UNIVERSIDADE FEDERAL DE GOIÁS (UFG)

INSTITUTO DE INFORMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

CIRO JOSÉ ALMEIDA MACEDO

Redes de Telecomunicações Convergentes: Modelagem e Implementação de Arquitetura para Infraestruturas Pós-5G

Goiânia
2024

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE INFORMÁTICA

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO (TECA) PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES

E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo das Teses e Dissertações disponibilizado na BDTD/UFG é de responsabilidade exclusiva do autor. Ao encaminhar o produto final, o autor(a) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do material bibliográfico

[ ] Dissertação [X] Tese [ ] Outro*:_____

*No caso de mestrado/doutorado profissional, indique o formato do Trabalho de Conclusão de Curso, permitido no documento de área, correspondente ao programa de pós-graduação, orientado pela legislação vigente da CAPES.

Exemplos: Estudo de caso ou Revisão sistemática ou outros formatos.

2. Nome completo do autor

Ciro José Almeida Macedo

3. Título do trabalho

Redes de Telecomunicações Convergentes: Modelagem e Implementação de Arquitetura para Infraestruturas Pós-5G

4. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador)

Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante:
a) consulta ao(à) autor(a) e ao(à) orientador(a);
b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo da tese ou dissertação.
O documento não será disponibilizado durante o período de embargo.
Casos de embargo:
- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

Obs. Este termo deverá ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Kleber Vieira Cardoso**, **Professor do Magistério Superior**, em 21/10/2024, às 11:57, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Ciro José Almeida Macedo**, **Discente**, em 21/10/2024, às 15:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4914937** e o código CRC **DD7CB8CA**.

CIRO JOSÉ ALMEIDA MACEDO

Redes de Telecomunicações Convergentes: Modelagem e Implementação de Arquitetura para Infraestruturas Pós-5G

Tese apresentada ao Programa de Pós–Graduação do Instituto de Informática da Universidade Federal de Goiás (UFG), como requisito parcial para obtenção do título de Doutor em Programa de Pós-Graduação em Ciência da Computação.

Área de concentração: Ciência da Computação.
Linha de Pesquisa: Sistemas de Computação.

Orientador: Prof. Dr. Kleber Vieira Cardoso

Co-Orientador: Prof. Dr. Cristiano Bonato Both

Goiânia
2024

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Macedo, Ciro José Almeida
Redes de Telecomunicações Convergentes [manuscrito] : Modelagem e Implementação de Arquitetura para Infraestruturas Pós-5G / Ciro José Almeida Macedo. - 2024.
128 f.

Orientador: Prof. Dr. Kleber Vieira Cardoso; co-orientador Dr. Cristiano Bonato Both.
Tese (Doutorado) - Universidade Federal de Goiás, Instituto de Informática (INF), Programa de Pós-Graduação em Ciência da Computação, Goiânia, 2024.
Bibliografia.
Inclui siglas, abreviaturas, gráfico, tabelas, lista de figuras, lista de tabelas.

1. Coleta de dados para AI/ML. 2. Redes móveis Pós-5G. 3. Acesso não-3GPP. 4. Softwarização de redes. 5. Análise estatística da rede. I. Cardoso, Kleber Vieira, orient. II. Título.

CDU 004

UNIVERSIDADE FEDERAL DE GOIÁS

INSTITUTO DE INFORMÁTICA

ATA DE DEFESA DE TESE

Ata nº **29** da sessão de Defesa de Tese de **Ciro José Almeida Macedo**, que confere o título de Doutor em Ciência da Computação, na área de concentração em Ciência da Computação.

Aos vinte e cinco dias do mês de setembro de dois mil e vinte e quatro, a partir das catorze horas, via sistema de webconferência, realizou-se a sessão pública de Defesa de Tese intitulada **"Redes de Telecomunicações Convergentes: Modelagem e Implementação de Arquitetura para Infraestruturas Pós-5G"**. Os trabalhos foram instalados pelo Orientador, Professor Doutor Kleber Vieira Cardoso (INF/UFG) com a participação dos demais membros da Banca Examinadora: Prof. Dr. Cristiano Bonato Both (UNISINOS), coorientador; Professor Doutor Antonio Carlos de Oliveira Júnior (INF/UFG), membro titular interno; Professor Doutor Aldebaro Barreto da Rocha Klautau Júnior (UFPA), membro titular externo; Prof. Dr. Antônio Marcos Alberti (INATEL), membro titular externo; e Prof. Dr. Joberto Sérgio Barbosa Martins (UNIFACS), membro titular externo. A realização da banca ocorreu por meio de videoconferência. Durante a arguição os membros da banca não fizeram sugestão de alteração do título do trabalho. A Banca Examinadora reuniu-se em sessão secreta a fim de concluir o julgamento da Tese, tendo sido o candidato **aprovado** pelos seus membros. Proclamados os resultados pelo Professor Doutor Kleber Vieira Cardoso, Presidente da Banca Examinadora, foram encerrados os trabalhos e, para constar, lavrou-se a presente ata que é assinada pelos Membros da Banca Examinadora, aos vinte e cinco dias do mês de setembro de dois mil e vinte e quatro.

TÍTULO SUGERIDO PELA BANCA

Documento assinado eletronicamente por **Antonio Carlos De Oliveira Junior**, **Professor do Magistério Superior**, em 25/09/2024, às 17:01, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Aldebaro Barreto da Rocha Klautau Junior**, **Usuário Externo**, em 25/09/2024, às 17:02, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Kleber Vieira Cardoso**, **Professor do Magistério Superior**, em 25/09/2024, às 17:06, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **CRISTIANO BONATO BOTH**, **Usuário Externo**, em 25/09/2024, às 17:06, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Ciro José Almeida Macedo**, **Discente**, em 25/09/2024, às 17:24, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Joberto Sergio Barbosa Martins**, **Usuário Externo**, em 25/09/2024, às 19:41, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Alberti registrado(a) civilmente como Antonio Marcos Alberti**, **Usuário Externo**, em 30/09/2024, às 16:40, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4851421** e o código CRC **70DAC534**.

Referência: Processo nº 23070.049699/2024-63 SEI nº 4851421

CIRO JOSÉ ALMEIDA MACEDO

Redes de Telecomunicações Convergentes: Modelagem e Implementação de Arquitetura para Infraestruturas Pós-5G

Tese defendida no Programa de Pós–Graduação do Instituto de Informática da Universidade Federal de Goiás (UFG) como requisito parcial para obtenção do título de Doutor em Programa de Pós-Graduação em Ciência da Computação, aprovada em 25 de Setembro de 2024, pela Banca Examinadora constituída pelos professores:

Prof. Dr. Kleber Vieira Cardoso
Instituto de Informática – UFG
Presidente da Banca

Prof. Dr. Cristiano Bonato Both
PPG em Computação Aplicada – Unisinos

Prof. Dr. Antonio Carlos de Oliveira Júnior
Instituto de Informática – UFG

Prof. Dr. Aldebaro Barreto da Rocha Klautau Júnior
Faculdade de Engenharia da Computação e Telecomunicações – UFPA

Prof. Dr. Antônio Marcos Alberti
Instituto Nacional de Telecomunicações – INATEL

Prof. Dr. Joberto Sérgio Barbosa Martins
Universidade de Salvador – UNIFACS

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e do orientador(a).

Ciro José Almeida Macedo

Possui graduação em Sistemas de Informação pela Universidade Salgado de Oliveira (2006), mestrado em Engenharia Elétrica e de Computação pela Universidade Federal de Goiás (2012). Atualmente é professor efetivo no Instituto Federal de Educação, Ciências e Tecnologias de Goiás (IFG). Tem experiência em Engenharia de Software, com ênfase em Sistemas de Informação, Linguagens de Programação, Bancos de Dados, Computação em Nuvem e Desenvolvimento e Operações (DevOps). Possui como temas de interesse os problemas de integração de tecnologias de comunicação sem fio não 3GPP com redes futuras e alocação de recursos em redes sem fio de próxima geração.

Minha esposa Rosana é maravilhosa e muito me apoiou neste projeto. Meus filhos Davi e Vítor são admiráveis e me incentivam a lutar. Dedico esta tese a eles que sempre me apoiaram e, em vários momentos durante esta pesquisa, se privaram da minha presença.

Agradecimentos

A Deus, por me dar saúde e sabedoria para conseguir finalizar esta etapa. Aos meus familiares por me darem apoio e carinho durante todo o tempo da pesquisa. Aos meus orientadores, Prof. Kleber Vieira Cardoso e Prof. Cristiano Bonato Both, pela oportunidade, incentivo, paciência, amizade, colaboração e aprendizado durante todo esse processo. Aos professores que participaram da banca, pelas contribuições. Aos demais professores do curso, pelas valorosas disciplinas e ensinamentos. E a todos os meus amigos, pela torcida e pelo apoio.

Resumo

Macedo, C. J. A. **Redes de Telecomunicações Convergentes: Modelagem e Implementação de Arquitetura para Infraestruturas Pós-5G**. Goiânia, 2024. 130p. Tese de Doutorado. Programa de Pós- Graduação. Instituto de Informática, Universidade Federal de Goiás (UFG).

A evolução das redes móveis celulares tem sido guiada por diretrizes especificadas por instituições como *Third Generation Partnership Project* (3GPP), para dar suporte a serviços desafiadores. Paralelamente, tecnologias de comunicação sem fio não 3GPP, também evoluíram e desempenham um papel significativo em diversos contextos. Essas tecnologias são fundamentais para a conectividade em diversos cenários, onde a comunicação de longa distância e baixo consumo de energia são cruciais. Trabalhos recentes têm mostrado que a integração e coexistência harmoniosa entre tecnologias 3GPP e não 3GPP são essenciais no contexto das redes pós-Quinta geração de rede móvel celular (5G), potencializando a conectividade onipresente e contínua. Neste contexto, a presente tese investigou a viabilidade da convergência de tecnologias de comunicação não 3GPP com o núcleo 5G, dividindo as investigações em duas fases. Na primeira fase, foi proposta uma arquitetura para integrar essas tecnologias. Na segunda fase, um protótipo funcional dessa arquitetura foi construído para realizar experimentos que demonstrassem sua viabilidade em diferentes casos de uso. A tese realizou uma análise técnica detalhada, oferecendo uma visão abrangente dos benefícios da convergência para consumidores e fornecedores de infraestrutura. Foram identificadas lacunas significativas que ainda precisam ser abordadas nas redes pós-5G/Sexta geração de rede móvel celular (6G), como a incapacidade atual de monitoramento de redes não 3GPP pelo operador da infraestrutura 5G. Algumas dessas lacunas foram exploradas e investigadas no contexto da solução proposta nesta tese.

Palavras–chave

Coleta de dados para AI/ML, Redes móveis Pós-5G, Acesso não-3GPP, Softwarização de redes, Análise estatística da rede

Abstract

Macedo, C. J. A. **Convergent Telecommunications Networks: Modeling and Implementation of Architecture for Beyond 5G Infrastructures**. Goiânia, 2024. 130p. PhD. Thesis. Programa de Pós- Graduação. Instituto de Informática, Universidade Federal de Goiás (UFG).

The evolution of cellular mobile networks has been guided by directives specified by institutions such as 3GPP, aimed at supporting demanding services. Simultaneously, non-3GPP wireless communication technologies have also evolved and play a significant role in various contexts. These technologies are essential for connectivity in diverse scenarios where long-range communication and low power consumption are crucial. Recent studies have shown that the integration and harmonious coexistence of 3GPP and non-3GPP technologies are vital in the context of post-5G networks, enhancing ubiquitous and seamless connectivity. In this context, the present thesis investigated the feasibility of converging non-3GPP communication technologies with the 5G core, dividing the investigation into two phases. In the first phase, an architecture was proposed to integrate these technologies. In the second phase, a functional prototype of this architecture was built to conduct experiments demonstrating its viability in different use cases. The thesis conducted a detailed technical analysis, offering a comprehensive view of the benefits of convergence for consumers and infrastructure providers. Significant gaps were identified that still need to be addressed in post-5G/6G networks, such as the current inability to monitor non-3GPP networks by the 5G infrastructure operator. Some of these gaps were explored and investigated in the context of the solution proposed in this thesis.

Keywords

Data Collection for AI/ML, Post-5G Mobile Networks, Non-3GPP Access, Network Softwarization, Statistical Network Analysis

Sumário

Lista de Figuras **14**

Lista de Tabelas **16**

1 Introdução **25**

2 Fundamentação teórica **29**
- 2.1 5G e suas aplicações 29
- 2.2 Tecnologias de comunicação sem fio 3GPP e não 3GPP 34
- 2.3 Padrões 3GPP e o caminho para a convergência 36
- 2.4 Lançamentos 16 e posteriores - Ampliando caminhos para convergência 43

3 Trabalhos relacionados **47**
- 3.1 Abordagens de convergência entre tecnologias 3GPP e não 3GPP 48
- 3.2 Procedimentos de integração para tecnologias não 3GPP no contexto do 5G 50
- 3.3 Aplicações e desafios na integração de redes não 3GPP com o núcleo 5G 52

4 Arquitetura convergente **59**
- 4.1 Caminhos para acesso ao núcleo 5G 60
- 4.2 Interfaces 66
- 4.3 Estruturação do plano de controle 67
- 4.4 Estruturação do plano de dados do usuário 69
- 4.5 Protocolos 70
- 4.6 Transição de estados para o gerenciamento de registro e de autenticação 77
- 4.7 Estruturação da sessão PDU - Acesso *não confiável* 78
- 4.8 Encerramento da sessão PDU 82

5 Protótipo de arquitetura convergente **87**
- 5.1 Definição do núcleo 5G 87
- 5.2 Implementação do acesso não confiável ao núcleo 5G 88
- 5.3 Parâmetros de configuração para acesso não 3GPP ao núcleo 5G 90
- 5.4 Parâmetros de configuração da N3IWF 92
- 5.5 Estatísticas das interfaces de rede no acesso *não confiável* 96

6 Metodologia e resultados experimentais da integração do UE não 3GPP com núcleo 5G **101**
- 6.1 Metodologia de implantação e configuração dos componentes 102
- 6.2 Experimento 1 - Conectividade dos componentes da arquitetura convergente 106
- 6.3 Experimento 2 - Avaliação de desempenho de vazão 108

6.4 Experimento 3 - Monitoramento de redes não 3GPP 110
6.5 Experimento 4 - Aplicação de realidade mista 112
6.6 Experimento 5 - Aplicações prioritárias para o agronegócio 115

7 Conclusão **117**
7.1 Resultados de divulgação científica 119
7.2 Trabalhos futuros 122

Referências Bibliográficas **124**

Lista de Figuras

2.1 Cenários (ou requisitos) definidos para as redes 5G. 30
2.2 Principais componentes de software do núcleo 5G apresentados no lançamento 15, destacando a função de rede responsável por gerenciar conexões oriundas de redes *non-3GPP*. 38
2.3 Diferentes caminhos de acesso de tecnologias de comunicação sem fio não-3GPP ao núcleo 5G através de N3IWF, TNGF e TWIF. 45

