proteção de integridade nesta configuração. Não foi possível isolar visualmente o campo MAC-I no Wireshark, uma vez que o dissector do PDCP-NR não dispõe das chaves de segurança da sessão necessárias para o distinguir do restante *payload*.

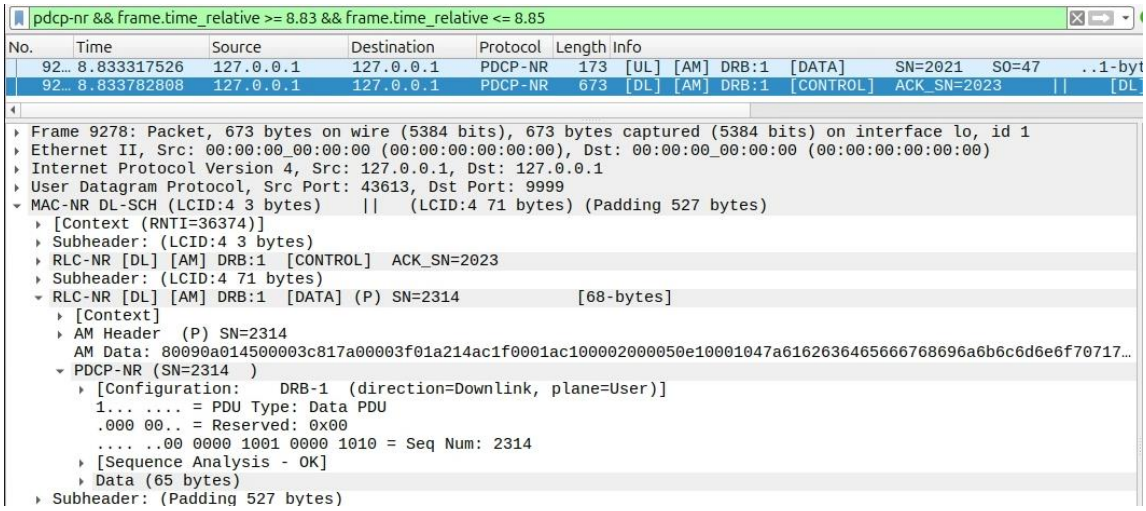


Figura 3-61: PDCP-NR, pacote Downlink (SN=2314), campo Data com 65 bytes

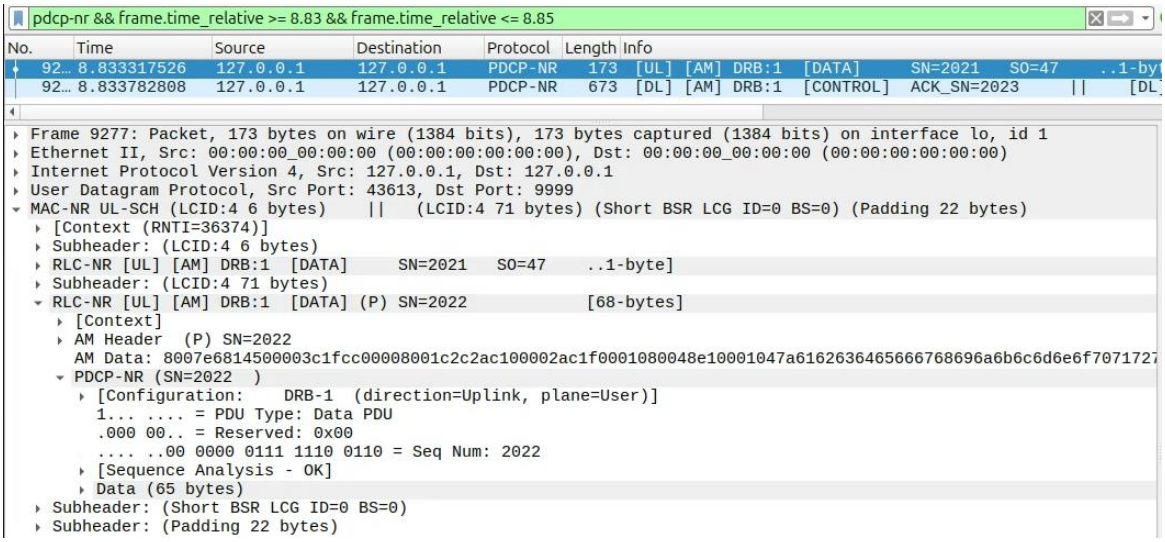


Figura 3-62: PDCP-NR, pacote Uplink (SN=2022), campo Data com 65 bytes

3.10.6.3 Com a cifra restrita a NEA2

A Figura 3-63 apresenta a configuração do *dashboard* com o algoritmo de cifra restrito a NEA2.

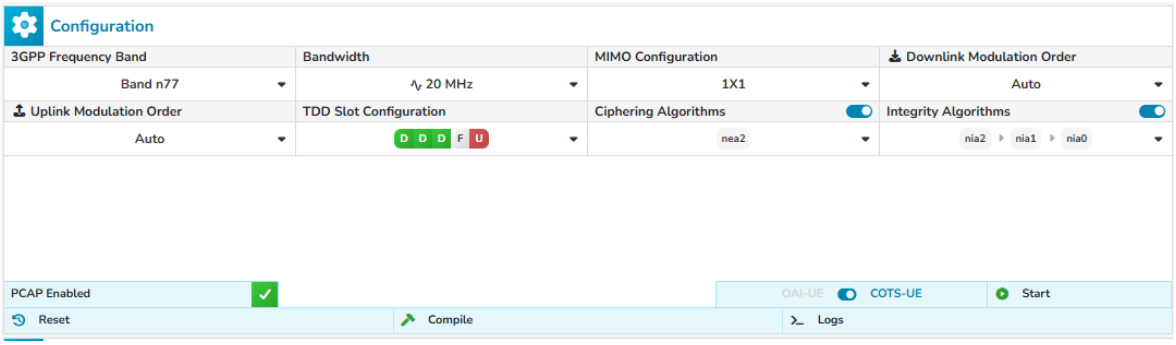


Figura 3-63: Dashboard do gNB, cifra restrita a NEA2

Com o algoritmo de cifra restrito a NEA2 (mantendo a integridade ativada), identificaram-se os pacotes PDCP-NR correspondentes ao pedido ping em *Downlink* (SN=5587) e *Uplink* (SN=4067), ambos na DRB-1 (Figura 3-64 e Figura 3-65).

O campo *Data* mantém os 65 bytes já observados na configuração anterior, mas o conteúdo, visível no campo *AM Data* da camada RLC-NR, deixa de corresponder à sequência ASCII reconhecível do *payload* do ping, apresentando antes uma sucessão de bytes sem padrão discernível. Esta alteração confirma o efeito da cifra NEA2 sobre o tráfego de utilizador, sem impacto no tamanho do PDU, uma vez que o AES opera como cifra de bloco preservando o comprimento dos dados.