4.1 Arquitetura convergente: caminhos para acesso ao núcleo 5G a partir de redes não 3GPP *confiáveis* e *não confiáveis*. 60
4.2 Módulos da arquitetura convergente para acesso ao núcleo 5G a partir de redes não 3GPP *não confiáveis*. 61
4.3 Componentes internos do UE não 3GPP, considerando o acesso *não confiável* ao núcleo 5G através da N3IWF. 62
4.4 Elementos internos do UE não 3GPP responsáveis por processamento IKE, NAS e estabelecimento de sessão PDU. 63
4.5 Componentes da API de coleta de métricas do UE não 3GPP. 64
4.6 Interfaces e túneis de comunicação *IPSec* para o trafego de dados e sinalização do Plano de Controle no acesso não-3GPP *não confiável* através de N3IWF. 65
4.7 Protocolos de comunicação envolvidos nos procedimentos de registro e autenticação no acesso não 3GPP *não confiável* através de N3IWF. 71
4.8 Protocolos de comunicação envolvidos nos procedimentos de construção do Plano de Dados do Usuário no acesso não-3GPP *não confiável* através de N3IWF. 71
4.9 Sequência de procedimentos para registro, autenticação e autorização do UE não 3GPP e o núcleo 5G. 74
4.10 Sequência de procedimentos para o estabelecimento da sessão PDU. 79

6.1 Topologia de rede utilizada na implantação do protótipo da arquitetura convergente. 102
6.2 Inicialização da N3IWF com destaque para a execução de procedimentos que viabilizam o acesso não 3GPP *não confiável*. 104
6.3 Inicialização do UE não 3GPP. Procedimentos de configuração NAS, IKE e *enlace* IPSec. 105
6.4 Túneis IPSec para sinalização NAS do plano de controle (1) e GRE para o trafego do plano de dados do usuário (2). 106
6.5 Teste de conectividade do UE não 3GPP através do uso de *ping* com inundação de pacotes (*flooding*). 107
6.6 Teste de conectividade do UE não 3GPP através do uso de *traceroute*. 108

6.7 Vazão da interface *gretun1* obtida a partir do serviço de API do UE não 3GPP. 109
6.8 Topologia de rede utilizada no experimento de monitoramento de redes não 3GPP por meio de métricas coletadas do UE não 3GPP. 110
6.9 Potência do sinal da interface de rede Wi-Fi vs taxa de transferência. Medidas obtidas através da API de coleta de métricas do UE não 3GPP durante aproximadamente 60 segundos. 112
6.10 Fluxo de funcionamento do MR-Leo integrado ao protótipo da arquitetura convergente através do acesso não confiável. 113
6.11 Aplicação de Realidade Mista com MR-Leo em operação no lado cliente. 114
6.12 Aplicações prioritárias para o Agronegócio com conectividade através de acesso não 3GPP não confiável. 116

Lista de Tabelas

2.1 Evolução das gerações dos sistemas de redes móveis 36

3.1 Comparação da arquitetura convergente apresentada neste trabalho com outros trabalhos relevantes da literatura 57

5.1 Critérios para escolha do núcleo 5G para compor protótipo de arquitetura convergente 88
5.2 Parâmetros de autenticação do UE não 3GPP no núcleo 5G 91
5.3 Parâmetros para identificação e registro do UE não 3GPP no núcleo 5G 91
5.4 Parâmetros de identificação de endereços IP e nomenclatura das interfaces de rede para os planos de dados do usuário e de plano de controle no UE não 3GPP 92
5.5 Parâmetros de identificação de fatias de rede e da sessão PDU do UE não 3GPP 93
5.6 Parâmetros de identificação da N3IWF no UE não 3GPP 93

6.1 Infraestrutura de Hardware e Software para Implantação do Protótipo 103
6.2 Resultados obtidos após o uso de *ping* com inundação de pacotes (*flooding*) 107
6.3 Configurações dos dispositivos físicos para o monitoramento de redes não 3GPP 111
6.4 Configurações do ponto de acesso Wi-Fi para o monitoramento de redes não 3GPP 111
6.5 Distribuição do tempo necessário para processar um quadro de vídeo pela aplicação de realidade mista com MR-Leo 115

7.1 Resultados científicos 120
7.2 Resultados técnicos 121

Lista de Abreviaturas

3D Tridimensional

3GPP *Third Generation Partnership Project*

1G Primeira geração de rede móvel celular

2G Segunda geração de rede móvel celular

3G Terceira geração de rede móvel celular

4G Quarta geração de rede móvel celular

5G Quinta geração de rede móvel celular

5GS Sistema 5G

5GNR *5G New Radio*

5G-GUTI *5G Globally Unique Temporary Identifier*

5G-AKA *5G Authentication and Key Agreement*

6G Sexta geração de rede móvel celular

AR Realidade Aumentada

AVR Realidade Virtual Aumentada

AES-CBC *Advanced Encryption Standard with a 256-bit key in Cipher Block Chaining*

AH *Authentication Header*

AKA *Authentication and Key Agreement*

AMF *Access and Mobility Management Function*

ANDSP *Access Network Discovery and Selection Policy*

API *Application Programming Interface*

AUSF *Authentication Server Function*

ATSSS *Access Traffic Steering, Switching, and Splitting*

BS *Base Station*

BNDES Banco Nacional de Desenvolvimento Econômico e Social

CSS *Chirp Spread Spectrum*

CM-CONNECTED *Connection Management - Connected Mode*

CM-IDLE *Connection Management - Idle Mode*

D2D *Device-to-Device*

DNN *Data Network Name*

DNS *Domain Name System*

eMBB *Enhanced Mobile Broadband*

EAP *Extensible Authentication Protocol*

EAP-AKA *Extensible Authentication Protocol - Authentication and Key Agreement*

EPC *Evolved Packet Core*

ESP *Encapsulating Security Payload*

FQDN *Fully Qualified Domain Name*

GTP *General Packet Radio Service Tunneling Protocol*

GTPU *General Packet Radio Service Tunneling Protocol for the User Plane*

GFDM *Generalized Frequency Division Multiplexing*

GRE *Generic Routing Encapsulation*

GUAMI *Globally Unique AMF Identifier*

Gbps Gigabits por segundo

GSM *Global System for Mobile communication*

HTTP *HyperText Transfer Protocol*

HPLMN *Home Public Land Mobile Network*

HMAC-SHA1-96 *Hash-based Message Authentication Code Secure Hash Algorithm 1-96*

IEEE *Institute of Electrical and Electronics Engineers*

IA Inteligência Artificial

ICMP *Internet Control Message Protocol*

IKE *Internet Key Exchange*

IKE-SA *Internet Key Exchange Security Association*

IMSI *International Mobile Subscriber Identity*

INPI Instituto Nacional de Propriedade Intelectual

IoT *Internet Of Things*

IPSec-SA *IPsec Security Association*

IP *Internet Protocol*

IPSec *Internet Protocol Security*

JSON *JavaScript Object Notation*

L1 *Physical Layer*

L2 *Data Link Layer*

LPWA *Low-Power Wide Area*

Li-Fi *Light Fidelity*

LTE *Long Term Evolution*

LoRa *Long Range*

LoRaWAN *Long Range Wide-Area Network*

LPWAN *Low Power Wide Area Networks*

Mbps Megabits por segundo

MB Megabyte

mMTC *Massive Machine-type communication*

MCC *Mobile Country Code*

MNC *Mobile Network Code*

MOBIKE *IKEv2 Mobility and Multihoming Protocol*

MRAT *Multiple Radio Access Technology*

MR Realidade Mista

MR-Leo *Mixed Reality Linköping Egde Offloading*

MSIN *Mobile Station Identification Number*

MTU *Maximum Transmission Unit*

N5CW *Non-5G Capable over WLAN*

NAS *Non-Access Stratum*

NEF *Network Exposure Function*

NGAP *Next-Generation Application Protoco*

NRF *Network Repository Function*

NSA *Non-Stand Alone*

NSSAI *Network Slice Selection Assistance Information*

N3IWF *Non-3GPP InterWorking Function*

N3AN *Non-3GPP Access Networks*

NR *New Radio*

NR-U *New Radio Unlicensed*

ODU *Outdoor Unit*

ORB *Oriented FAST and Rotated BRIEF*

PLMN *Public Land Mobile Network*

PCF *Policy Control Function*

PDU *Protocol Data Unit*

QoS *Quality of Service*

REST *Representational State Transfer*

RM-REGISTERED *Registered Mode*

RM-DEREGISTERED *Deregistered Mode*

SA *Stand-Alone*

SD *Slice Differentiator*

SST *Slice/Service Type*

SCTP *Stream Control Transmission Protocol*

SBA *Service-Based Architecture*

SDR *Software-Defined Radio*

SEAF *Security Anchor Function*

SMF *Session Management Function*

S-NSSAI *Single Network Slice Selection Assistance Information*

SLAM *Simultaneous Localization and Mapping*

SUCI *Subscription Concealed Identifier*

SUPI *Subscription Permanent Identifier)*

TCP *Transmission Control Protocol*

TNAP *Trusted Non-3GPP Access Point*

TNGF *Trusted Non-3GPP Gateway Function*

TVWS *TV White Space*

TWAP *Trusted WLAN Access Point*

TWIF *Trusted WLAN Interworking Function*

UMTS *Universal Mobile Telecommunications System*

UDM *Unified Data Management*

UDR *Unified Data Repository*

UDP *User Datagram Protocol*

UE *User Equipment*

UPF *User Plane Function*

URL *Uniform Resource Locator*

URLLC *Ultra Reliable Low Latency Communication*

VANT Veículo Aéreo não Tripulado

V2I *Vehicle-to-Infrastructure Communication*

V2V *Vehicle-to-vehicle*

VNF *Virtual Network Function*

VR Realidade Virtual

VM *Virtual Machine*

WLAN *Wireless Local-Area Network*

WLANSP WLAN Selection Policy

Wi-Fi *Wireless Fidelity*

YAML *YAML Ain't Markup Language*

CAPÍTULO 1

Introdução

Ao longo das últimas décadas, as redes móveis celulares evoluíram seguindo diretrizes especificadas pelos chamados lançamentos (*Releases*) de entidades de padronização, como, por exemplo, o 3GPP. Redes da Quarta geração de rede móvel celular (4G) foram introduzidas em 2008, no Lançamento 8 [3GPP TR-21.101 2009], e, desde então, passaram a receber várias atualizações, até que a 5G fosse introduzida oficialmente no Lançamento 15, em 2018 [3GPP TR-21.915 2018-12]. Cada geração possui, como alicerce, um conjunto de fatores técnicos. Por exemplo, na rede 5G, isso aparece no uso do espectro, que, além de ampliar a utilização das bandas tradicionalmente alocadas, na ordem de centenas de MHz até algumas unidades de GHz, introduz ainda a utilização de bandas de dezenas de GHz. Além disso, redes 5G consolidam um intenso processo de *softwarização*, que se destaca pela adoção de sistemas de nuvem e tecnologias como virtualização, redes definidas por software, fatiamento de rede (*Network Slicing*) e arquitetura de software baseada em microsserviços [Both et al. 2020].

Por outro lado, tecnologias de comunicação sem fio não 3GPP também evoluíram e se consolidaram, desempenhando um papel relevante e multifacetado, contribuindo significativamente para a conectividade em diversos contextos. O *Wireless Fidelity* (Wi-Fi), por exemplo, é consolidado em residências, escritórios, espaços públicos e industriais, oferecendo acesso rápido e confiável à Internet. Além de seu uso tradicional, o Wi-Fi possui características que habilitam sua utilização em casos de uso e aplicações avançadas, que ainda estão em desenvolvimento, como, por exemplo, a comunicação entre veículos - *Vehicle-to-vehicle* (V2V) e a comunicação envolvendo veículos e a infraestrutura - *Vehicle-to-Infrastructure Communication* (V2I) [Nguyen et al. 2021]. Tecnologias como *Long Range* (LoRa) / *Long Range Wide-Area Network* (LoRaWAN) ganham destaque nas aplicações de Internet das coisas - *Internet Of Things* (IoT), onde a necessidade de comunicação em longas distâncias e baixo consumo de energia é um fator crítico [Sunny et al. 2021]. LoRa possui características que o tornam ideal para monitoramento ambiental, agricultura inteligente, gestão de recursos hídricos e outras aplicações que requerem dispositivos com baixo consumo de energia, operando em áreas extensas e de difícil acesso [Duan et al. 2020].

A relevância de tecnologias não 3GPP é amplificada quando consideramos a integração e coexistência com redes 3GPP, especialmente no contexto da 6G. A coexistência harmoniosa entre tecnologias 3GPP e não 3GPP possui potencial para habilitar uma conectividade onipresente e contínua, combinando a alta velocidade e baixa latência das redes móveis 3GPP com a ampla cobertura e eficiência energética das redes não 3GPP. A integração entre tecnologias 3GPP e não 3GPP se mostra relevante no sentido de suportar as demandas crescentes de uma sociedade cada vez mais interconectada e dependente de tecnologias avançadas de comunicação, podendo trazer benefícios tanto para clientes quanto para fornecedores de infraestrutura [Torroglosa-Garcia et al. 2020]. No entanto, apesar do potencial promissor, os caminhos para que a coexistência de tecnologias de comunicação 3GPP e não 3GPP se estabeleça de fato ainda não estão totalmente claros. Os padrões definidos pelo 3GPP não fornecem diretrizes detalhadas para a integração de algumas tecnologias importantes, como, por exemplo, LoRa/LoRaWAN, Sigfox ou Weightless, o que representa um desafio significativo para a criação de um ecossistema de comunicação unificado. A ausência de especificações claras para essa integração pode resultar em dificuldades na implementação prática e na interoperabilidade entre diferentes sistemas.

Nesse sentido, o presente trabalho apresenta duas questões de pesquisa de interesse, que norteiam as investigações desempenhadas, sendo ambas relacionadas à convergência de tecnologias de comunicação sem fio não 3GPP e ao núcleo 5G:

1. Quais são os requisitos e desafios para o desenvolvimento de uma arquitetura de sistema que permita a convergência de tecnologias 3GPP e não 3GPP em redes de acesso de próxima geração ?
2. Como essa arquitetura convergente amplia a observabilidade e o monitoramento da infraestrutura 5G para redes de acesso não 3GPP ?

Nesse contexto, o presente trabalho visa contribuir para a viabilidade da convergência de diferentes tecnologias de comunicação não 3GPP com o núcleo 5G. Para isso, as investigações foram divididas em duas fases. Na primeira fase, foi proposta uma arquitetura convergente que integre tecnologias não 3GPP de maneira coesa, seguindo as diretrizes 3GPP, que especificam como o acesso ao núcleo 5G deve ser realizado. Na segunda fase, foi construído um protótipo funcional dessa arquitetura, com o objetivo de executar experimentos que demonstrarão sua viabilidade, considerando diferentes casos de uso. O protótipo em questão permite avaliar como tecnologias não 3GPP podem ser combinadas com redes 5G para proporcionar uma conectividade mais robusta e abrangente.

Além disso, o presente estudo se propôs a analisar os benefícios potenciais dessa convergência, tanto para os consumidores quanto para os fornecedores de infraestrutura. A integração de tecnologias não 3GPP com o núcleo 5G pode trazer vantagens significativas,

como maior cobertura, uma eficiência energética aprimorada e a capacidade de suportar uma vasta gama de aplicações em diferentes cenários. Além disso, a convergência entre tecnologias não 3GPP e 3GPP tem o potencial de habilitar a observabilidade, por parte do operador da infraestrutura, sobre o comportamento das redes não 3GPP. Isso ampliaria o poder de decisão, permitindo aos operadores do sistema a aplicação de melhorias na infraestrutura de comunicação, como, por exemplo, o fatiamento de rede e a otimização dos recursos. Essas vantagens podem se traduzir em serviços mais avançados e acessíveis para os usuários finais, bem como em novas oportunidades de mercado para os fornecedores de tecnologia. Ao identificar e compreender esses benefícios, através dos experimentos realizados com o protótipo funcional, este trabalho forneceu uma base sólida para futuras pesquisas e desenvolvimento na área de telecomunicações, promovendo uma conectividade contínua e onipresente que atenda às demandas de uma sociedade cada vez mais interconectada.

O restante do documento está organizado conforme descrito a seguir.

- No Capítulo 2, o referencial teórico é apresentado. Este capítulo aborda conceitos essenciais para o entendimento do restante do trabalho. Inicialmente, são introduzidas as redes 5G e suas variadas aplicações, desde cidades inteligentes e IoT até telemedicina e Indústria 4.0. Além disso, discute-se a convergência de tecnologias de comunicação sem fio 3GPP e não 3GPP com o núcleo 5G, destacando o potencial para uma conectividade contínua e onipresente. O capítulo inclui, ainda, a apresentação da arquitetura 5G, conforme estabelecida no lançamento 15 do 3GPP, com ênfase nas funções de rede como a função de gerenciamento de acesso e mobilidade - *Access and Mobility Management Function* (AMF), função de gerenciamento de sessão - *Session Management Function* (SMF) e a função de interconexão não-3GPP - *Non-3GPP InterWorking Function* (N3IWF), e explora as melhorias introduzidas nos lançamentos subsequentes, visando suportar uma ampla gama de serviços e aplicações com diferentes requisitos de desempenho.
- No Capítulo 3, são apresentados os principais trabalhos que abordam aspectos associados à convergência de tecnologias não 3GPP e o núcleo 5G. O capítulo oferece uma visão geral de trabalhos que exploram cenários onde diferentes tecnologias de rede se integram com o 5G para criar uma infraestrutura de comunicação coesa e eficiente. Estudou-se diversas abordagens e soluções para a integração de tecnologias não 3GPP e redes de 4G/5G, destacando-se métodos que incluem a modificação de *gateways* e a utilização de computação em borda. Além disso, avaliou-se desafios como a complexidade de implementação e a necessidade de escalabilidade e segurança na comunicação entre redes heterogêneas.
- No capítulo 4, a proposta de arquitetura convergente é apresentada, detalhando a integração de tecnologias de comunicação sem fio não 3GPP com o núcleo

5G. A arquitetura inclui acesso não confiável via N3IWF, destacando elementos fundamentais e funções de rede disponíveis em implementações de núcleo 5G de código aberto, como free5GC [free5GC 2022] e Open5GS [Open5GC 2019]. A proposta visa garantir a flexibilidade e segurança na comunicação entre diferentes tecnologias e o núcleo 5G.

- No capítulo 5, o protótipo da arquitetura convergente é apresentado, detalhando a construção e validação da integração entre tecnologias de comunicação sem fio não 3GPP e o núcleo 5G. O capítulo descreve os componentes e etapas do protótipo, destacando as funcionalidades desenvolvidas e os desafios enfrentados. A escolha do free5GC como núcleo 5G baseia-se na sua robustez e no suporte para N3IWF. A implementação envolve a criação de um *User Equipment* (UE) não 3GPP em GO [Google 2022], garantindo a segurança da comunicação com o núcleo 5G através de túneis *Internet Protocol Security* (IPSec) e protocolos de autenticação como *Internet Key Exchange* (IKE)-v2 e *Extensible Authentication Protocol* (EAP)-5G. Por fim, o capítulo apresenta e discute os os experimentos, voltados para analisar o desempenho da arquitetura convergente proposta e sua capacidade de integrar tecnologias não 3GPP ao núcleo 5G.
- No capítulo 6, são realizados os experimentos que validam a proposta de arquitetura convergente, demonstrando a viabilidade da integração de tecnologias de comunicação sem fio não 3GPP com o núcleo 5G. Os experimentos foram conduzidos utilizando a implementação de núcleo 5G de código aberto free5GC [free5GC 2022], com foco na avaliação de desempenho do acesso não confiável via N3IWF. São detalhados os procedimentos de configuração, testes de conectividade e análises de desempenho, incluindo a capacidade da arquitetura em suportar aplicações críticas em diferentes cenários de uso, assegurando a eficácia da comunicação e a flexibilidade na gestão dos recursos de rede.
- Por fim, o capítulo 7 apresenta a conclusão sobre as pesquisas e investigações aqui descritas e enumera as contribuições geradas como publicações. Além disso, são exploradas as implicações dos resultados para a evolução futura das redes 5G e 6G, com sugestões de melhorias e possíveis adaptações na arquitetura para maximizar a eficiência e a segurança da comunicação em diversos cenários, incluindo aplicações críticas e ambientes complexos.

CAPÍTULO 2

Fundamentação teórica

Este capítulo apresenta a fundamentação teórica dentro do escopo da pesquisa. Iniciando pelos conceitos fundamentais envolvendo 5G e suas aplicações, apresenta-se a evolução das redes móveis e suas capacidades de alta velocidade e baixa latência, essenciais para tecnologias emergentes como realidade aumentada e IoT. Em seguida, aborda-se a integração das tecnologias de comunicação sem fio 3GPP e não 3GPP, enfatizando a importância da convergência para garantir conectividade contínua e eficiente. Por fim, são explorados os padrões 3GPP, com destaque para as arquiteturas avançadas e as funções de rede que possibilitam a integração segura e eficiente dessas tecnologias no contexto das redes 5G.

2.1 5G e suas aplicações

Antes do 5G, as redes móveis sem fio tinham como foco principal o aumento da taxa de transmissão de dados e a oferta de acesso para os consumidores finais. Contudo, além de aprimorar a capacidade de transmissão e diminuir o tempo de resposta [Shafi et al. 2017], as redes 5G possibilitam o surgimento de inovações transformadoras em uma ampla variedade de setores industriais [Kaloxylos 2018]. Comparadas ao seu antecessor, as redes 5G oferecem taxas de transferência de dados exponencialmente mais rápidas e latência reduzida. Esse avanço não só melhora a experiência do usuário, permitindo downloads mais rápidos, *streaming* sem interrupções, pausas ou atrasos e jogos contínuos, mas também facilita a adoção de novas tecnologias, como realidade aumentada, realidade virtual e IoT. Além disso, a menor latência e a maior largura de banda do 5G o tornam adequado para aplicações críticas, como cirurgia remota, veículos autônomos e infraestruturas de cidades inteligentes. No geral, a transição para o 5G representa uma nova era de conectividade, abrindo possibilidades de inovação e transformando a forma como as pessoas interagem com a tecnologia de uma forma geral. Embora o 5G esteja disponível em alguns países desde 2019, ainda está nas fases iniciais da transição entre a 4G e 5G. De acordo com estimativas [Ericsson 2024], o número de assinaturas de *smartphones* 5G em todo o mundo atingiu 1,5 bilhões até o

final de 2023 e a expectativa é que mais de 2,4 bilhões de dispositivos utilizem redes 5G até 2025 [Felix Richter 2024]. Atualmente, taxas de transmissão que se aproximam ou até ultrapassam 1 Gigabits por segundo (Gbps) representam a inovação que mais se destaca; no entanto, diversos serviços, especialmente aqueles fundamentados em IoT, estão em fase de planejamento e implementação. Veículos autônomos, Indústria 4.0 e as experiências em realidade virtual, aumentada ou mista são vistos como investimentos promissores, frequentemente considerados como exemplos práticos interessantes para explorar as novas capacidades oferecidas pela rede.

Para conseguir atender a essas expectativas, as redes 5G foram projetadas com algumas mudanças tecnológicas consideráveis. As especificações do 3GPP estruturam as redes 5G tendo como base um intenso processo de *softwarização*, que se destaca pela adoção de sistemas de nuvem e tecnologias como virtualização [Abdelwahab et al. 2016], redes definidas por software [Chen et al. 2015], fatiamento de rede [Foukas et al. 2017] e arquitetura de software baseada em serviços [Mademann 2018] e microsserviços. Além das inovações tecnológicas, também foram introduzidas mudanças no modelo de negócios das empresas. Os operadores de sistemas de comunicação móvel, que tinham como foco principal os usuários finais, passam a ter a possibilidade de ampliar sua área de atuação, tendo a indústria como principal cliente [Palattella et al. 2016]. Para dar suporte a essa ampliação do modelo de negócios dos operadores, três requisitos principais foram definidos: Banda larga móvel aprimorada – *Enhanced Mobile Broadband* (eMBB), Comunicações de baixa latência ultra confiáveis – *Ultra Reliable Low Latency Communication* (URLLC) e Comunicações massivas de tipo máquina – *Massive Machine-type communication* (mMTC). Esses cenários, bem como o posicionamento dos possíveis casos de uso associados a cada um deles, podem ser ilustrados pela Figura 2.1.

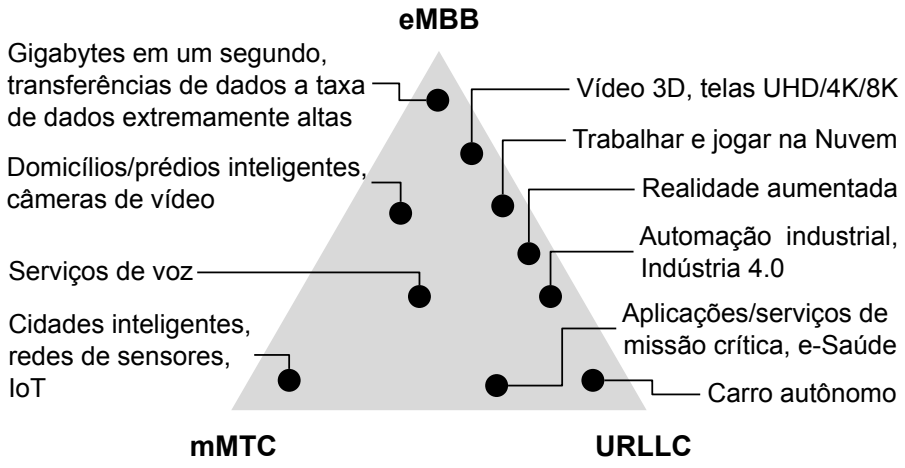

Figura 2.1: Cenários (ou requisitos) definidos para as redes 5G.

Com o objetivo de atender às demandas das possíveis aplicações associadas a

cada um dos cenários ilustrados na Figura 2.1, a ideia de *softwarização* das redes começou a ser implementada e o termo passou a ser adotado tanto pela academia quanto pela indústria [Both et al. 2020]. A razão principal para a adoção extensiva de software em sistemas 5G está associada à necessidade de proporcionar maior flexibilidade à arquitetura de rede móvel, de modo a atender a variados requisitos em casos de uso emergentes na sociedade digital [Foukas et al. 2017]. Nas seções a seguir, apresenta-se detalhes de cada um dos requisitos técnicos e aplicações práticas delineadas para as redes 5G, conforme ilustrado na Figura 2.1. A seção aborda as aplicações URLLC, eMBB e mMTC, destacando como cada um desses cenários suporta diferentes casos de uso. Além disso, discute-se a integração de tecnologias não 3GPP com o núcleo 5G, explorando como essa convergência tem potencial de ampliar ainda mais as possibilidades de inovação e flexibilidade das redes de nova geração.

Aplicações URLLC

No contexto das redes 5G, URLLC foi projetado para atender às necessidades de comunicação que exigem alta confiabilidade (i.e., 99,999%) e baixa latência (i.e., inferior a 1 ms) [ITU-R M.2083-0 2015]. Essas características permitem que aplicações estruturadas com base nos parâmetros de URLLC possam atender a requisitos em que o tempo de resposta e a confiabilidade na transmissão de dados são cruciais. Esse avanço possibilita o desenvolvimento e a implementação de tecnologias inovadoras em setores como saúde, manufatura, transporte e segurança pública, onde atrasos mínimos e alta confiabilidade podem ser a diferença entre sucesso e falha, segurança e perigo [Khan et al. 2022].

Por exemplo, no setor da saúde, URLLC pode habilitar cirurgias remotas realizadas por robôs controlados em tempo real por cirurgiões que podem estar a quilômetros de distância do paciente. A baixa latência e a alta confiabilidade são fundamentais para garantir a precisão dos movimentos do robô e a segurança do paciente, permitindo que procedimentos complexos sejam realizados com maior precisão e menores riscos. Além disso, URLLC pode facilitar o monitoramento remoto de pacientes críticos em tempo real, possibilitando intervenções imediatas em casos de emergência, o que pode salvar vidas e reduzir significativamente os custos hospitalares [Tebe et al. 2022].

Nos transportes, veículos autônomos podem se beneficiar de URLLC, pois a comunicação em tempo real, com latência quase zero, é importante para a segurança e eficiência em cenários de comunicações do tipo V2V e V2I. Nesse contexto, as características de URLLC podem habilitar a tomada de decisões em tempo quase real, contribuindo para a redução no número de acidentes e na otimização do fluxo de tráfego, melhorando a mobilidade urbana [Noor-A-Rahim et al. 2022].

Em regiões onde a cobertura 5G é insuficiente ou inexistente, veículos autônomos e outros dispositivos que dependem de comunicações URLLC podem ter sua capacidade de operar de forma segura e eficiente comprometida. A situação se agrava se considerar o transporte autônomo, onde a capacidade de realizar comunicações em tempo real V2V e V2I é vital para evitar acidentes e otimizar o fluxo de tráfego. Nesses cenários, uma abordagem híbrida pode ser a solução para estender a cobertura de comunicação e preencher as lacunas deixadas pelo 5G em áreas remotas. Nesse sentido, a convergência de tecnologias não 3GPP com o núcleo 5G pode assegurar conectividade contínua e confiável.

Aplicações eMBB

Aplicações caracterizadas como eMBB demandam alta largura de banda e baixa latência. Esses requisitos geralmente estão associados a aplicações voltadas para o *streaming* de vídeo em ultra-alta definição (4K/8K), jogos online e aplicações de realidade virtual/aumentada sem atrasos perceptíveis. As características de eMBB são importantes para dar suporte à crescente produção de conteúdo de vídeo na Internet, jogos online de próxima geração e à crescente utilização de serviços de comunicação em vídeo.

Além do entretenimento, eMBB atua como elemento habilitador de novas aplicações em diversos setores. Na saúde, por exemplo, eMBB pode viabilizar consultas médicas à distância em alta definição, permitindo diagnósticos e tratamentos mais rápidos e eficazes. Isso é especialmente relevante em áreas remotas ou com escassez de especialistas [Peralta-Ochoa et al. 2023]. Além disso, a capacidade de transmitir grandes quantidades de dados em tempo real pode trazer benefícios à telemedicina, com aplicações como cirurgias remotas assistidas por robôs e monitoramento contínuo da saúde dos pacientes através de dispositivos vestíveis.

No setor industrial, eMBB pode beneficiar setores como manufatura e logística por meio da implementação de fábricas inteligentes que utilizam dispositivos IoT. A alta capacidade e velocidade das redes 5G permitem a comunicação em tempo real entre uma grande quantidade de dispositivos e sensores, facilitando a manutenção preditiva e a otimização da cadeia de suprimentos [Khan et al. 2022].

Fatores relacionados à infraestrutura podem prejudicar ou até mesmo inviabilizar o funcionamento de aplicações que fazem uso de eMBB. As redes 5G, em especial nas faixas de frequência mais altas, têm um alcance mais curto e baixa penetração [Barb et al. 2022]. Isso significa que uma quantidade maior de antenas e células é necessária para prover cobertura ampla e contínua. Considerando áreas rurais ou remotas, o alto custo logístico e de implantação pode inviabilizar a expansão da infraestrutura. Uma abordagem híbrida, envolvendo tecnologias não 3GPP consolidadas e de amplo uso, como, por

exemplo, Wi-Fi, integradas ao núcleo 5G, pode representar um caminho para prover conectividade contínua e confiável a áreas rurais ou remotas, viabilizando o funcionamento de aplicações caracterizadas como eMBB.