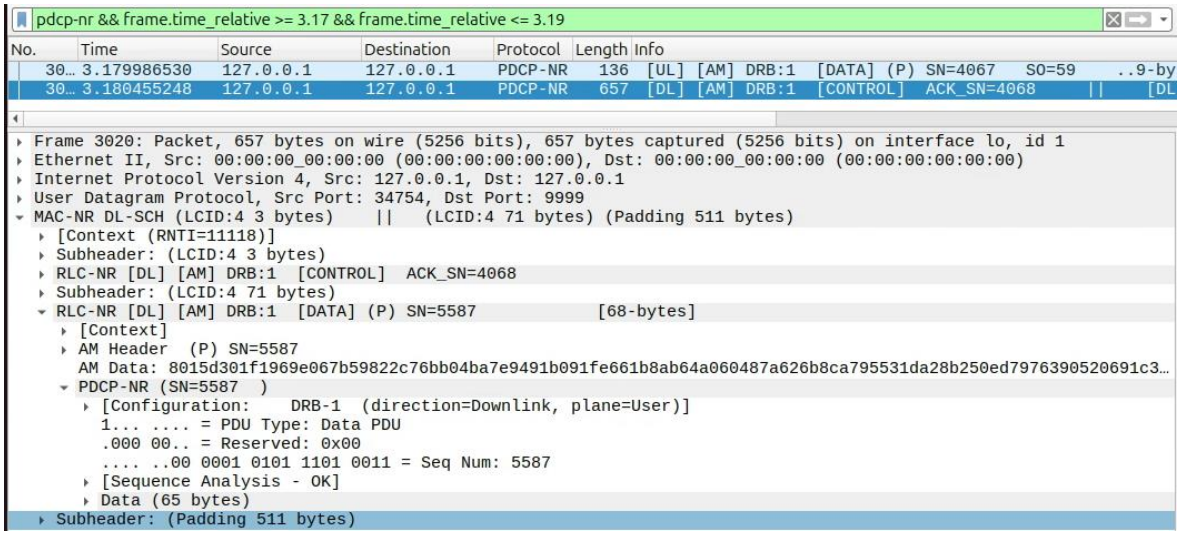


Figura 3-64: PDCP-NR, pacote Downlink (SN=5587), payload cifrado

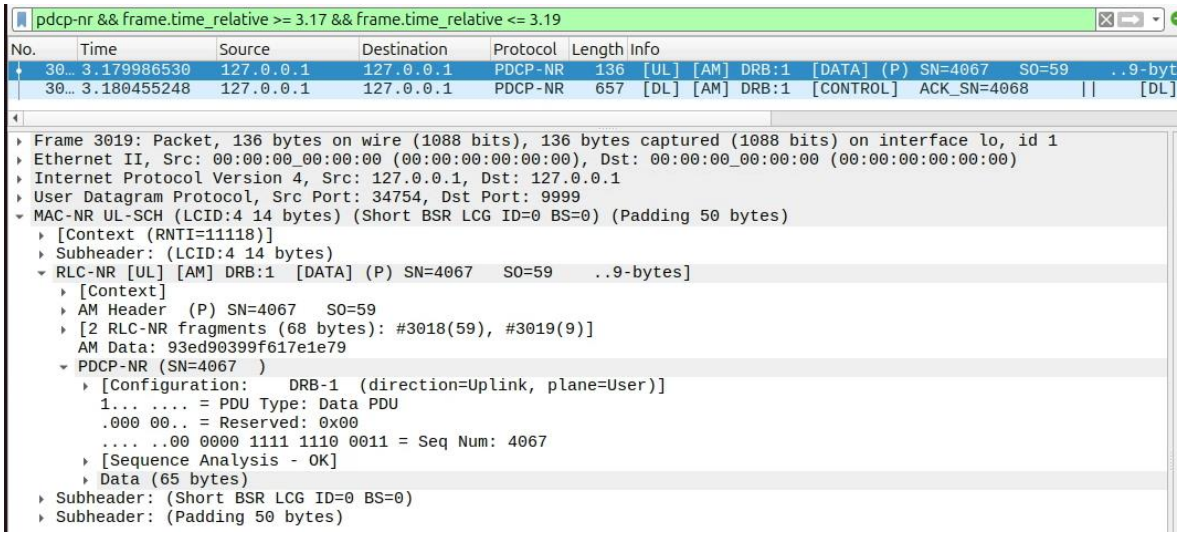


Figura 3-65: PDCP-NR, pacote Uplink (SN=4067), payload cifrado

A Tabela 3:20 resume os resultados obtidos nas três configurações analisadas.

Tabela 3:20 Resumo da proteção observada no plano de utilizador, por configuração

Configuração	Cifra	Integridade	Tamanho do Data (bytes)	Conteúdo do *payload*
Por omissão	NEA0	Desativada	61	Sequência ASCII reconhecível
Integridade ativada	NEA0	NIA2	65	Sequência ASCII reconhecível
Cifra NEA2	NEA2	NIA2	65	Sem padrão reconhecível

Verifica-se que a ativação da integridade acrescenta 4 bytes ao PDU, correspondentes ao campo MAC-I, sem alterar a legibilidade do conteúdo transmitido, enquanto a cifra NEA2 não altera o tamanho do PDU, mas torna o conteúdo transmitido irreconhecível. Estes resultados confirmam experimentalmente a independência entre a K_UPenc e a K_UPint referida na secção 2.7.6.1, evidenciando que a confidencialidade e a integridade do plano de utilizador são protegidas por chaves distintas, podendo ser ativadas de forma independente uma da outra.

3.10.7 Interfaces de comunicação do UE

O UE dispõe de duas interfaces lógicas, N1 e AS, cada uma protegida por um contexto de segurança próprio estabelecido sequencialmente. Primeiro é estabelecido o contexto NAS, através do *NAS Security Mode Command*/*Complete*, já analisado na secção 3.10.2. Só depois é estabelecido o contexto AS, através do *AS Security Mode Command* e da *RRC Reconfiguration*, já analisado na secção 3.10.4. Em ambos os casos, a proteção cobre confidencialidade e integridade, com chaves distintas derivadas da mesma hierarquia, como detalhado na secção 2.7.6.

3.10.8 Correspondência com os mecanismos teóricos de segurança

A hierarquia de chaves e o mecanismo de derivação (KDFs baseadas em HMAC-SHA-256, conforme a TS 33.220 [29]) encontram-se detalhados na secção 2.7.6. A cifra assimétrica no 5G NR é usada exclusivamente na cifra do SUCI, através do esquema ECIES nos perfis *Profile A* e *Profile B*, e o processo de criação e decifração do SUCI,

incluindo a estrutura dos seus campos e o papel da SIDF, encontra-se integralmente detalhado na secção 2.7.4.2.

3.10.9 Cifra simétrica ou assimétrica

O 5G NR usa predominantemente cifra simétrica. Os algoritmos de cifra do NAS e do AS observados neste trabalho, NEA0 e NEA2, são ambos simétricos, tal como o algoritmo de integridade NIA2 (AES-CMAC). A única exceção observada foi a cifra do SUCI, que usa ECIES, um esquema assimétrico, embora, como já referido na secção 3.10.8, o *Null-scheme* ativo neste ambiente experimental nem tenha chegado a exercitar essa cifra.

Em suma, este laboratório confirmou experimentalmente a arquitetura de segurança do 5G NR ao longo de todo o percurso do UE até à rede.

A mensagem *Registration Request* revelou o SUCI sob *Null-scheme* (secção 3.10.2). O procedimento de autenticação 5G-AKA confirmou, através do RAND, do AUTN e do RES*, o caráter mutuamente autenticado da ligação (secção 3.10.3).