Aplicações mMTC

mMTC refere-se à capacidade de suportar um grande número de dispositivos (dezenas ou centenas de milhares por quilômetro quadrado) conectados em uma área. mMTC é especialmente relevante para IoT, considerando uma vasta quantidade de sensores, dispositivos e máquinas que precisam se comunicar uns com os outros e com sistemas centrais, sem intervenção humana. Nesses cenários, eficiência, escalabilidade e capacidade de gerenciamento das redes 5G são características habilitadoras para a comunicação em massa.

No setor de saúde, mMTC tem a capacidade de habilitar sistemas de monitoramento remoto, onde dispositivos vestíveis podem coletar dados de saúde em tempo real e transmiti-los para profissionais de saúde, melhorando o diagnóstico e a personalização do tratamento [Peralta-Ochoa et al. 2023]. Na agricultura de precisão, sensores e dispositivos IoT podem monitorar as condições do solo, do clima e da saúde das plantas, automatizando a irrigação e a aplicação de nutrientes [Khanh et al. 2022]. Cidades inteligentes são outro exemplo, onde uma ampla gama de sensores pode gerenciar o fluxo de tráfego e sistemas de iluminação pública, melhorando a eficiência dos serviços urbanos e a qualidade de vida dos habitantes [Yang et al. 2022].

É importante destacar que aplicações que utilizam mMTC dependem fortemente de uma infraestrutura de rede robusta e bem desenvolvida. Se considerar o setor agrícola, onde as áreas de cultivo podem alcançar dezenas de quilômetros quadrados, a ausência de infraestrutura de comunicação pode inviabilizar o funcionamento de aplicações que fazem uso de mMTC. A convergência de tecnologias não 3GPP e o núcleo 5G emerge como uma solução em potencial. Especialmente em setores como o agronegócio, tecnologias não 3GPP de longo alcance, como LoRa e LoRaWAN, podem operar dispositivos IoT com baixo consumo de energia [Yasmin et al. 2017, Navarro-Ortiz et al. 2018, Mikhaylov et al. 2018]. Considerando a convergência dessas tecnologias não 3GPP e o núcleo 5G, benefícios adicionais, tais como ampliação da capacidade, baixa latência e ampliação da cobertura, poderiam ser agregados. A combinação dessas tecnologias possibilitaria a implementação de soluções avançadas de agricultura de precisão, otimização de recursos hídricos e monitoramento ambiental. Além disso, a integração entre redes 5G privadas e redes 3GPP pode abrir caminho para infraestruturas de comunicação controladas e seguras, garantindo a confidencialidade e integridade dos dados.

2.2 Tecnologias de comunicação sem fio 3GPP e não 3GPP

Quando refere-se especificamente sobre tecnologias de comunicação sem fio, é importante distinguir entre aquelas definidas pelo 3GPP e as que não são. As tecnologias 3GPP (i.e., *Global System for Mobile communication* (GSM), *Universal Mobile Telecommunications System* (UMTS), *Long Term Evolution* (LTE) e 5G) são padronizadas por um consórcio global que inclui organizações de padronização de telecomunicações de várias partes do mundo. Essas tecnologias são projetadas e padronizadas para garantir interoperabilidade, segurança e eficiência em comunicações móveis, facilitando uma ampla adoção global e suportando serviços de comunicação, desde voz até dados de alta velocidade. Entretanto, as tecnologias de comunicação sem fio não 3GPP (i.e., Wi-Fi, LoRa, LoRaWAN, *SigFox*, *Weightless*) são definidas por outros orgãos de padronização e tendem a ser focadas em aplicações de curto alcance. Enquanto as tecnologias 3GPP são projetadas para operar em larga escala e oferecer mobilidade global, as tecnologias não 3GPP são mais adaptadas para redes locais ou aplicações que requerem menos mobilidade [Lemes et al. 2022]. A principal diferença entre essas duas categorias reside no escopo de aplicação, no alcance e nas entidades de padronização envolvidas. A seguir, mais detalhes relevantes sobre cada uma das tecnologias de comunicação sem fio não 3GPP são apresentados, considerando o escopo deste trabalho:

- ***SigFox*** é uma tecnologia de comunicação sem fio do tipo *Low-Power Wide Area* (LPWA). Projetada especificamente para IoT, ela permite que dispositivos se comuniquem em longas distâncias com baixo consumo de energia. Diferente das tecnologias de comunicação celular tradicionais, *SigFox* opera em uma banda de frequência estreita, o que significa que transmite dados em pequenas quantidades, mas de forma muito eficiente em termos de energia. Isso a torna ideal para aplicações em que os dispositivos precisam enviar pequenos volumes de dados ao longo de grandes distâncias, sem a necessidade de recarregar ou substituir baterias frequentemente.
- ***LoRa / LoRaWAN*** são termos frequentemente usados em conjunto no contexto de IoT, mas referem-se a componentes distintos de uma mesma tecnologia de comunicação sem fio de longo alcance [Semtech Corp. 2024]. LoRa é uma tecnologia de modulação de rádio, patenteada pela empresa *Semtech*, que permite a comunicação sem fio de longo alcance entre dispositivos de IoT. LoRa utiliza uma técnica de modulação *Chirp Spread Spectrum* (CSS), com alta penetração em ambientes urbanos densos e capacidade de comunicação em longas distâncias no campo, com baixo consumo energético [Nguyen et al. 2019]. LoRaWAN é a arquitetura de sistema para redes baseadas na tecnologia LoRa. Enquanto LoRa define a camada

física, ou a tecnologia de modulação sem fio utilizada para criar a ligação de comunicação, LoRaWAN define a camada de controle, que é responsável pela gestão da comunicação entre dispositivos finais e *gateways*, bem como entre os *gateways* e o servidor de rede.

- ***Weightless*** *Weightless* é uma tecnologia de comunicação sem fio que propõe padrões de conectividade de baixo custo, longo alcance e baixo consumo de energia para atender às demandas de IoT. Existem diferentes versões de *Weightless*, incluindo *Weightless-P*, *Weightless-N* e *Weightless-W*, cada uma otimizada para diferentes aplicações e ambientes de uso. O objetivo principal é fornecer uma solução abrangente para a comunicação sem fio de dispositivos IoT em ambientes urbanos e rurais, superando limitações de outras tecnologias, como cobertura insuficiente ou alto consumo de energia [Weightless 2024, al 2024].
- ***Wi-Fi*** surgiu na década de 1990 sob o padrão IEEE 802.11 [IEEE Std 802.11 2016] e evoluiu com novas versões (i.e., 802.11b [Ohrtman 2003], 802.11g [Vassis et al. 2005], 802.11n [Xiao 2005], e, mais recentemente, 802.11ax [Khorov et al. 2018]), cada uma delas com diferentes velocidades de transmissão e alcances. Wi-Fi utiliza ondas de rádio para transmitir informações através de redes *Wireless Local-Area Network* (WLAN) e é bastante consolidada, com ampla adoção global, suportando uma ampla gama de aplicações de comunicação e entretenimento [Ericcson 2024].

As tecnologias de comunicação 3GPP e não 3GPP apresentam características técnicas e focos de atuação parcialmente distintos. No entanto, ao considerar um cenário de redes futuras, onde a demanda por conectividade tende a crescer exponencialmente e novas aplicações do tipo eMBB, mMTC e URLLC se tornam cada vez mais prevalentes, a coexistência e integração coesa dessas tecnologias podem trazer benefícios consideráveis em diversos contextos. A combinação dessas diferentes abordagens tecnológicas pode proporcionar maior flexibilidade e capacidade de adaptação às necessidades específicas de cada aplicação, otimizando o uso de recursos e melhorando a eficiência global da rede. Além disso, a convergência de tecnologias não 3GPP com o núcleo 5G pode ampliar ainda mais as possibilidades de inovação, permitindo a implementação de soluções mais robustas e abrangentes.

Integrar tecnologias de comunicação sem fio não 3GPP com tecnologias 3GPP é um caminho para aprimorar a conectividade e a experiência dos usuários. A combinação dessas tecnologias permite uma transição suave entre redes celulares e locais sem fio, assegurando que os usuários mantenham uma conexão estável e de alta velocidade. Por exemplo, a integração de Wi-Fi e 3GPP facilita a implementação de cidades inteligentes, onde uma grande quantidade de serviços e aplicações pode ser fornecida de forma mais eficaz. A evolução dos padrões 3GPP, especialmente a partir do lançamento 15

[3GPP TR-21.915 2018-12], sugere que o 3GPP reconhece que algumas tecnologias não 3GPP estão bem estabelecidas e que substituí-las seria inviável. A seção a seguir apresenta mais detalhes sobre os lançamentos recentes, bem como os possíveis caminhos descritos nas especificações técnicas, aptos a habilitar a convergência de tecnologias não 3GPP com o núcleo 5G.

2.3 Padrões 3GPP e o caminho para a convergência

Os sistemas de redes móveis definidos pelo 3GPP têm evoluído de forma significativa desde que foram introduzidos. Essas evoluções são caracterizadas como *gerações* e apresentam um conjunto de novas tecnologias que modificam os serviços ofertados pela rede móvel. A Tabela 2.1 sumariza as principais características que marcaram cada uma das gerações anteriores ao 5G. Analisando as evoluções das gerações, pode-se compreender o aprimoramento das características arquiteturais (rede de acesso e núcleo) e o crescente emprego de soluções de *software* nas novas gerações.

Tabela 2.1: Evolução das gerações dos sistemas de redes móveis

	1G	**2G**	**3G**	**4G**
Implementação	≈ 1984	≈ 1991	≈ 1999	≈ 2009
Serviços	Voz analógica	Voz digital SMS	Pacotes de dados de alta capacidade	Comunicação IP
Taxa de dados	1.9 kbps	14.4 kbps	384 kbps	200 Mbps
Multiplexação	FDMA	TDMA, CDMA	TDMA, CDMA	OFDMA, SC-FDMA
Rede de acesso	AMPS	GSM, PDC, IS-95, IS-136, EDGE, GPRS	CDMA 2000, UMTS, TD-SCDMA,WCDMA	LTE, WiMAX
Núcleo da rede	PSTN	PSTN - SS	PSTN - SS, rede de pacotes	EPC
3GPP	-	-	Lançamento 1999	Lançamento 8

Observando a Tabela 2.1, pode-se constatar que cada geração ofereceu um conjunto relevante de novas tecnologias que modificaram a oferta de serviços pela rede móvel. A Primeira geração de rede móvel celular (1G) se caracterizou por oferecer serviço de comunicação de voz analógica, estendendo a rede telefônica comutada. A Segunda geração de rede móvel celular (2G) introduziu suporte a modulações digitais, apesar de ainda continuar baseada na transmissão de dados com comutação por circuitos em sua primeira versão. A Terceira geração de rede móvel celular (3G) proporcionou taxas de dados ainda maiores que a geração anterior, com melhor qualidade de serviço - *Quality of Service* (QoS) e cobertura de sinal, além de consolidar o suporte à comunicação sem fio com altas taxas de transmissão para serviços multimídia (i.e., dados, voz e vídeo). A 4G surgiu de dois padrões distintos: o LTE, desenvolvido pelo 3GPP, e o IEEE 802.16, desenvolvido por um grupo de trabalho do *Institute of Electrical and Electronics Engineers* (IEEE), e tem como principais características:

- Ser integralmente baseado em comutação por pacotes *Internet Protocol* (IP);

- Suportar taxas de dados de pico de até aproximadamente 100 Megabits por segundo (Mbps), para acesso móvel de alta mobilidade, e 1 Gbps, para acesso móvel de baixa mobilidade;
- Incrementar a capacidade de atendimento de usuários por célula com uso de recursos de rede compartilhados;
- Suportar a conexão simultânea a duas ou mais células durante uma conexão para oferecer transição suave (*smooth handover*) em redes heterogêneas;
- Suportar aplicações multimídia de próxima geração de alta qualidade.

Ao analisar a evolução das redes móveis celulares, constata-se que a evolução de cada uma das gerações sempre buscou atingir um rádio onipresente de alta capacidade, com níveis cada vez mais baixos de latência e maior capacidade de transmissão. A transição da 4G para a 5G adiciona a essa evolução a abertura de um caminho para tecnologias de IoT e comunicação inteligentes, explorando novas formas de conectividade tais como V2I, V2V e *Device-to-Device* (D2D). A seção a seguir apresenta mais detalhes sobre arquitetura 5G disponibilizada no lançamento 15 [3GPP TR-21.915 2018-12], dando ênfase em características que podem atuar como elementos habilitadores para a convergência de tecnologias de comunicação não 3GPP e o núcleo 5G.

Arquitetura 5G - lançamento 15 do 3GPP

A 5G é a geração mais dinâmica e flexível das redes celulares já projetada, fazendo uso extensivo de aplicativos e núcleo nativos em nuvem. A arquitetura 5G tem o potencial de ser moldada durante seu desenvolvimento, a fim de absorver novos saltos evolutivos dentro do mesmo padrão. Essa característica visa acompanhar a evolução exponencial de tecnologias-chave, como Inteligência Artificial (IA) e automação. Para atingir essa maturidade, a arquitetura 5G foi projetada para fazer amplo uso da virtualização de serviços e microsserviços.

A arquitetura 5G foi oficialmente apresentada no lançamento 15 [3GPP TR-21.915 2018-12], que foi dividido em duas fases. A primeira fase, introduzida em meados de 2017, é uma arquitetura de transição da 4G para 5G, intitulada como arquitetura *Non-Stand Alone* (NSA) [Both et al. 2020]. A arquitetura NSA tem como objetivo prover, de forma rápida, conectividade de alta vazão de dados, aproveitando os ativos de rede existentes da geração LTE, sem a necessidade de implantar um novo sistema completo de ponta a ponta para a rede 5G. A segunda fase, executada em 2018, apresenta a arquitetura *Stand-Alone* (SA), considerada a arquitetura 5G definitiva, incluindo melhorias na transmissão de rádio juntamente com o núcleo 5G nativo em nuvem.

Na arquitetura SA, o núcleo *Evolved Packet Core* (EPC) da geração LTE é substituído por um núcleo *Service-Based Architecture* (SBA), permitindo a utilização de um conjunto de funções de rede virtualizadas que fornecem serviços para outras funções da arquitetura ou, até mesmo, para aplicações de usuários finais. Essa característica consolida o conceito de dissociação entre os planos de dados e controle, permitindo o posicionamento flexível e sem estado de funções virtuais nos diferentes segmentos de rede que compõem um sistema 5G.

Dentro do escopo das redes móveis, o núcleo é o elemento de maior criticidade em um sistema 5G. A arquitetura SA da 2ª fase do lançamento 15 [3GPP TR-21.915 2018-12] estruturou o núcleo com base em um conjunto de componentes interconectados por uma camada de serviços. Cada componente possui uma responsabilidade específica, além de consumir e fornecer serviços para os demais elementos do sistema 5G por meio de *Application Programming Interface*s (APIs) definidas pelo padrão. Essa estrutura, formada por componentes de software e suas interconexões via APIs, é ilustrada na Figura 2.2. O lançamento 15 [3GPP TR-21.915 2018-12] introduziu mudanças substanciais na maneira como as redes móveis são projetadas, com o objetivo de fornecer suporte a uma ampla gama de serviços e aplicações, cada um deles com requisitos de desempenho distintos [Foukas et al. 2017]. Dada a relevância do núcleo 5G, cada um dos elementos que o compõem necessita ser robusto, resiliente, ter alta disponibilidade e escalabilidade. Essas são características normalmente associadas ao conceito de computação em nuvem. Por esse motivo, no lançamento 15, cada um dos elementos que compõem o novo núcleo 5G foi decomposto em *Virtual Network Function*s (VNFs), que podem estar disponíveis sob demanda em uma infraestrutura na nuvem, oferecendo um ou mais serviços para outras VNFs por meio de *Representational State Transfer* (REST), trafegando sobre *HyperText Transfer Protocol* (HTTP).