O estabelecimento dos contextos de segurança NAS e AS (secções 3.10.2 e 3.10.4) mostrou como as chaves derivadas da hierarquia (secção 2.7.6) protegem cada estrato da comunicação de forma independente. Já a mensagem *PDU Session Establishment Request* (secção 3.10.5) expôs a fronteira de confiança entre o NAS, protegido fim a fim entre o UE e a AMF, e a interface N11, onde a identidade do subscritor já circula em claro.

Por fim, os testes sobre o plano de utilizador (secção 3.10.6) confirmaram que a cifra e a integridade são ativadas de forma independente, com impacto direto no tráfego observado.

3.11 Uso de Network Slicing em 5G usando uma xApp

O objetivo deste ensaio consistiu em criar uma segunda *network slice*, dedicada a comunicações URLLC, distinta da *slice* eMBB por omissão, e avaliar experimentalmente o efeito da alocação de recursos rádio (PRBs) no desempenho de cada *slice*, com recurso à xApp de *Network Slicing* disponibilizada pela plataforma OAIBOX™ através do FlexRIC [25].

3.11.1 Configuração da slice URLLC

Manteve-se a banda n77 e o modo de duplexagem TDD (configuração de *slots* DDDFU), configurando-se a largura de banda do gNB para 40 MHz, correspondente a um total de 106 PRBs disponíveis, atribuídos por omissão a uma única *slice* eMBB (SST 1, conforme descrito na secção 2.3.2.1).

Através da xApp *Network Slicing*, criou-se uma segunda *slice*, URLLC (SST 2), com início no PRB 82 e alocação de 24 PRBs em *downlink* e em *uplink*, associada ao APN *oai.urllc* e à subnet IPv4 172.16.20.0/24, como mostra a Figura 3-66.

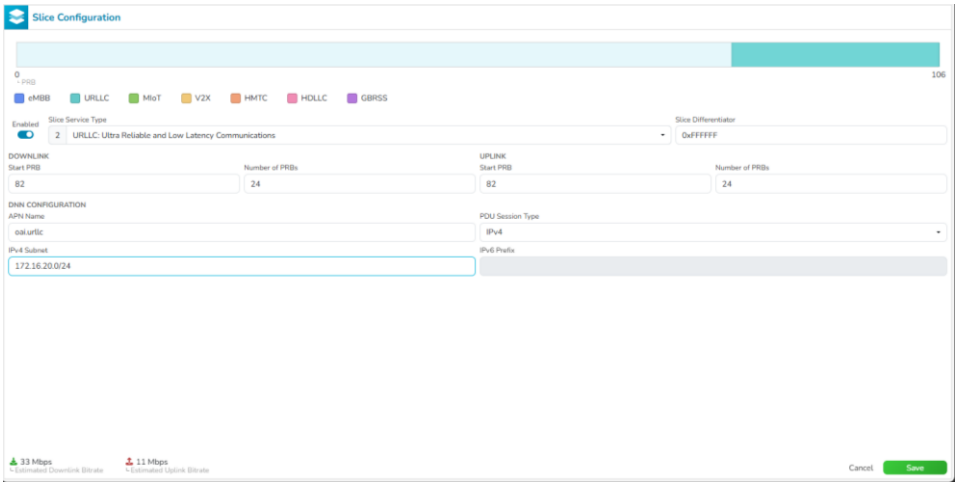


Figura 3-66: Slice Configuration, criação da slice URLLC (SST 2, Start PRB 82, 24 PRBs)

Gravada a configuração, confirmou-se a coexistência das duas *slices* no grid de recursos da xApp: a eMBB com os 106 PRBs e a URLLC com os 24 PRBs reservados, como mostra a Figura 3-67. Importa notar que estes 24 PRBs atribuídos à URLLC têm precedência sobre a slice eMBB, pelo que esta última só pode utilizar a totalidade dos 106 PRBs quando não existem UEs a consumir recursos na slice URLLC; caso contrário, a eMBB fica limitada aos restantes 82 PRBs.

Para cada *slice*, a plataforma apresenta ainda o débito teórico máximo (*Estimated Downlink/Uplink Bitrate*), calculado segundo o modelo de *bitrate* por PRB e MCS já apresentado na secção 2.8.2.3, aplicado à fração de PRBs atribuída a cada *slice*: 146/47 Mbps para a eMBB, valor correspondente à totalidade dos 106 PRBs disponíveis na ausência de tráfego na slice URLLC, e 33/11 Mbps para a URLLC (24 PRBs).

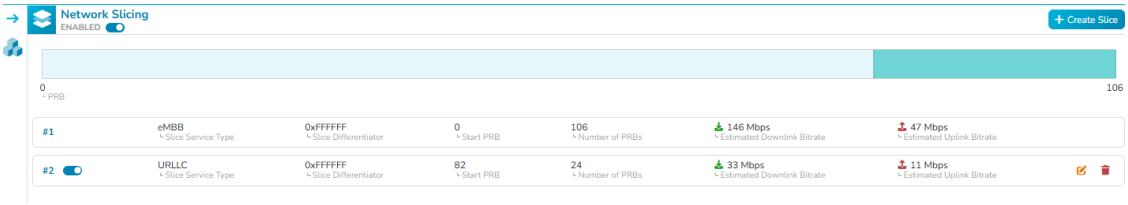


Figura 3-67: Network Slicing, slices eMBB e URLLC configuradas

3.11.2 Medição de desempenho da slice eMBB

Com o CN5G, o FlexRIC e o gNB em execução, o UE ligou-se através da *slice* eMBB, por omissão. A evolução do *bitrate* durante um teste de velocidade (*speedtest*) é apresentada na Figura 3-68, e o resumo final do teste, na Figura 3-69, com um débito de 144,9 Mbps em *downlink* e 23,4 Mbps em *uplink*, uma latência de 18 ms e um *jitter* de 0,8 ms.

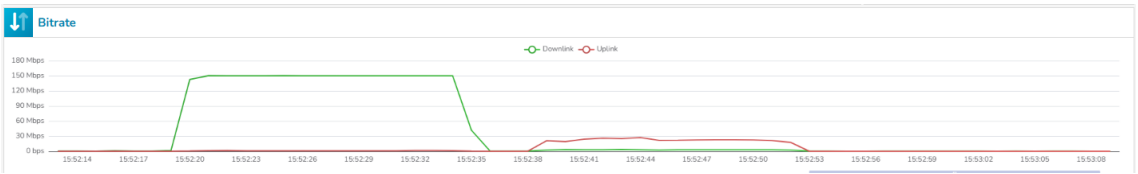


Figura 3-68: Bitrate, teste de velocidade na slice eMBB

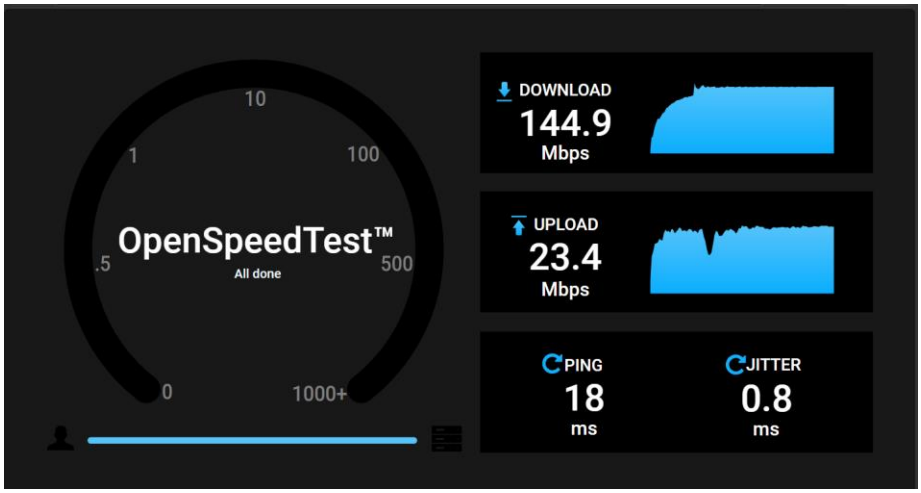


Figura 3-69: OpenSpeedTest, resumo do teste de velocidade na slice eMBB

Face ao débito teórico estimado pela plataforma para a eMBB (146/47 Mbps, Figura 3-67), o valor de *downlink* medido está muito próximo, com uma diferença de cerca de 1%. O valor de *uplink* medido é sensivelmente metade do teórico, diferença atribuível à assimetria da trama TDD, que reserva mais símbolos ao *downlink* do que ao *uplink*.

3.11.3 Estabelecimento da sessão PDU na slice URLLC

Configurou-se no módulo *Quectel* um segundo contexto PDP associado ao SST 2, confirmado através de AT+CGDCONT?, como mostra a Figura 3-70.

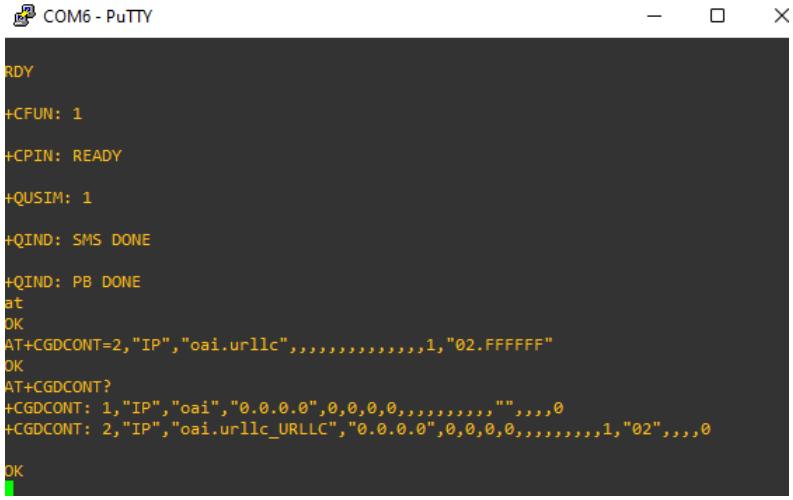


Figura 3-70: PuTTY, confirmação dos dois contextos PDP configurados (eMBB e URLLC)

Ativada a sessão, capturou-se no Wireshark, com o filtro *ngap*, a mensagem *UplinkNASTransport*, cujo campo S-NSSAI confirma o pedido de sessão com SST 2 e cujo campo DNN confirma o APN *oai.urllc*, como mostra a Figura 3-71.

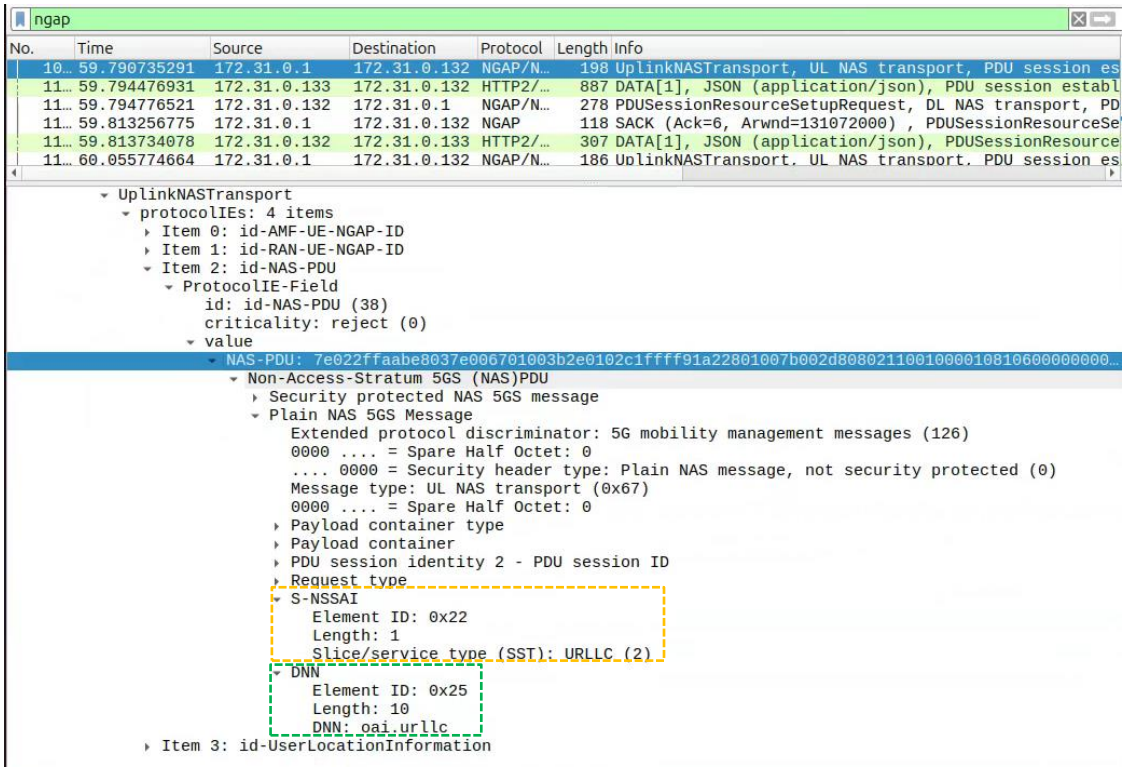


Figura 3-71: Wireshark, pedido de sessão PDU com S-NSSAI URLLC (SST 2) e DNN oai.urllc

Na resposta da rede, o campo *PDU address* confirma a atribuição do endereço 172.16.20.2 ao UE, dentro da subnet definida para a *slice* URLLC, como mostra a Figura 3-72.