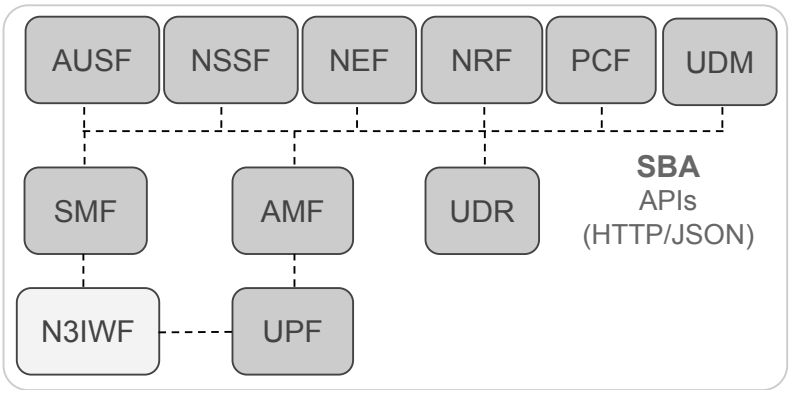

Figura 2.2: Principais componentes de software do núcleo 5G apresentados no lançamento 15, destacando a função de rede responsável por gerenciar conexões oriundas de redes *non-3GPP*.

Os componentes que constituem o núcleo 5G, ilustrados na Figura 2.2, podem ser vistos como uma malha interconectada de serviços. Cada VNF de um componente desempenha responsabilidades específicas e se interconecta a outras VNFs, produzindo e consumindo serviços. Considerando o contexto de convergência de tecnologias de comunicação não 3GPP e o núcleo 5G, tema principal deste trabalho, destaca-se, no lançamento 15, a função de rede N3IWF. A seguir, são descritas brevemente as principais características de cada uma das funções de rede, com ênfase especial na N3IWF.

Access and Mobility Management Function (AMF)

O gerenciamento de mobilidade é iniciado no momento em que uma nova conexão é estabelecida entre um UE e o núcleo da rede. Esse processo desencadeia uma série de procedimentos críticos destinados a identificar o UE e a fornecer uma estrutura de segurança robusta. A principal função dessa estrutura é criar um canal seguro para o transporte de mensagens. A entidade responsável por esse gerenciamento é a função de gerenciamento de acesso e mobilidade AMF.

A AMF desempenha um papel crucial ao assegurar que o processo de comunicação seja realizado de forma coesa e transparente, levando em consideração a mobilidade do usuário como um fator chave. Esse gerenciamento eficaz é essencial para manter a continuidade da comunicação, especialmente quando o UE se desloca entre diferentes áreas de cobertura.

Entre os diversos procedimentos implementados na AMF, destaca-se a capacidade da rede de localizar um determinado usuário para notificá-lo sobre mensagens ou chamadas recebidas. Esse processo envolve a coordenação entre múltiplos componentes da rede para garantir que o usuário possa ser alcançado independentemente de sua localização atual. A AMF, portanto, não só facilita a comunicação contínua, mas melhora a experiência do usuário ao garantir que as notificações importantes sejam entregues prontamente, mesmo em um ambiente de mobilidade elevada [Rommer et al. 2019, Toskala e Poikselkä 2020].

Session Management Function (SMF)

As principais responsabilidades da função de gerenciamento de sessão SMF envolvem atividades essenciais para a operação da rede, como estabelecer, modificar e liberar as sessões individuais dos UEs. Além disso, a SMF é responsável por alocar endereços IP para cada UE conectado, garantindo que cada dispositivo tenha uma identificação única e funcional na rede. A comunicação entre os UEs e a SMF ocorre de forma indireta, mediada pela AMF. É responsabilidade da AMF encaminhar as mensagens associadas à sessão

de um determinado UE à SMF correspondente, que gerencia a sessão. Essa intermediação é crucial para manter a integridade e a eficiência das comunicações na rede.

Os microsserviços da SMF interagem com outras VNFs em diversos contextos. Em particular, a SMF tem a responsabilidade de controlar diferentes funções associadas à *User Plane Function* (UPF). Esse controle inclui a capacidade da SMF de configurar a direção do tráfego de dados associado a um UPF para uma determinada sessão do UE. Além disso, a SMF executa ações de monitoramento e controle, garantindo que o tráfego de dados seja gerido de forma eficiente e que a qualidade do serviço seja mantida.

A interação entre a SMF e a UPF é vital para a manutenção da qualidade e do desempenho da rede. A SMF, ao configurar a direção do tráfego de dados, assegura que as necessidades de comunicação dos UEs sejam atendidas adequadamente, mesmo em cenários de alta demanda ou mobilidade. O monitoramento contínuo e o controle exercido pela SMF são fundamentais para detectar e mitigar quaisquer problemas que possam surgir, garantindo uma operação contínua e eficiente da rede [Rommer et al. 2019].

User Plane Function (UPF)

No contexto do lançamento 15, a UPF pode ser vista como uma parte fundamental do processo de separação entre o Plano de Controle e o Plano de Dados, que foi inicialmente introduzido no lançamento 14 [3GPP TS-133.185 2017-10]. Esse desacoplamento entre dados e controle permite que a arquitetura SBA descentralize ainda mais seus componentes. Por exemplo, atividades como o processamento de pacotes podem ser posicionadas mais próximas da borda da rede, o que pode melhorar a QoS para o usuário e reduz o tráfego na rede central.

Os funcionalidades implementadas na UPF são constantemente acionadas pela SMF. A principal função da UPF está associada ao encaminhamento e processamento de dados dos UEs. Além disso, a UPF é responsável por gerar notificações relacionadas ao tráfego de dados e realizar inspeção de pacotes. A UPF também atua como um ponto estável de ancoragem entre o núcleo da rede e redes externas, permitindo que a comunicação ocorra de forma transparente e ocultando a complexidade associada à mobilidade do usuário.

A separação de planos de dados e de controle gera uma arquitetura mais flexível e escalável, onde componentes críticos podem ser distribuídos conforme a necessidade. Pacotes IP destinados a um determinado UE são encaminhados da rede de dados para a UPF responsável por atender esse UE, garantindo a continuidade do serviço mesmo quando o usuário está em movimento. Isso não apenas melhora a eficiência da rede, mas também aprimora a experiência do usuário ao reduzir a latência e aumentar a velocidade de transmissão de dados.

Authentication Server Function (AUSF)

A AUSF desempenha um papel relevante na arquitetura de redes 5G, sendo responsável pela autenticação dos UEs através das credenciais de acesso fornecidas pela *Unified Data Management* (UDM). Além de prover microsserviços de autenticação, o AUSF oferece microsserviços de criptografia que garantem a segurança do tráfego de informações, possibilitando a execução segura de processos de atualização de informações de deslocamento (*roaming*) e outros parâmetros associados ao UE.

De maneira geral, os serviços microsserviços pelo AUSF são consumidos pela AMF. A AMF solicita recursos necessários para o processo de autenticação dos UEs, e essas solicitações são processadas internamente pela AUSF. Subsequentemente, a AUSF delega as tarefas aos serviços providos pelo UDM para a execução dos procedimentos de registro e manutenção no repositório de dados. Essa interação entre AUSF e UDM é fundamental para manter a integridade e a segurança da rede. A AUSF não só autentica os UEs, mas também implementa mecanismos robustos de criptografia que protegem as comunicações contra interceptações e outras ameaças. Esse processo integrado garante que todas as informações de autenticação e segurança sejam gerenciadas de forma eficiente e segura.

Unified Data Mangement (UDM)

A UDM é a VNF responsável por gerenciar os dados dos usuários da rede em um único elemento centralizado. Diversas VNFs da arquitetura SBA ilustrada na Figura 2.2, executam diferentes ações, tais como: registro e autenticação de UEs, identificação de usuários, aplicação de políticas de acesso e autorização, dentre outras. O componente UDM interage diretamente com o AMF que encaminha as solicitações dos demais componentes. Além disso, em cenários onde existem mais de uma instância de AMF, o UDM é responsável por controlar quais instâncias serão as responsáveis por atender um determinado UE [Toskala e Poikselkä 2020]. A UDM atua como *front-end* para os dados de assinatura do usuário que são armazenados na *Unified Data Repository* (UDR). A UDM usa esses dados de assinatura para executar a lógica de diversas aplicações, como autorização de acesso, gerenciamento de registro e acessibilidade para o encerramento de eventos [Both et al. 2020].

Policy Control Function (PCF)

A PCF é a VNF responsável por controlar o comportamento da rede, aplicando regras de segurança e controle, relacionadas ao gerenciamento das sessões, sobretudo àquelas funcionalidades associadas à mobilidade do usuário. Ele interage diretamente

com a AMF, visando prover uma política de acesso e de mobilidade que pode incluir dentre outras coisas, o gerenciamento de restrições de acesso a serviços de uma determinada área, bem como a gestão de questões associadas à prioridade de acesso ao meio de determinados UEs em detrimento a outros [Both et al. 2020].

Network Repository Function (NRF)

A NRF é o repositório onde todas as funções disponíveis para uma determinada rede são listadas. O objetivo da NRF é permitir que outras VNFs consigam encontrar a função adequada para atender suas demandas de serviço. Neste sentido, cabe a NRF a responsabilidade de selecionar o componente provedor de serviços mais adequado mediante critérios de desempenho fornecidos. Desta forma, a NRF é atualizada sempre que uma nova instância de VNF for implantada ou modificada [Both et al. 2020].

Network Exposure Function (NEF)

A NEF é a VNF responsável por expor alguns eventos internos, relacionados a UEs e a arquitetura SBA. A exposição desses eventos visa atender a potenciais demandas de aplicações específicas e VNFs de outros componentes. O acesso ao núcleo 5G é restrito e controlado, a NEF é o micro-serviço através do qual artefatos de software externos podem ter acesso a informações do núcleo.

Non-3GPP InterWorking Function (N3IWF)

A N3IWF e a VNF projetada para facilitar a interconexão de redes não 3GPP com o núcleo 5G através de uma rede de acesso *não confiável*. Ela atua como um ponto de entrada para dispositivos que se conectam através de redes não 3GPP, permitindo que esses dispositivos acessem os serviços e recursos da rede 5G. A N3IWF realiza funções de controle e de plano de usuário, interagindo com a AMF e com a UPF, respectivamente. Os microsserviços contidos na N3IWF pavimentam um canal de comunicação eficiente e seguro com o núcleo 5G, que pode ser percorrido através de diferentes tecnologias de comunicação sem fio não 3GPP o que a torna um elemento bastante relevante no contexto da convergência, investigado por este trabalho.

Além de habilitar a conectividade, a N3IWF atua na segurança das comunicações entre redes não 3GPP e o núcleo 5G. Ela utiliza túneis IPSec para garantir a integridade e a confidencialidade dos dados transmitidos entre os dispositivos e a rede 5G, empregando criptografia para proteger contra acessos não autorizados. A N3IWF não apenas habilita a integração de diferentes tecnologias de comunicação sem fio, mas também assegura

que essa integração ocorra de maneira segura e confiável, possibilitando o suporte a uma ampla gama de aplicações e serviços.

2.4 Lançamentos 16 e posteriores - Ampliando caminhos para convergência

O lançamento 16 do 3GPP [TR-21.916 2024] trouxe avanços em relação ao lançamento 15 [3GPP TR-21.915 2018-12], expandindo as capacidades e a flexibilidade das redes 5G. Uma das principais evoluções foi a introdução de funcionalidades avançadas para suportar comunicações URLLC, voltadas para aplicações críticas como controle industrial, telemedicina e veículos autônomos. Além disso, o lançamento 16 aprimorou a eficiência espectral e a capacidade de suporte para IoT, permitindo a conexão de um número maior de dispositivos com maior eficiência energética. O lançamento 16 também incluiu melhorias em redes não públicas, possibilitando que empresas e indústrias criem suas próprias redes 5G privadas, com segurança e desempenho otimizados.

Outro avanço apresentado no lançamento 16 foi a integração de serviços de posicionamento aprimorados, relevantes para aplicações que requerem localização precisa, como logística, transporte e serviços de emergência. Além disso, o lançamento 16 introduziu avanços em computação de borda, permitindo que o processamento de dados ocorra mais próximo do local onde eles são gerados, reduzindo a latência e melhorando o desempenho de aplicativos em tempo real [Penttinen 2021]. Essas melhorias complementam as capacidades do lançamento 15, que focou na implementação inicial da arquitetura 5G e na integração com redes LTE existentes, estabelecendo a base para uma conectividade robusta e de alta velocidade.

No que diz respeito à coexistência com tecnologias de comunicação sem fio não 3GPP, o lançamento 16 [TR-21.916 2024] introduziu melhorias consideráveis na arquitetura SBA. As funções *Trusted Non-3GPP Gateway Function* (TNGF) e *Trusted WLAN Interworking Function* (TWIF), apresentadas no lançamento 16, complementam e expandem as funcionalidades da N3IWF, introduzida no lançamento 15. A TNGF e a TWIF foram projetadas para facilitar a integração segura de redes não 3GPP com o núcleo 5G, com o objetivo de melhorar a interoperabilidade e a segurança. A TNGF serve como um ponto de interconexão seguro entre redes não 3GPP *confiáveis* e o núcleo 5G, garantindo que apenas dispositivos autorizados possam acessar os serviços da rede 5G. A TWIF, por sua vez, tem como foco específico a integração de redes WLAN *confiáveis*, utilizando IPSec como base para tunelamento seguro nas operações de autenticação e autorização. Conceitualmente, TNGF e TWIF complementam as funcionalidades da N3IWF ao fornecer opções adicionais e mais especializadas para conectar redes não 3GPP

ao núcleo 5G. No lançamento 15, a N3IWF estabeleceu a base para a integração de redes não 3GPP com a arquitetura 5G; a introdução da TNGF e da TWIF no lançamento 16 amplia a flexibilidade e a segurança, habilitando uma transição mais suave e eficiente entre diferentes tipos de redes. Essas melhorias são relevantes para ampliar o suporte a novas aplicações e serviços avançados que demandam conectividade contínua, alta segurança e baixa latência [Penttinen 2021].

Com base nos recentes lançamentos das especificações técnicas 3GPP [3GPP TR-21.915 2018-12, 3GPP TR-23.501 2021-12-23, 3GPP TS-23.502 2024-03], a Figura 2.3 ilustra os possíveis caminhos através dos quais as tecnologias de comunicação sem fio não 3GPP podem acessar o núcleo 5G, viabilizando um cenário no qual redes de acesso, controladas ou não controladas pelo 3GPP, com ou sem fio, serão partes integrais de um único ecossistema *superconvergente*. Esse cenário de *superconvergência* é um dos princípios de projeto para redes 6G [Tataria et al. 2021], e as funções TNGF, TWIF e N3IWF possuem mecanismos para viabilizar essa integração. Considerando um contexto de *convergência*, aspectos relacionados à segurança e autenticação são críticos. Nesse sentido, o núcleo 3GPP se apresenta como uma escolha natural para um caminho inicial de convergência, devido ao fato de o próprio núcleo 5G já possuir componentes previstos para uma integração inicial e a possibilidade de sua extensão para um núcleo 6G *superconvergente*. Além disso, o núcleo de redes 3GPP é tradicionalmente projetado seguindo boas práticas no que diz respeito aos aspectos de segurança e autenticação, sendo, portanto, uma opção adequada para a integração das redes de acesso 3GPP e não 3GPP. Usar um núcleo 3GPP para integração traz a vantagem de ter disponíveis outras tecnologias que vêm sendo integradas às redes 5G e posteriores, tais como fatiamento de rede, computação de borda e IA.

De acordo com a arquitetura de referência do Sistema 5G (5GS) [ETSI TS-123.501 2018-09], a integração de redes de acesso não 3GPP com o núcleo pode ocorrer de três formas: *confiável*, *não-confiável* ou com fio (redes cabeadas). A principal diferença entre o acesso *confiável* e o *não-confiável* está no tipo de relação que existe entre o ponto de acesso sem fio não 3GPP e o núcleo 3GPP. No acesso *confiável*, o ponto de acesso sem fio pode garantir que a comunicação com o UE ocorre de acordo com os padrões 3GPP para segurança e autenticação. Em outras palavras, o operador da infraestrutura tem controle total sobre o *Trusted Non-3GPP Access Point* (TNAP) / *Trusted WLAN Access Point* (TWAP) e o acesso ao enlace de rádio; portanto, a criptografia é controlada pelo operador ou há confiança na segurança oferecida pela rede de acesso não 3GPP. Assim, o UE pode realizar a sinalização de controle com o núcleo 5G de maneira similar ao que faria em um acesso 3GPP, sem necessidade de procedimentos adicionais de criptografia para garantir a segurança. No acesso *confiável*, os possíveis caminhos para convergência com o núcleo 5G envolvem as funções TNGF e TWIF,

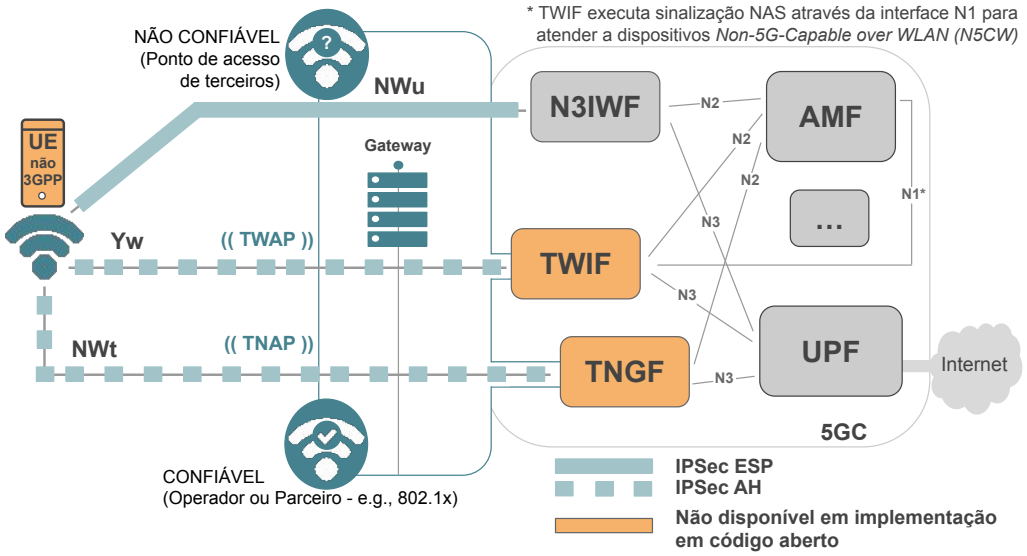

Figura 2.3: Diferentes caminhos de acesso de tecnologias de comunicação sem fio não-3GPP ao núcleo 5G através de N3IWF, TNGF e TWIF.

conforme ilustrado na Figura 2.3. Nativamente, apenas o acesso não 3GPP *confiável* oferece suporte a dispositivos que não são capazes de fazer sinalização *Non-Access Stratum* (NAS) com o núcleo 3GPP, chamados de dispositivos *Non-5G Capable over WLAN* (N5CW). Nesses cenários, o caminho para convergência com o núcleo 5G é através da função TWIF, que se encarrega de realizar a sinalização NAS com a AMF, em nome do dispositivo N5CW, através da interface N1, como ilustrado na Figura 2.3. Os túneis para o tráfego de dados construídos através do acesso provido pelas funções TNGF e TWIF são estruturados com base em IPSec *Authentication Header* (AH). Como em ambos os casos o acesso é *confiável*, os dados não são criptografados, mas são assinados digitalmente através do protocolo AH, para garantir que não foram alterados durante a transmissão e que a origem dos dados é autêntica. Em outras palavras, não é necessário utilizar procedimentos adicionais de criptografia, visto que o operador da infraestrutura controla o TNAP / TWAP e o enlace de rádio.

No acesso não 3GPP *não confiável*, não se sabe se o ponto de acesso sem fio pode garantir que a comunicação com o UE ocorra de acordo com os padrões 3GPP para segurança e autenticação; por isso, é declarado *não confiável*. Portanto, o UE deve criar um canal seguro diretamente com o núcleo 3GPP e, apenas sobre esse canal, realizar sua sinalização de controle. Conforme ilustrado na Figura 2.3, o caminho para convergência com o núcleo 5G, considerando o acesso *não confiável*, se dá através da N3IWF. Ela é responsável por permitir que UEs se conectem ao núcleo 5G através de redes de acesso não 3GPP. A N3IWF utiliza protocolos de tunelamento, como o IPSec *Encapsulating Security Payload* (ESP), para estabelecer túneis seguros para o plano de dados do usuário

e para a sinalização de controle entre o UE e o núcleo 5G. Isso garante que os dados sejam transmitidos de maneira segura, preservando a confidencialidade e a integridade das informações. A N3IWF também suporta mecanismos de autenticação e autorização para garantir que apenas dispositivos e usuários autorizados possam acessar os serviços do núcleo 5G. Isso é realizado através de protocolos padrão, como EAP. Além disso, ela colabora com outras funções de rede no núcleo, como a SMF, para gerenciar as sessões de dados, incluindo a configuração, modificação e liberação de conexões de dados conforme necessário. No contexto desta tese, a N3IWF representa um elemento facilitador para a convergência de redes heterogêneas, permitindo que UEs utilizem os recursos do núcleo 5G através de redes não 3GPP não controladas pelo operador da infraestrutura.

Considerando os possíveis caminhos para a convergência de tecnologias não 3GPP com o núcleo 5G, até o momento, não existe nenhuma implementação de código aberto das funções TNGF e TWIF. No que concerne à N3IWF, implementações de núcleo 5G, como o free5GC [free5GC 2022], disponibilizam desde sua versão 3.0 uma implementação funcional dessa função. Contudo, não há registros de implementação em código aberto de UE que seja capaz de realizar os procedimentos necessários para a construção dos túneis destinados ao tráfego de dados e à sinalização de controle por meio da N3IWF. Essa lacuna evidencia um obstáculo significativo para o avanço e a adoção de soluções 5G que podem tirar proveito do acesso não 3GPP, limitando o potencial de experimentação e desenvolvimento em ambientes de pesquisa e inovação abertos.

Ao concluir este capítulo, foi possível explorar detalhadamente os aspectos técnicos e conceituais que fundamentam a proposta de integração de tecnologias de comunicação sem fio não 3GPP com o núcleo 5G. Discutimos as especificações e os padrões que sustentam essa convergência, destacando os principais componentes e funções de rede que permitem essa integração, com especial atenção às evoluções trazidas pelos recentes lançamentos do 3GPP. Essa análise não apenas reforça a importância de uma arquitetura flexível para suportar a crescente demanda por conectividade em cenários diversos, mas também evidencia os desafios e as oportunidades associados a essa convergência tecnológica. O próximo capítulo se dedicará a examinar os trabalhos relacionados que abordam essa temática. No capítulo 4, é apresentada uma proposta de arquitetura *convergente* para a integração de tecnologias não 3GPP e o núcleo 5G. No capítulo 5, é exibido um protótipo funcional desta arquitetura, com a implementação do primeiro UE não 3GPP apto a prover conectividade ao núcleo 5G através de N3IWF.

CAPÍTULO 3

Trabalhos relacionados

Este capítulo apresenta uma visão geral dos trabalhos da literatura que exploram a convergência de tecnologias de comunicação sem fio não 3GPP com o núcleo 5G. A convergência representa um avanço significativo na forma como diferentes tecnologias de comunicação sem fio se integram para oferecer uma infraestrutura de comunicação coesa, eficiente e flexível. Estudos anteriores têm investigado diversos aspectos dessa integração [Yasmin et al. 2017, Navarro-Ortiz et al. 2018, Mikhaylov et al. 2018, Torroglosa-Garcia et al. 2020, Aijaz 2020, Zhang et al. 2020, Kunz et al. 2020, Mendes et al. 2020, Roseti 2021, Cogalan et al. 2022, Lagen et al. 2020, Luglio et al. 2022, Lemes et al. 2022, Yadav et al. 2023, Chinchilla-Romero et al. 2023, Chen et al. 2024], desde as funcionalidades e arquiteturas de rede necessárias até os protocolos e mecanismos que garantem interoperabilidade e desempenho aprimorado. O capítulo está estruturado em três subseções que agrupam os trabalhos relacionados ao tema da convergência entre tecnologias 3GPP e não 3GPP. A primeira subseção explora as diversas abordagens de convergência entre essas tecnologias, destacando os métodos e arquiteturas propostas para unificar essas redes. Em seguida, a segunda subseção discute os procedimentos de integração específicos para tecnologias não 3GPP no contexto do 5G, abordando as metodologias e padrões empregados para garantir uma interoperabilidade eficiente. Por fim, a terceira subseção foca nas aplicações práticas e nos desafios enfrentados na integração de redes não 3GPP com o núcleo 5G, analisando os problemas encontrados e as soluções propostas na literatura. Ao revisar esses trabalhos, este capítulo fornece uma base sólida para entender as abordagens, desafios e soluções propostas na literatura, destacando a importância e o impacto da convergência de redes no ecossistema 5G.

3.1 Abordagens de convergência entre tecnologias 3GPP e não 3GPP

Em [Yasmin et al. 2017], os autores investigam a integração de LoRaWAN com uma rede de testes 5G. O foco principal do trabalho é explorar como as redes *Low Power Wide Area Networks* (LPWAN), especificamente LoRaWAN, podem ser integradas com a infraestrutura do 5G para oferecer suporte eficiente a aplicações IoT. No trabalho, os autores discutem quatro métodos de integração de LoRaWAN com 5G: (*i*) através da rede de acesso 3GPP, (*ii*) através de uma rede de acesso não confiável não 3GPP, (*iii*) como parte do *eNodeB*, e (*iv*) virtualmente, como parte da rede central. A implementação prática do método de integração demonstra a viabilidade técnica e oferece uma referência para futuros estudos e aplicações. No entanto, a integração apresenta complexidade elevada, especialmente nos métodos que envolvem a fusão com o eNodeB ou a virtualização na rede central. Outro aspecto a ser observado é que, mesmo sendo fortemente baseada no conceito de *softwarização* [Both et al. 2020], algumas opções de integração podem sofrer limitações de desempenho, devido a gargalos de capacidade ou requisitos específicos de hardware e software. A escalabilidade pode ser uma preocupação, particularmente na integração virtual na rede central, que apresenta desafios em termos de capacidade e gerenciamento de recursos.

Em [Navarro-Ortiz et al. 2018], os autores propõem uma solução para a integração de LoRaWAN com redes móveis 4G/5G. A proposta permite que operadores de redes móveis reutilizem suas infraestruturas existentes, modificando apenas o *gateway* LoRaWAN para atuar como um *eNodeB*, facilitando a integração transparente para os dispositivos finais e para o núcleo EPC. O *gateway* modificado implementa parte do protocolo *eNB*, assegurando que todos os pacotes de dados transportados pela rede principal sejam criptografados e protegidos por integridade, garantindo segurança de ponta a ponta. Os autores demonstram a viabilidade da solução através de um conceito validado com um EPC de código aberto, que demonstra a capacidade de reutilizar infraestruturas existentes. No entanto, a complexidade de modificar os *gateways* LoRaWAN e a necessidade de garantir a compatibilidade contínua com evoluções futuras das redes 4G/5G são pontos críticos a serem considerados.

Em [Mikhaylov et al. 2018], os autores também exploram a integração entre LoRaWAN e redes móveis 4G/5G, propondo uma solução que permite que os operadores de redes móveis reutilizem suas infraestruturas existentes com baixo custo de investimento. A proposta apresentada pelos autores é transparente para os dispositivos finais LoRaWAN e para o núcleo da rede EPC. De acordo com os autores, apenas o *gateway* LoRaWAN precisa ser modificado, passando a atuar como um *eNB* da perspectiva da rede EPC. A solução proposta implementa a sinalização LTE necessária para o estabe-

lecimento dos procedimentos de vínculo do UE, garantindo segurança de ponta a ponta para os pacotes de dados transportados, mantendo tanto a integridade quanto a confidencialidade dos dados. Embora a proposta se destaque pelo fato de reutilizar a infraestrutura existente, a necessidade de modificar os *gateways* LoRaWAN pode ser vista como uma limitação, além da dependência de um EPC compatível. Além disso, o trabalho menciona a utilização de projetos financiados pelo programa H2020 e outros projetos de pesquisa que frequentemente promovem a disseminação de softwares *open-source*, não está claro se todos os componentes da solução, desde o hardware até o software e as especificações de integração, estão disponíveis sob licença *open-source*.

Em [Lagen et al. 2020], os autores abordam a evolução das tecnologias não 3GPP (Wi-Fi) 3GPP (LTE e *New Radio* (NR)) no contexto do espectro não licenciado, destacando como a competição entre essas tecnologias levou à convergência de suas características de acesso ao espectro. Os autores argumentam que historicamente, o Wi-Fi dominou o uso do espectro não licenciado, mas com a expansão das tecnologias celulares para essas bandas, iniciou-se uma competição que resultou em ambas as tecnologias adotarem características semelhantes, como a capacidade de utilizar bandas de frequência com grandes larguras de banda para transmitir dados. No artigo, os autores discutem as opções futuras para a convergência dessas tecnologias, incluindo a interconexão entre redes celulares e Wi-Fi, e avaliam, por meio de simulações, a coexistência de *New Radio Unlicensed* (NR-U) e Wi-Fi na banda de 60 GHz. Os resultados sugerem que, embora a competição tenha gerado benefícios na eficiência do uso do espectro, a verdadeira convergência no nível de rede de acesso pode trazer ainda mais vantagens para os usuários. No entanto, os autores não oferecem uma solução prática ou diretrizes para implementação que abordem os desafios de integrar redes não confiáveis ao núcleo 5G.

Os autores [Yadav et al. 2023] apresentam uma arquitetura projetada para a convergência entre redes de transmissão não 3GPP e redes 5G, visando atender às crescentes demandas por serviços multimídia em redes móveis. No trabalho, os autores apresentam uma arquitetura baseada em serviço de sinalização, que tem como foco principal, atuar na troca de sinalização entre o UE e a rede como um dado ou serviço, aumentando assim a escalabilidade e a modularidade da rede. A avaliação de desempenho da arquitetura é realizada por meio de simulações baseadas em álgebra de processos. De acordo com os autores, os resultados demonstram uma redução no número de mensagens de sinalização necessárias para o estabelecimento de sessões, em comparação com a arquitetura 3GPP 5G convencional. Embora os resultados apresentados sejam promissores, em termos de escalabilidade quando comparados com a arquitetura SBA proposta pelo 3GPP, os autores não exploram de maneira detalhada os desafios específicos associados ao acesso através de redes não confiáveis. Isso inclui aspectos como segurança, latência, e a complexidade adicional de gerenciar conexões através de redes não confiáveis, que são cruciais para a

integração de redes não 3GPP com o núcleo 5G. Embora os autores apresentem simulações e avaliações teóricas da arquitetura proposta, não há menção de uma implementação prática ou validação experimental em ambientes reais, especialmente para cenários envolvendo a N3IWF.