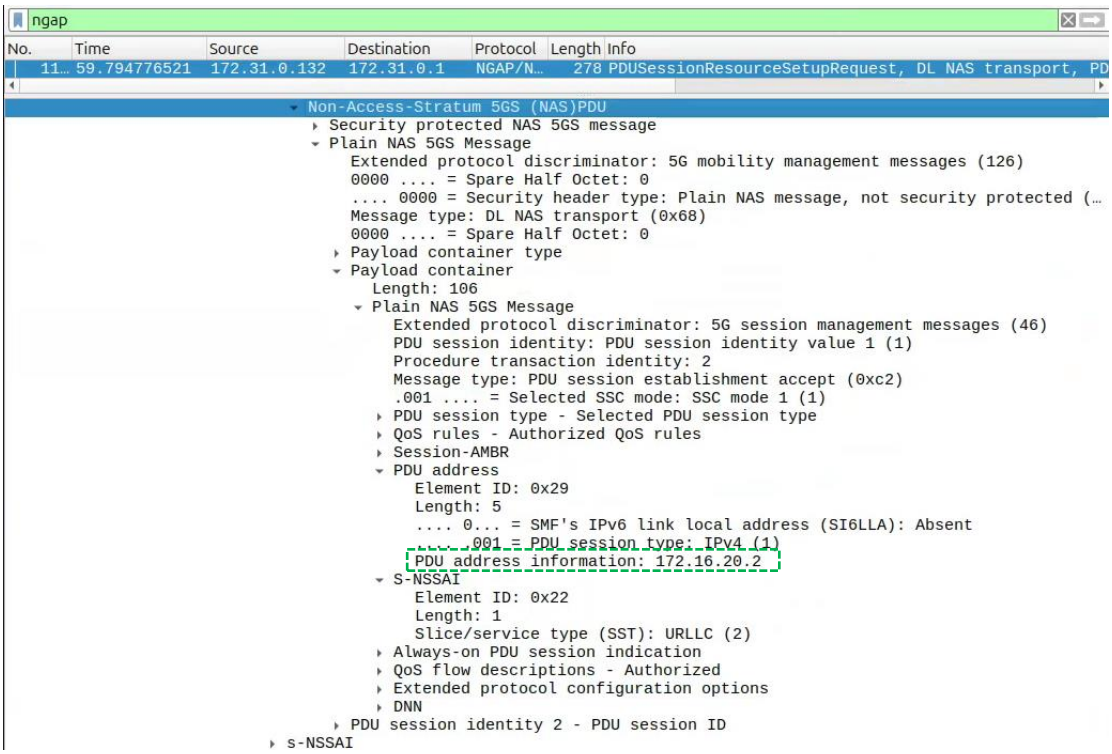


Figura 3-72: Wireshark, resposta da rede com o endereço IP atribuído na subnet da URLLC

3.11.4 Medição de desempenho da slice URLLC

Direcionando o tráfego do teste de velocidade para o endereço 172.16.20.2 (endereço atual do UE), a evolução do *bitrate* é apresentada na Figura 3-73, e o resumo final do teste, na Figura 3-74, com um débito de 33,0 Mbps em *downlink* e 6,9 Mbps em *uplink*, uma latência de 18 ms e um *jitter* de 0,4 ms.

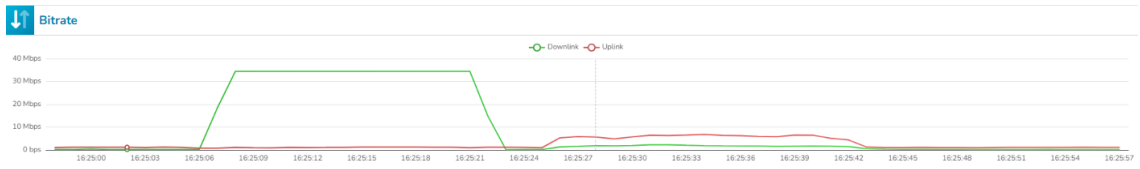


Figura 3-73: Bitrate, evolução do teste de velocidade na slice URLLC

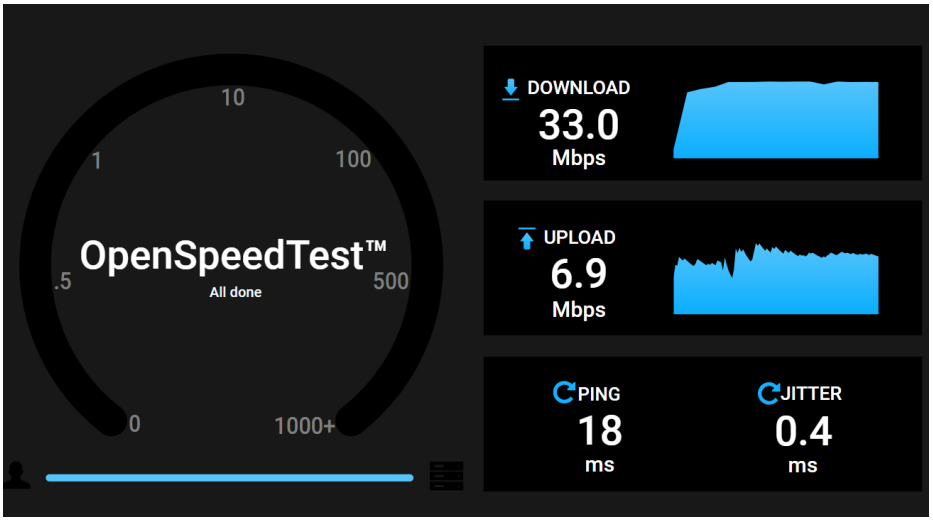


Figura 3-74: OpenSpeedTest, resumo do teste de velocidade na slice URLLC

Face ao débito teórico estimado para a URLLC (33/11 Mbps, Figura 3-67), o valor de *downlink* medido corresponde quase exatamente; o de *uplink* fica novamente bem abaixo do teórico, consistente com a assimetria TDD já referida.

3.11.5 Efeito da variação de PRBs no throughput

Gerou-se tráfego UDP contínuo em *downlink*, dirigido ao endereço da *slice* URLLC, e alterou-se em tempo real, através da xApp *Network Slicing*, o número de PRBs atribuídos, sem interromper o tráfego. Testaram-se as três condições da Tabela 3:21.

Tabela 3:21 Condições de alocação de PRBs testadas

Condição	Start PRB	Nº de PRBs	Débito teórico (DL)
1	82	24	≈ 33 Mbps
2	90	15	≈ 21 Mbps
3	100	6	≈ 8 Mbps

O gráfico de *bitrate* resultante (Figura 3-75) mostra três patamares de *downlink* correspondentes às condições testadas.

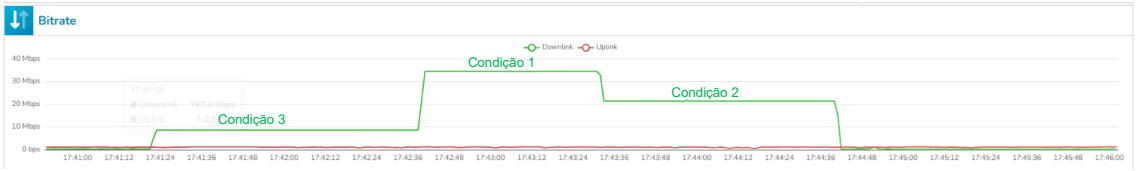


Figura 3-75: Bitrate, efeito da variação de PRBs da slice URLLC no throughput

Os valores observados em cada patamar (aproximadamente 8, 33 e 21 Mbps) acompanham os valores teóricos esperados, confirmando experimentalmente a relação linear entre o número de PRBs atribuídos a uma *slice* e o débito máximo que esta oferece.

Este laboratório confirmou experimentalmente que o *network slicing* permite repartir os recursos rádio de uma célula em múltiplas *slices* com desempenho independente entre si, cada uma ajustada ao tipo de serviço que suporta. A criação da *slice* URLLC não afetou o desempenho da *slice* eMBB já existente, e o débito medido em ambas acompanhou de forma consistente o valor teórico estimado com base na fração de PRBs atribuída. A variação em tempo real do número de PRBs da URLLC confirmou ainda a relação direta entre a alocação de recursos e o débito máximo disponível, validando o *network slicing* como mecanismo de isolamento de desempenho entre serviços distintos sobre a mesma infraestrutura física.