Em [Torroglosa-Garcia et al. 2020], os autores investigam a integração de LoRaWAN com a rede 5G, visando habilitar *roaming* em redes IoT heterogêneas. O objetivo é abordar as limitações de interoperabilidade e confiança entre diferentes redes LPWAN e propor um mecanismo de *handover roaming* que utilize a infraestrutura confiável da rede 5G para autenticação e gerenciamento de chaves. O trabalho propõe duas abordagens de integração: uma utilizando a conectividade do espectro 5G com autenticação padrão e outra realizando a autenticação 5G através da rede LoRaWAN. A validação prática das abordagens em um ambiente de testes integrado 5G-LoRaWAN demonstrou a viabilidade e segurança da solução. No trabalho, destacam-se a interoperabilidade avançada, a escalabilidade global e a segurança aprimorada. Entretanto, a complexidade de implementação, a dependência de cobertura dupla e os custos potenciais envolvidos são pontos críticos a serem considerados.

3.2 Procedimentos de integração para tecnologias não 3GPP no contexto do 5G

Esta subseção apresenta trabalhos que abordam os procedimentos necessários para a integração de tecnologias não 3GPP com o núcleo 5G, destacando as metodologias utilizadas para assegurar a comunicação entre essas redes. Em [Kunz et al. 2020], os autores discutem as tecnologias de acesso não 3GPP e sua integração com o núcleo 5G, detalhando os protocolos e procedimentos necessários para garantir a segurança nesses cenários. O texto abrange o acesso não confiável e confiável, enfatizando o uso de tunelamento IPSec para proteger as comunicações em ambientes não confiáveis. O artigo explora a evolução das especificações do 3GPP, incluindo uma descrição detalhada de EAP-5G, um novo método de transporte para mensagens NAS, e as melhorias introduzidas na lançamento 16, que permitem o acesso confiável e suportam dispositivos N5CW. Os autores focam principalmente na descrição teórica dos protocolos e procedimentos, mas não fornecem exemplos práticos ou estudos de caso que demonstrem a aplicação real dessas tecnologias. Isso pode limitar a compreensão da implementação prática e dos desafios que podem surgir em diferentes contextos. Também não há uma análise detalhada do desempenho dos procedimentos de segurança descritos, como o impacto na latência ou na eficiência do tráfego de dados quando utilizando a N3IWF. A falta de dados quantitativos ou métricas de desempenho pode ser uma limitação para pesquisadores que desejam

avaliar a viabilidade dessas soluções em suas próprias implementações.

Em [Roseti 2021] os autores exploram a integração de interfaces de satélite não 3GPP em redes 5G, destacando as oportunidades e desafios na criação de uma arquitetura híbrida que combina acesso terrestre e satelital. O estudo busca desenvolver mecanismos avançados para melhorar o desempenho e a confiabilidade das comunicações, utilizando técnicas como o *Access Traffic Steering, Switching, and Splitting* (ATSSS). Os autores também discutem a adaptação de funcionalidades da rede 5G para suportar acessos simultâneos ou alternados através de redes não 3GPP, especialmente em cenários onde a latência e a cobertura do satélite diferem significativamente das redes terrestres. Essa integração visa expandir o uso de serviços 5G para áreas com pouca infraestrutura terrestre, aproveitando as características únicas das comunicações por satélite. Embora o artigo apresente um estudo robusto sobre a integração, com discussões teóricas e propostas de arquitetura, faltam detalhes sobre implementações práticas ou resultados experimentais concretos que demonstrem a viabilidade e o desempenho da integração proposta. A ausência de uma prova de conceito tangível pode limitar a aplicabilidade prática das ideias discutidas pelos autores. O artigo também não menciona a disponibilização de artefatos de software ou ferramentas desenvolvidas durante a pesquisa. Isso significa que outros pesquisadores podem ter dificuldades em reproduzir ou validar os resultados apresentados.

Os autores [Zampognaro et al. 2024] exploram uma abordagem inovadora para integrar serviços de borda diretamente na função N3IWF em redes 5G. Tradicionalmente, o acesso não 3GPP através de N3IWF utiliza pontos de acesso não confiáveis (e.g, Wi-Fi) para se conectar ao núcleo 5G, e essa conexão é estabelecida de maneira segura através do protocolo IPSec. No artigo, os autores propõe que, ao invés de encaminhar todo o tráfego para o núcleo 5G, parte dele possa ser processada localmente pelo N3IWF, reduzindo a latência e aumentando a eficiência, especialmente em cenários onde a rede de retorno é limitada, como em conexões via satélite. Embora os resultados demonstram benefícios em termos de desempenho, como a redução de latência e a economia de recursos na rede, a abordagem está fora do escopo das especificações atuais do 3GPP. Isso significa que, embora a solução proposta possa ser tecnicamente viável, ela não segue os padrões estabelecidos, o que pode limitar sua adoção em ambientes que requerem conformidade estrita com as especificações 3GPP. Além disso, a implementação de serviços de borda diretamente na N3IWF pode adicionar complexidade ao sistema, especialmente em termos de gestão e manutenção, particularmente se considerarmos a necessidade de configurar e manter várias instâncias de N3IWF distribuídas, conforme apresentado no trabalho.

Em [Luglio et al. 2022] os autores abordam a integração de redes de satélite como método de acesso não confiável ao núcleo 5G, utilizando a N3IWF. No trabalho, os

autores exploram as implicações do uso de links de satélite, na comunicação com redes 5G, destacando o impacto significativo na latência devido às características inerentes das comunicações por satélite. O estudo inclui a implementação de um ambiente de teste em tempo real utilizando uma rede 5G compatível com o lançamento 15 do 3GPP, com emulação de comunicações via satélite para avaliar a latência, *overhead*, e outros aspectos de desempenho. Os resultados mostram que, embora o acesso via satélite incremente a latência, essa abordagem pode ampliar significativamente o alcance dos serviços 5G em áreas rurais e outras regiões com cobertura terrestre limitada, apesar de algumas limitações para aplicações sensíveis ao tempo. O artigo sugere, ainda, o futuro desenvolvimento de mecanismos confiáveis para acesso não 3GPP via satélite, visando mitigar as limitações identificadas. Embora o estudo tenha implementado e avaliado a arquitetura proposta em um ambiente de teste, a análise detalhada das implicações práticas, como segurança e resiliência do sistema, é relativamente limitada. A latência elevada introduzida pelo uso de links via satélite, embora esperada, é um fator crítico que não é abordado em profundidade em termos de mitigação de impactos em diferentes cenários de uso. Outro ponto a ser considerado é a ausência de uma discussão mais abrangente sobre como as variações nas condições de rede, especialmente em ambientes de satélite, podem afetar a qualidade do serviço e a continuidade da conexão. A aderência às especificações 3GPP é apresentada de maneira satisfatória, no entanto os autores poderiam explorar mais como as futuras versões das especificações poderiam melhorar o uso de N3IWF em cenários similares. Os autores utilizam o projeto free5GC [free5GC 2022] e o emulador OpenSand [OpenSAND 2022] para conduzir os experimentos, mas não indicam que tenham tornado disponíveis as modificações ou configurações específicas realizadas nesses sistemas. Isso pode limitar a capacidade de outros pesquisadores replicarem o estudo ou adaptarem a metodologia a outros contextos.

3.3 Aplicações e desafios na integração de redes não 3GPP com o núcleo 5G

Esta subseção foca nas aplicações práticas e nos desafios enfrentados na integração de redes não 3GPP com o núcleo 5G. Em [Zhang et al. 2020], os autores investigam a integração de múltiplas redes LoRaWAN com o núcleo EPC de redes 4G/LTE, com o objetivo de expandir a interoperabilidade e a integração, considerando um cenário *multi-vendor* em redes de operadores móveis, com produtos de diferentes fabricantes e fornecedores. No trabalho, os autores apresentam uma proposta que inclui a implementação de *gateways* LoRa que atuam como *eNodeB's* virtuais, possibilitando o encaminhamento de pacotes LoRa através do núcleo EPC para servidores de aplicação. Eles abordam pro-

blemas de roteamento e agendamento de pacotes para otimizar a integração de múltiplos *gateways* LoRa, garantindo que possam operar conjuntamente em regiões geográficas distribuídas. A viabilidade da solução foi demonstrada por meio de simulações numéricas, mostrando que a solução pode reduzir significativamente o atraso médio dos pacotes. No entanto, a complexidade da implementação, especialmente na configuração e manutenção dos *gateways* LoRa, e a necessidade de garantir compatibilidade contínua com futuros avanços nas redes móveis 4G e 5G são pontos relevantes a serem considerados.

Em [Chen et al. 2024], os autores propõem a integração *Multiple Radio Access Technology* (MRAT), envolvendo uma rede LoRa de baixa potência e longa distância com a infraestrutura 5G, para monitoramento inteligente de condições meteorológicas ao longo das vias ferroviárias. O objetivo do trabalho é solucionar a limitação de cobertura das redes celulares tradicionais, utilizando a rede 5G para *backhaul* e processamento em nuvem, enquanto a rede LoRa estende a cobertura de forma econômica. A arquitetura inclui um servidor LoRa operando em uma nuvem privada da rede 5G para gerenciar a rede LoRa e integrar computação de borda, resultando em uma arquitetura colaborativa entre nuvem, borda e terminal. Embora a proposta de uma arquitetura colaborativa, envolvendo a integração de computação em nuvem, borda e terminal, tenha potencial para otimizar o processamento de dados e a eficiência da rede, a integração de várias tecnologias pode aumentar a dificuldade de implantação e manutenção da infraestrutura.

[Mendes et al. 2020] aborda a importância de desenvolver redes de comunicação móvel para áreas remotas e rurais, um cenário segundo os autores, negligenciado pelas normas atuais de redes móveis. No trabalho, os autores propõem a utilização de bandas de frequência não utilizadas, caracterizadas como *TV White Space* (TVWS) por meio de técnicas de rádio cognitivo, integrando essas redes ao núcleo 5G através da função N3IWF. Os autores descrevem a hipótese desse mecanismo, destacando a necessidade de um UE para interconectar 5G *longa distância* ao núcleo 5G através da N3IWF, garantindo flexibilidade e eficiência espectral, além de habilitar o suporte a casos de uso como conectividade de voz e dados, agricultura inteligente e monitoramento ambiental. Os pontos fortes do trabalho incluem a flexibilidade da camada física com modulação *Generalized Frequency Division Multiplexing* (GFDM), a eficiência espectral e a robustez contra canais seletivos em frequência. A abordagem cognitiva e a integração com o núcleo 5G são bem delineadas. No entanto, a implementação descrita com integração através de N3IWF é ainda rudimentar e considerada um protótipo. Aspectos associados à comunicação segura entre o núcleo 5G e as redes de acesso não 3GPP, utilizando IPSec, IKE e outras tecnologias de segurança, é um aspecto que necessita de maior exploração e aprimoramento. Melhorar a implementação desses elementos é essencial para validar a viabilidade técnica e prática da integração proposta e garantir a segurança e a eficiência na comunicação entre redes heterogêneas.

Os autores [Aijaz 2020] apresentam uma visão técnica abrangente sobre as redes privadas 5G e sua aplicação em ambientes industriais, destacando seu potencial para impulsionar a transformação digital impulsionada por iniciativas como a indústria 4.0. O artigo explora a arquitetura funcional dessas redes, ressaltando os benefícios de cobertura dedicada, capacidade e controle exclusivos, que permitem a personalização de serviços para casos de uso industrial. Além disso, o texto aborda as oportunidades de espectro para o 5G privado, os desafios de design, como o fatiamento de rede e a integração com redes sensíveis ao tempo, e discute o ecossistema emergente de inovação aberta que pode acelerar a adoção dessa tecnologia no setor industrial. Embora apresente uma análise técnica robusta, os autores não se aprofundam nos desafios específicos relacionados à segurança e à confiabilidade ao utilizar redes não confiáveis. Embora os autores mencionem a utilização da N3IWF para interconectar redes privadas e públicas, eles não oferecem uma análise detalhada dos desafios de segurança e de desempenho que podem surgir nessa configuração, nem exploram em profundidade como essas interconexões aderem estritamente às especificações 3GPP. Além disso, a ausência de exemplos práticos ou estudos de caso que demonstrem a utilização do N3IWF em cenários reais de redes não confiáveis, limita a compreensão dos leitores sobre as dificuldades práticas e as soluções potenciais para esses desafios.

Em [Lemes et al. 2022], os autores abordam de forma detalhada os mecanismos de acesso ao núcleo 5G através de redes não 3GPP, tanto em cenários confiáveis quanto não confiáveis. O trabalho explora a convergência dessas redes com a infraestrutura 5G, destacando aspectos como procedimentos de autenticação, autorização e estabelecimento de sessões de dados. O tutorial apresenta um experimento envolvendo o acesso não confiável usando redes Wi-Fi, demonstrando como um usuário é autenticado no núcleo 5G e como a conectividade é estabelecida. Além disso, o artigo analisa o desempenho desse acesso em termos de tempo consumido, número de mensagens trocadas e sobrecarga de protocolo. Embora essas discussões tenham relevância para entender os desafios e as oportunidades na integração de tecnologias emergentes em uma arquitetura de rede unificada e convergente, a implementação apresentada pelos autores possui algumas limitações significativas. A solução é bastante rudimentar, permitindo apenas a constatação básica da conectividade com o núcleo 5G através de uma rede de acesso não confiável. Reproduzir o experimento exige uma quantidade considerável de configurações, uma vez que o código é altamente acoplado e muitas configurações não estão parametrizadas. Além disso, não foi apresentado nenhum experimento que demonstrasse a estabilidade da conexão não 3GPP. A complexidade elevada da implementação, devido ao alto nível de acoplamento, significa que a reprodução do experimento em um ambiente diferente daquele utilizado no artigo demanda um trabalho árduo de programação, tornando o processo pouco prático e limitado em termos de aplicabilidade a outros cenários.

Em [Chinchilla-Romero et al. 2023] os autores abordam o uso de múltiplas tecnologias de acesso sem fio em redes privadas industriais 5G para atender aos requisitos variados de serviços emergentes da indústria 4.0, como o suporte a comunicações URLLC. Os autores destacam que, ao alavancar as capacidades de conectividade múltipla do sistema 5G, é possível integrar de forma eficiente essas tecnologias, otimizando a utilização da banda de espectro do 5G para serviços críticos e descarregando tráfego menos crítico para redes Wi-Fi através de N3IWF. De acordo com os autores, essa abordagem melhora a eficiência espectral e a capacidade da rede, reduzindo os custos operacionais e estendendo a vida útil das infraestruturas Wi-Fi existentes. Embora o artigo mencione a N3IWF ele não aborda detalhadamente os desafios e implicações de segurança associados ao uso de redes não confiáveis. O artigo também não explora em profundidade como as especificações 3GPP garantem a interoperabilidade e segurança ao utilizar multi-conectividade entre 5G NR e Wi-Fi.