3.12 Configuração de PLMN e programação de cartões SIM 5G

O objetivo deste ensaio consistiu em alterar o PLMN de omissão da OAIBOX™ (00101) para um PLMN privado (99999), percorrendo os diferentes pontos de configuração envolvidos no gNB, no CN5G e na interação com o SIM do UE, cujo programador e cartão SIM 5G utilizados são apresentados na Figura 3-76.

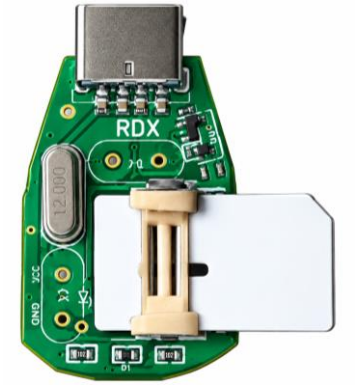


Figura 3-76: Programador de cartões SIM 5G e cartão SIM

3.12.1 Alteração do PLMN na configuração do gNB

Manteve-se a configuração de banda n77 (TDD), com largura de banda de 20 MHz, sendo o PLMN o único parâmetro alterado neste ensaio, do valor de omissão (00101) para o PLMN privado 99999. No ficheiro *OAIBOX™.yaml*, o campo *plmn_list* foi atualizado para MCC 999 e MNC 99, como mostra a Figura 3-77.

```
export-mod-symbols: 0
export-mod-symbols-ip: "127.0.0.1"
export-mod-symbols-port: 63138
export-srs-channel: 0
export-srs-channel-ip: "127.0.0.1"
export-srs-channel-port: 63139
export-srs-isac: 0
thread-pool: -1,-1,-1,-1,-1,-1,-1,-1,-1,-1,-1,-1,-1,-1,-1,-1
tune-offset: 0
gNBs:
  - gNB_ID: "0xe00"
    gNB_name: gNB-OAI
    maxMIMO_layers: 1
    tracking_area_code: 1
    plmn_list:
      - mcc: "999"
        mnc: "99"
        mnc_length: 2
        snssaiList:
          - sst: "1"
```

Figura 3-77: OAIBOX™.yaml, campo plmn_list alterado para MCC 999 e MNC 99

Ao iniciar o CN5G e o gNB, o procedimento NG *Setup* falhou, tendo sido devolvida a mensagem *NGSetupFailure* com a causa Misc=unknown-PLMN, como mostra a Figura 3-78.

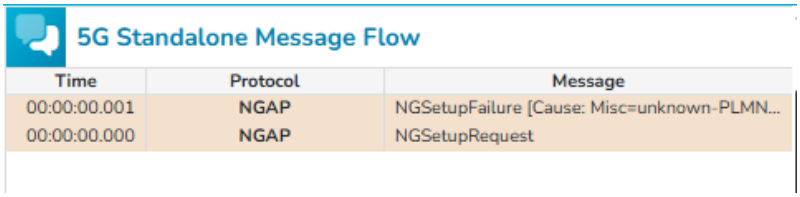


Figura 3-78: Dashboard, NGSetupFailure após alteração do PLMN no gNB

O *NG Setup Procedure* corresponde ao estabelecimento inicial da ligação entre o gNB e a AMF pela interface N2, através do protocolo NGAP. O gNB envia uma mensagem *NGSetupRequest* com o seu identificador global, as *Tracking Areas* suportadas e os PLMNs anunciados. A AMF valida esta informação e responde com uma *NGSetupResponse*, ficando o gNB apto a atender pedidos de registo dos UEs [27]. Neste caso a falha ocorreu porque o gNB passou a anunciar o PLMN 999/99, enquanto a AMF permanecia configurada com o PLMN de omissão 001/01. Não existindo correspondência na lista *plmn_support_list*, a AMF rejeitou o pedido, confirmando a incompatibilidade entre os dois PLMNs.

3.12.2 Alteração do PLMN na configuração do CN5G

Para corrigir a falha anterior, foram atualizados os ficheiros *config.yaml* e *nssf_slice_config.yaml*, alinhando o PLMN da AMF e da NSSF com o do gNB. No *config.yaml* foram alterados os campos *served_guami_list* e *plmn_support_list* para MCC 999 e MNC 99, como ilustra a Figura 3-79.

```
pid_directory: /var/run
amf_name: OAI-AMF
support_features_options:
  enable_simple_scenario: "no"
  enable_nssf: "yes"
  enable_smf_selection: "yes"
  use_external_udm: "no"
relative_capacity: 30
statistics_timer_interval: 20
emergency_support: false
served_guami_list:
- mcc: "999"
  mnc: "99"
  amf_region_id: "01"
  amf_set_id: "001"
  amf_pointer: "01"
plmn_support_list:
- mcc: "999"
  mnc: "99"
  tac: "0x0001"
```

Figura 3-79: config.yaml, served_guami_list e plmn_support_list da AMF, MCC 999 e MNC 99

No *nssf_slice_config.yaml* foi alterado o campo *taInfoList*, que associa o TAI de cada *Tracking Area* às *slices* suportadas nessa área, como mostra a Figura 3-80. O TAI corresponde à combinação do PLMN com o TAC (*Tracking Area Code*), sendo usado pela AMF na gestão da mobilidade e do *paging* do UE. O TAC tem de coincidir com o valor configurado no gNB, e o PLMN tem de ser consistente entre o gNB, a AMF e a NSSF, garantindo que o UE é corretamente localizado e que lhe são atribuídas as *slices* adequadas [10].

```
GNU nano 7.2                    nssf_slice_config.yaml

taInfoList:
  - tai:
      plmnId:
        mcc: '999'
        mnc: '99'
      tac: '1'
    supportedSnssaiList:
      - sst: 1
        sd: 'ffffff'
      - sst: 2
        sd: 'ffffff'
amfInfoList:
  - targetAmfSet: oai5gcn.mcc001.mnc01.regionid1.setid1.3gppnetwork.org
    nrfAmfSet: http://oai-nrf:8080/nnrf-disc/v1/nf-instances'
    nrfAmfSetNfMgtUri: http://oai-nrf:8080/nnrf-nfm/v1/nf-instances
    amfList:
      - nfId: 405e8251-cc5a-45dd-a494-efb9eaf1cd58
        supportedNssaiAvailabilityData:
          tai:
            plmnId:
              mcc: 999
              mnc: 99
            tac: 1
          supportedSnssaiList:
            - sst: 1
```

Figura 3-80: nssf_slice_config.yaml, taInfoList e supportedSnssaiList da NSSF

3.12.3 Atualização da base de dados do CN5G

O ficheiro *oai_db.sql* corresponde ao script de inicialização e definição do esquema da base de dados do CN5G, onde são pré provisionados os subscritores, os perfis de sessão

e os dados de autenticação. A variável *@plmn*, definida no início do ficheiro, determina o PLMN usado na geração dos IMSIs dos subscritores. Esta variável foi alterada para 99999, como mostra a Figura 3-81, garantindo que os subscritores pré-provisionados passam a corresponder ao PLMN anunciado pela rede [25].

```
 GNU nano 7.2                          oai_db.sql
-- phpMyAdmin SQL Dump
-- version 5.1.0
-- https://www.phpmyadmin.net/
--
-- Host: 172.16.200.10:3306
-- Generation Time: Mar 22, 2021 at 10:31 AM
-- Server version: 5.7.33
-- PHP Version: 7.4.15

SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
START TRANSACTION;
SET time_zone = "+00:00";

SET @plmn = "99999";
SET @num_users = 128;
```

Figura 3-81: oai_db.sql, variável @plmn configurada para 99999

Após reiniciar o CN5G e o gNB com a configuração de PLMN corrigida em todos os ficheiros, o procedimento *NG Setup* foi concluído com sucesso, confirmado pela troca das mensagens *NGSetupRequest* e *NGSetupResponse* observada no *dashboard*, como mostra a Figura 3-82.

5G Standalone Message Flow

Time	Protocol	Message
00:00:00.000	NGAP	NGSetupResponse
00:00:00.000	NGAP	NGSetupRequest

Figura 3-82: Dashboard, NGSetupRequest e NGSetupResponse após correção do PLMN

3.12.4 Verificação e reprogramação do cartão SIM

Além da correção do PLMN nos ficheiros de configuração do gNB e do CN5G, foi necessário reprogramar o cartão SIM utilizado pelo UE, uma vez que este permanece associado ao PLMN gravado numa configuração anterior, independentemente da rede a que a OAIBOX™ está associada.

Confirmou-se o estado do SIM através dos comandos AT+COPS=? e AT+CIMI no módulo *Quectel.* O primeiro devolveu apenas redes comerciais visíveis na zona (Vodafone, MEO), sem qualquer referência à rede da OAIBOX™; o segundo devolveu o IMSI 001010000000001, cujos primeiros cinco dígitos (00101) confirmam a associação ao PLMN de omissão, como mostra a Figura 3-83.



Figura 3-83: PuTTY, estado do SIM antes da reprogramação

Até ao momento, a ligação do UE não é possível porque o SIM permanece provisionado com o PLMN 00101, enquanto a rede está configurada para o PLMN 99999. Como visto na secção 2.7.4.1, o UE só tenta o registo em PLMNs presentes no seu USIM; não existindo correspondência entre os dois, o pedido de registo nem chega a ser iniciado, impossibilitando a ligação 5G sem a reprogramação do cartão.

A reprogramação foi feita através da ferramenta *program_uicc*, do projeto *Open Cells*, atribuindo ao SIM um novo IMSI (999990000000001) e as chaves de autenticação correspondentes às definidas na base de dados do CN5G. A Figura 3-84 confirma a leitura dos valores originais e a gravação bem-sucedida dos novos valores, validada pela autenticação *Milenage* com sincronização do número de sequência (SQN 256 → 288).

```
Existing values in USIM
ICCID: ffffffffffffffffffff
WARNING: iccid luhn encoding of last digit not done
USIM IMSI: 001010000000001
PLMN selector: : 0x00f1107c
Operator Control PLMN selector: : 0x00f1107c
Home PLMN selector: : 0x00f1107c
USIM MSISDN: 00000001
USIM Service Provider Name: OpenAirInterface

Setting new values

Reading UICC values after uploading new values
ICCID: ffffffffffffffffffff
WARNING: iccid luhn encoding of last digit not done
USIM IMSI: 999990000000001
PLMN selector: : 0x99f9997c
Operator Control PLMN selector: : 0x99f9997c
Home PLMN selector: : 0x99f9997c
USIM MSISDN: 00000001
USIM Service Provider Name: OpenAirInterface
Succeeded to authentify with SQN: 256
set HSS SQN value as: 288
```

Figura 3-84: Terminal, reprogramação do SIM via program_uicc

3.12.4.1 Relação entre --key/--opc e a autenticação Milenage

Os parâmetros *--key* (K) e *--opc* (*Operator Code*) são os segredos partilhados entre o SIM e a rede, usados pelo algoritmo *Milenage* no procedimento de autenticação 5G-AKA, definido em TS 33.501 [13] e já analisado na secção sobre segurança no 5G NR (3.10). É com base nestes valores que a UDM/AUSF gera o vetor de autenticação e o SIM calcula a resposta e as chaves de sessão, permitindo confirmar a identidade do UE sem transmitir o próprio K. Reprogramar o SIM com um K/OPc sincronizado com a base de dados do CN5G é o que torna possível a autenticação com o novo IMSI.

Reinserido o SIM no módulo *Quectel*, o comando AT+COPS=? passou a listar também a rede da OAIBOX™ (999 99, PLMN 99999), confirmando o reconhecimento do cartão pela rede privada, como mostra a Figura 3-85.



Figura 3-85: PuTTY, AT+COPS=? após reprogramação

3.12.5 Configuração final do modem e confirmação da ligação

Concluída a reprogramação do SIM, configurou-se o perfil do modem e os contextos PDP necessários à ligação. O comando *AT+QENG="servingcell"* confirmou o registo do UE na célula da OAIBOX™, com MCC 999 e MNC 99, como mostra a Figura 3-86.

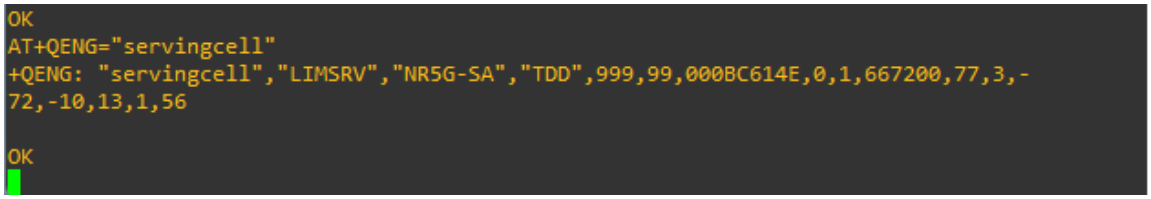


Figura 3-86: PuTTY, confirmação da célula servidora após reprogramação do SIM

Este laboratório confirmou experimentalmente que a alteração do PLMN de uma rede 5G privada exige a atualização coerente do gNB, do CN5G e do SIM, e não apenas de um destes elementos isoladamente.

A alteração do PLMN apenas no gNB (*OAIBOX™.yaml*) foi insuficiente, resultando numa *NGSetupFailure* por incompatibilidade com o PLMN configurado na AMF. Só após alinhado o PLMN também na AMF, na NSSF (*config.yaml*, *nssf_slice_config.yaml*) e na base de dados de subscritores (*oai_db.sql*), o procedimento NG *Setup* foi concluído com sucesso.

A ligação do UE manteve-se, no entanto, impossível enquanto o SIM permaneceu associado ao PLMN de origem, uma vez que o UE só regista em PLMNs presentes no próprio cartão. A reprogramação do SIM, através da ferramenta *program_uicc* e dos parâmetros de autenticação *Milenage* (K, OPc), sincronizou o cartão com a nova identidade da rede, permitindo o registo do UE, confirmado pelo comando *AT+QENG="servingcell"* com MCC 999 e MNC 99.

3.13 Análise dos resultados obtidos

Considerando o conjunto dos ensaios realizados, nomeadamente a variação da largura de banda, da banda de frequência e do cenário de propagação, da configuração TDD e FDD, do esquema de modulação e codificação e da configuração MIMO, os valores medidos de RSRP, SINR e *bitrate* aproximam se, de forma consistente ao longo de todo o capítulo, dos valores calculados pela equação de Friis, pelo mapeamento SINR para CQI e pelo modelo de bitrate por alocação de slots TDD, apresentados ao longo da secção 2.8.2. As diferenças observadas são explicáveis por um conjunto de fatores recorrentes ao longo dos ensaios, entre os quais a sobrecarga de sinalização associada ao PDCCH e aos sinais de referência, o comportamento do mecanismo HARQ em condições reais de erro, o multipercurso e a margem de recuo face ao EIRP máximo especificado nas configurações da OAIBOX™, e as características do canal de propagação no ambiente de testes. Este padrão confirma a validade destes modelos como limite teórico de referência, calculado em condições ideais de propagação, evidenciando ao mesmo tempo a importância da experimentação prática para quantificar os desvios que surgem em condições reais de operação.

Os ensaios de Inspeção Profunda de Pacotes, de segurança, de *network slicing*, de reconfiguração de PLMN e reprogramação de cartão SIM complementaram esta análise ao nível dos planos de controlo e de utilizador, confirmando que o comportamento observado nesses procedimentos é igualmente consistente com o descrito nas especificações normativas do 3GPP.

4 Conclusão

O trabalho desenvolvido cumpriu o objetivo geral proposto, tendo permitido implementar, configurar e avaliar experimentalmente uma rede 5G NR *Standalone* na plataforma OAIBOX™, com base na implementação de código aberto *OpenAirInterface*, e caracterizar a arquitetura do sistema, os procedimentos de ligação entre o UE, o gNB e o CN5G, e as especificações normativas do 3GPP que os regem.

A avaliação experimental do impacto de diferentes configurações da interface rádio, nomeadamente a largura de banda, a banda de frequência, o modo TDD e FDD, a modulação e o MIMO, através da monitorização dos principais KPIs, mostrou desvios entre os valores teóricos e os medidos consistentes com fatores conhecidos, como a sobrecarga de sinalização, o mecanismo HARQ e as condições reais de propagação, e não com comportamentos anómalos da implementação. Complementarmente, a Inspeção Profunda de Pacotes e a análise de segurança validaram os procedimentos de registo, autenticação e proteção das comunicações, enquanto os ensaios de *network slicing* e de de reconfiguração de PLMN e do cartão SIM confirmaram a flexibilidade do 5G Core e a exigência de coerência entre o gNB, a AMF, a NSSF e a base de dados de subscritores.

Estes resultados confirmam o potencial da OAIBOX™ enquanto plataforma de ensino e investigação, ao permitir observar de forma controlada procedimentos que a especificação 3GPP descreve, através de uma implementação assente inteiramente em código aberto. A possibilidade de configurar e testar cada um destes procedimentos numa rede real, mas em ambiente controlado, ilustra o valor prático deste tipo de acesso para estudantes e investigadores, um valor que se estende a outras iniciativas *open source* atualmente em curso na área das redes móveis.

Este projeto contribuiu ainda para o desenvolvimento de competências relevantes para a prática profissional em telecomunicações, nomeadamente a análise comparativa entre resultados experimentais e modelos teóricos e a autonomia na utilização da ferramenta de monitorização Wireshark.

Como trabalho futuro, seria pertinente alargar esta análise a cenários de maior complexidade, como a integração de múltiplos UEs em simultâneo ou a avaliação de mecanismos de mobilidade entre células. Seria também relevante desenvolver uma aplicação dedicada à interpretação dos pacotes capturados nas diferentes interfaces do sistema, traduzindo a informação técnica de protocolos como o NGAP, o NAS-5GS, o RRC-NR, o PDCP-NR e o GTP-U para uma representação mais acessível, reduzindo a dependência da leitura manual dos dissectores do Wireshark demonstrada neste trabalho.

5 REFERÊNCIAS

[1] 3GPP. *TS 24.501: Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3*. 3rd Generation Partnership Project.

[2] 3GPP. *TS 38.331: NR; Radio Resource Control (RRC); Protocol specification*. 3rd Generation Partnership Project.

[3] 3GPP. *TS 38.104: NR; Base Station (BS) radio transmission and reception*. 3rd Generation Partnership Project.

[4] 3GPP. *TS 38.323: NR; Packet Data Convergence Protocol (PDCP) specification*. 3rd Generation Partnership Project.

[5] 3GPP. *TS 38.322: NR; Radio Link Control (RLC) protocol specification*. 3rd Generation Partnership Project.

[6] 3GPP. *TS 38.321: NR; Medium Access Control (MAC) protocol specification*. 3rd Generation Partnership Project.

[7] 3GPP. *TS 38.211: NR; Physical channels and modulation*. 3rd Generation Partnership Project.

[8] 3GPP. *TR 21.916: Release description; Release 16*. 3rd Generation Partnership Project.

[9] 3GPP. *TS 22.261: Service requirements for the 5G system*. 3rd Generation Partnership Project.

[10] 3GPP. *TS 23.501: System architecture for the 5G System (5GS)*. 3rd Generation Partnership Project.

[11] 3GPP. *TS 23.502: Procedures for the 5G System (5GS)*. 3rd Generation Partnership Project.

[12] 3GPP. *TS 29.500: 5G System; Technical Realization of Service Based Architecture; Stage 3*. 3rd Generation Partnership Project.

[13] 3GPP. *TS 33.501: Security architecture and procedures for 5G System*. 3rd Generation Partnership Project.

[14] 3GPP. *TS 38.300: NR; NR and NG-RAN Overall Description; Stage 2*. 3rd Generation Partnership Project.

[15] 3GPP. *TS 37.324: E-UTRA and NR; Service Data Adaptation Protocol (SDAP) specification*. 3rd Generation Partnership Project.

[16] Poynting Antennas. *Signal Strength Measure: RSRP, RSRQ and SINR Reference for LTE & 5G Cheat Sheet*. Disponível em: https://poynting.tech/articles/antenna-faq/signal-strength-measure-rsrp-rsrq-and-sinr-reference-for-lte-cheat-sheet/

[17] 3GPP. *TS 38.401: NG-RAN; Architecture description*. 3rd Generation Partnership Project.

[18] 3GPP. *3GPP Specification Series: 38 series*. Disponível em: https://www.3gpp.org/dynareport?code=38-series.htm

[19] Allbesmart, Lda. *OAIBOX™ Dashboard*. Disponível em: https://my.OAIBOX™.com

[20] 3GPP. *TS 38.101-1: NR; User Equipment (UE) radio transmission and reception; Part 1: Range 1 Standalone*. 3rd Generation Partnership Project.

[21] Allbesmart, Lda. OAIBOX™. Disponível em: https://OAIBOX™.com

[22] EURECOM. *OpenAirInterface Alliance*. Disponível em: https://www.eurecom.fr/en/research/communication-system-department/openairinterface-alliance

[23] OAIBOX™ website | 5G LAB Manual

[24] 3GPP. *TR 36.873: Study on 3D channel model for LTE*. 3rd Generation Partnership Project.
[25] Allbesmart, Lda. *OAIBOX™ 5G Lab Manual*, versão v2026-01-07
[26] 3GPP. *TS 38.214: NR; Physical layer procedures for data*. 3rd Generation Partnership Project.
[27] 3GPP. *TS 38.413: NG-RAN; NG Application Protocol (NGAP)*. 3rd Generation Partnership Project.
[28] 3GPP. *TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)*. 3rd Generation Partnership Project.
[29] 3GPP. *TS 33.220: Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)*. 3rd Generation Partnership Project.
[30] 3GPP. *TS 31.102: Characteristics of the USIM application*. 3rd Generation Partnership Project.