[Cogalan et al. 2022] apresenta a arquitetura 5G-*CLARITY*, que tem como objetivo, integrar as tecnologias *5G New Radio* (5GNR), Wi-Fi e *Light Fidelity* (Li-Fi) para redes privadas e o núcleo 5G. De acordo com os autores, o sistema apresentado tem como objetivo atender às rigorosas demandas de setores industriais por alta disponibilidade, confiabilidade, segurança, baixa latência e alta precisão de posicionamento, relevantes para a indústria 4.0. No trabalho, os autores destacam três principais características do sistema: (*i*) um *framework* de multi-conectividade para acesso simultâneo e otimizado às redes 5GNR, Wi-Fi e Li-Fi; (*ii*) um servidor de posicionamento de alta precisão que combina sinais de diferentes tecnologias para fornecer precisão de centímetros; e (*iii*) um sistema de gerenciamento e orquestração que facilita o provisionamento de fatias de rede privada, garantindo isolamento de recursos e desempenho de serviços multi-locatários. De acordo com o artigo, o sistema foi avaliado através de simulações em nível de pacote e testes experimentais, demonstrando capacidade de gerenciar tráfego de redes de acesso e alcançar precisão de posicionamento de centímetros, além de provisionar fatias de rede em menos de um minuto. Entretanto, os autores não disponibilizam nenhum recurso de código utilizado nos experimentos para validação em pares. Um ponto fraco é a falta de clareza sobre a natureza *open-source* ou proprietária dos artefatos produzidos. Embora o uso de ferramentas como *OpenStack* e *Open Source MANO* sugira uma inclinação para o código aberto, nenhum registro de repositório em plataformas como *GitHub* foi encontrado. Neste contexto, não é possível comparar o desempenho com a solução proposta por este trabalho. O artigo é um dos resultados da proposta de arquitetura 5G-CLARITY [CLARITY 2022], que descreve a integração entre tecnologias de comunicação sem fio não 3GPP e o núcleo 5G através das funções N3IWF e TNGF. A leitura da especificação permite interpretar que no escopo do projeto um dos entregáveis seria um UE responsável por pavimentar a interconexão entre redes não 3GPP e núcleo 5G, no entanto, de forma

similar ao ocorrido na tentativa de localizar o código para replicação dos experimentos do artigo, novamente nenhum registro de repositório de acesso público foi encontrado.

Os principais trabalhos que tratam da integração de tecnologias de comunicação sem fio não 3GPP com o núcleo 5G apresentam distintas abordagens e metodologias diferentes visando alcançar a convergência. Cada trabalho foi avaliado com base no caminho utilizado para a acesso ao núcleo 5G (e.g., acesso *não confiável* não 3GPP). Além disso, foi analisada a complexidade de se reproduzir e/ou implantar os métodos de integração propostos, onde soluções menos complexas são preferíveis para facilitar a implementação e manutenção. A capacidade de escalabilidade das soluções, tanto vertical quanto horizontal, foi um critério crucial, especialmente considerando as características de computação em nuvem que permitem a adaptação às demandas crescentes de rede. A avaliação também levou em conta o quão voltadas ao uso de software são as soluções, priorizando aquelas que minimizam a necessidade de configuração manual, e possuem baixo acoplamento. Trabalhos que adotam uma metodologia de código aberto receberam uma avaliação positiva, pois esta abordagem facilita a adaptação e a flexibilidade do desenvolvimento. Um outro critério avaliado foi a capacidade das soluções aplicarem conceitos de observabilidade em redes não 3GPP, permitindo que o operador da infraestrutura tenha acesso em tempo real a métricas e parâmetros dessas redes. Soluções que oferecem uma visão abrangente dos indicadores de desempenho, como latência, perda de pacotes, variações na intensidade do sinal e taxa de transmissão, permitem uma melhor gestão da infraestrutura, promovendo uma operação mais eficiente e segura. Por fim, foi considerada a capacidade das soluções serem testadas e funcionarem em diferentes implementações de núcleo 5G de código aberto, garantindo a interoperabilidade e a aplicabilidade prática. Essas avaliações foram sintetizadas na Tabela 3.1 que resume os critérios e as pontuações de cada trabalho, proporcionando uma visão comparativa clara sobre a viabilidade das diversas abordagens de integração de tecnologias de comunicação sem fio não 3GPP com o núcleo 5G. Na Tabela 3.1, critérios rotulados com N/D indicam soluções com código *não disponível*, portanto qualquer característica não descrita na documentação do projeto/artigo é assumida como não implementada.

Tabela 3.1: Comparação da arquitetura convergente apresentada neste trabalho com outros trabalhos relevantes da literatura

Trabalho	*não 3GPP*	*Reprodutibilidade*	*Escalabilidade*	*Softwarização*	*Código aberto*	*Métricas não 3GPP*	*Multi-núcleo*
[Yasmin et al. 2017]	NÃO	MÉDIA	BAIXA	MÉDIA	N/D	NÃO	NÃO
[Navarro-Ortiz et al. 2018]	NÃO	MÉDIA	BAIXA	MÉDIA	SIM	NÃO	NÃO
[Mikhaylov et al. 2018]	NÃO	ALTA	MÉDIA	MÉDIA	N/D	NÃO	NÃO
[Torroglosa-Garcia et al. 2020]	NÃO	ALTA	MÉDIA	ALTA	N/D	NÃO	NÃO
[Zhang et al. 2020]	NÃO	MÉDIA	MÉDIA	MÉDIA	NÃO	NÃO	NÃO
[Chen et al. 2024]	NÃO	ALTA	MÉDIA	ALTA	NÃO	NÃO	NÃO
[Mendes et al. 2020]	SIM	ALTA	BAIXA	MÉDIA	N/D	NÃO	NÃO
[Lemes et al. 2022]	SIM	ALTA	BAIXA	ALTA	SIM	NÃO	NÃO
[Cogalan et al. 2022]	SIM	N/D	N/D	N/D	NÃO	NÃO	N/D
Este trabalho	SIM	BAIXA	ALTA	ALTA	SIM	SIM	PARCIAL

Convém destacar que a avaliação indicada como *PARCIAL* do UE não 3GPP, no quesito denominado *multi-núcleo*, deve-se ao fato de que, atualmente, a única implementação em código aberto de núcleo 5G que possui uma implementação funcional da N3IWF é o free5GC [free5GC 2022]. O experimento realizado para avaliar esse critério envolveu a integração da N3IWF do free5GC com as demais funções de núcleo do Open5GS [Open5GC 2019], na tentativa de executar os procedimentos de registro e autenticação com o UE não 3GPP no acesso não confiável. Durante o experimento, os procedimentos iniciais ocorreram conforme o esperado: (i) a N3IWF do free5GC registrou-se no Open5GS, (ii) recebeu a solicitação de registro do UE não 3GPP e (iii) iniciou os processos subsequentes de registro e autenticação, envolvendo os microsserviços das funções AMF, SMF e outras. No entanto, o AMF do Open5GS não foi capaz de completar os procedimentos necessários, pois este componente é projetado para tratar registros de UE em redes de acesso 3GPP, utilizando parâmetros como *Mobile Country Code* (MCC), *Mobile Network Code* (MNC) e informações da *Base Station* (BS) para controlar a localização e realizar a operação de *paging*. No caso de acessos não confiáveis via N3IWF, a operação de *paging* não é suportada. As especificações exigem que o AMF processe as requisições e realize o *paging* com base nos endereços IP da N3IWF, o que ainda não é suportado pelo Open5GS. Assim, a limitação na AMF do Open5GS impediu a conclusão do experimento, resultando na qualificação do UE não 3GPP como *PARCIAL* no quesito *multi-núcleo*, já que o suporte fim a fim não pôde ser plenamente demonstrado.

Conforme ilustrado na Tabela 3.1, a análise dos trabalhos relacionados evidencia

a necessidade de soluções que integrem tecnologias de comunicação sem fio não 3GPP ao núcleo 5G de forma eficiente, confiável, fáceis de serem implantadas e aderentes à *softwarização*, especialmente no que diz respeito às características de software voltadas para microsserviços e computação em nuvem. Este capítulo revisa diversas abordagens e metodologias propostas na literatura, avaliando a escalabilidade, aderência ao código aberto e a eficiência dessas soluções. A arquitetura desenvolvida nessa tese se destaca por apresentar a primeira solução de convergência, implementada por meio de um UE não 3GPP capaz de suportar conexões não confiáveis via N3IWF. Além disso, o UE não 3GPP disponibiliza um mecanismo que permite ao operador de infraestrutura de comunicação coletar métricas de redes de acesso não 3GPP e utilizar essas métricas para tomar decisões informadas sobre a gestão e otimização da infraestrutura de comunicação. A arquitetura convergente proposta nesta tese, também se caracteriza devido a facilidade de implantação e configuração, sendo uma solução totalmente baseada em software e de código aberto, disponível no GitHub. No próximo capítulo, são apresentados em detalhes os elementos que compõem esta arquitetura, proporcionando uma compreensão aprofundada de sua funcionalidade e dos benefícios que traz para o ecossistema 5G.

CAPÍTULO 4

Arquitetura convergente

Este capítulo apresenta uma análise detalhada da arquitetura convergente proposta por esta tese, que visa à integração de tecnologias de comunicação sem fio não 3GPP com o núcleo 5G. O capítulo inicia explorando os elementos fundamentais da arquitetura convergente, destacando como essas tecnologias podem ser integradas para criar uma infraestrutura robusta e versátil. A arquitetura convergente é ilustrada com diagramas que explicam as funções de rede envolvidas e as interfaces utilizadas para acesso não confiável ao núcleo 5G. São discutidos os principais desafios e soluções para garantir a segurança, autenticidade, e qualidade de serviço, essenciais para a comunicação segura entre o UE não 3GPP e o núcleo 5G. Além disso, são apresentados os procedimentos para registro, autenticação e autorização, bem como os mecanismos de estabelecimento e gerenciamento de sessões *Protocol Data Unit* (PDU), que são fundamentais para assegurar que o tráfego de dados seja conduzido de forma eficaz e segura. A análise inclui uma visão detalhada dos protocolos utilizados e das transições de estado que ocorrem durante o processo de comunicação, proporcionando uma compreensão robusta dos aspectos técnicos que sustentam essa integração.

A contribuição inovadora desta tese está no desenvolvimento de um artefato de software que não existia anteriormente: o UE não 3GPP, responsável por permitir o acesso ao núcleo 5G através de redes de acesso não 3GPP não confiáveis, resolvendo o problema crítico da interoperabilidade entre tecnologias de acesso não 3GPP e o núcleo 5G. Este artefato foi projetado e implementado com base nos princípios descritos ao longo do capítulo, sendo uma peça essencial para a integração dessas tecnologias com o núcleo 5G. A criação desse UE não 3GPP representa um avanço significativo, permitindo que dispositivos conectados a redes não confiáveis possam acessar o núcleo 5G de forma segura, algo que até então não havia sido realizado de forma prática. Além disso, o UE não 3GPP foi projetado para permitir ao operador da infraestrutura coletar métricas de redes não 3GPP, habilitando a possibilidade de incorporar essas métricas nas tomadas de decisão sobre o comportamento da infraestrutura de comunicação.

4.1 Caminhos para acesso ao núcleo 5G

A Figura 4.1 apresenta uma visão geral da arquitetura, evidenciando: (i) os possíveis caminhos para acesso ao núcleo 5G e (ii) os possíveis casos de uso que podem se beneficiar da integração de tecnologias como LoRa, LoRaWAN, Wi-Fi e 5G *longa distância* [Mendes et al. 2020] com o núcleo 5G. À esquerda da figura estão ilustradas distintas aplicações. No centro, encontram-se os elementos que alicerçam a arquitetura convergente e, consequentemente, viabilizam o acesso de tecnologias não 3GPP ao núcleo 5G. À direita, são exibidas as funções de rede que compõem o núcleo 5G, especificado no lançamento 15 [3GPP TR-21.915 2018-12]. Boa parte desses elementos foram implementados e estão acessíveis em distribuições de código aberto, como, por exemplo, *free5GC* [free5GC 2022] e *Open5GS* [Open5GC 2019].

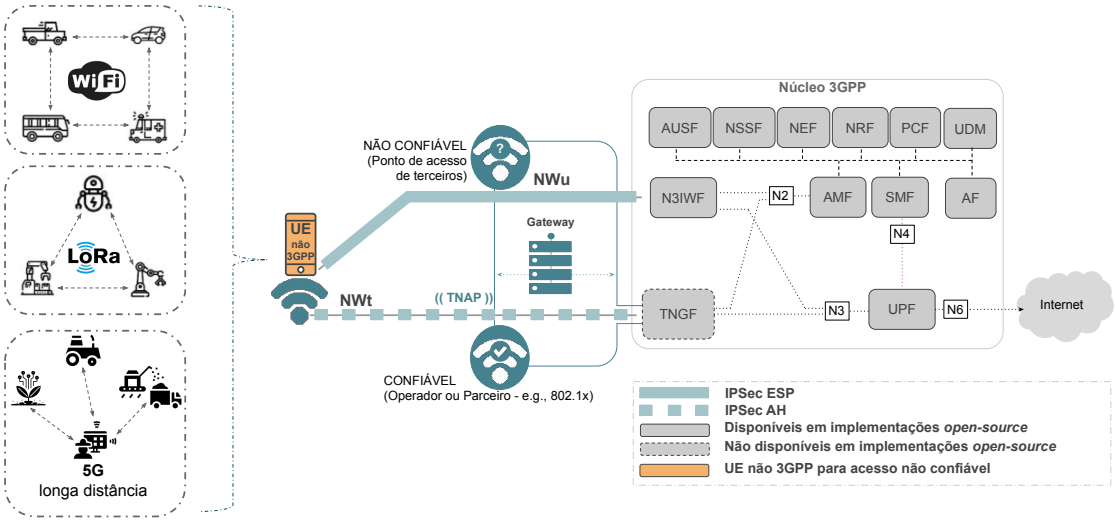

Figura 4.1: Arquitetura convergente: caminhos para acesso ao núcleo 5G a partir de redes não 3GPP *confiáveis* e *não confiáveis*.

A arquitetura convergente é composta por três módulos principais, conforme ilustrado na Figura 4.2. De baixo para cima, o primeiro módulo corresponde ao UE não 3GPP. O módulo intermediário corresponde à N3IWF e o módulo superior corresponde às demais funções do núcleo 5G. As camadas física e de controle são a base para o enlace entre UE não 3GPP e N3IWF. Elas provem suporte a comunicação IKE e à comunicação segura através de IPSec ESP para a sinalização NAS do plano de controle e para o plano de dados do usuário. Métricas dessas camadas podem ser obtidas a partir da funcionalidade de coleta de dados, contida no bloco API do UE não 3GPP. A coleta de dados também monitora parâmetros dos procedimentos IKE, da sinalização NAS e da sessão PDU. O bloco API foi projetado para coletar dados de diferentes fontes e exportar estes dados em formato *JavaScript Object Notation* (JSON).

Projetamos o bloco de Interface do Usuário com três opções: (i) a primeira é baseada na Interface de Linha de Comando, que permite o acompanhamento da execução do UE não 3GPP em tempo real, (ii) a segunda utiliza uma interface de rede virtual, onde o usuário também pode integrar software de terceiros para fornecer carga de trabalho para cenários de teste e (iii) um *Dashboard*, que facilita o monitoramento e visualização gráfica dos dados disponibilizados pelo serviço de API.

O bloco UE é o mais importante componente implementado em nossa arquitetura. Este bloco é responsável por tarefas como (i) executar os procedimentos iniciais de troca de chaves através de IKE; (ii) executar os procedimentos de registro e autenticação com o núcleo 5G atrvés de IPSec, (iii) executar os procedimentos de sinalização NAS do plano de controle, (iv) estabelecer a sessão de PDU para contrução do plano de dados do usuário e (v) fornecer os logs sobre o funcionamento do sistema.

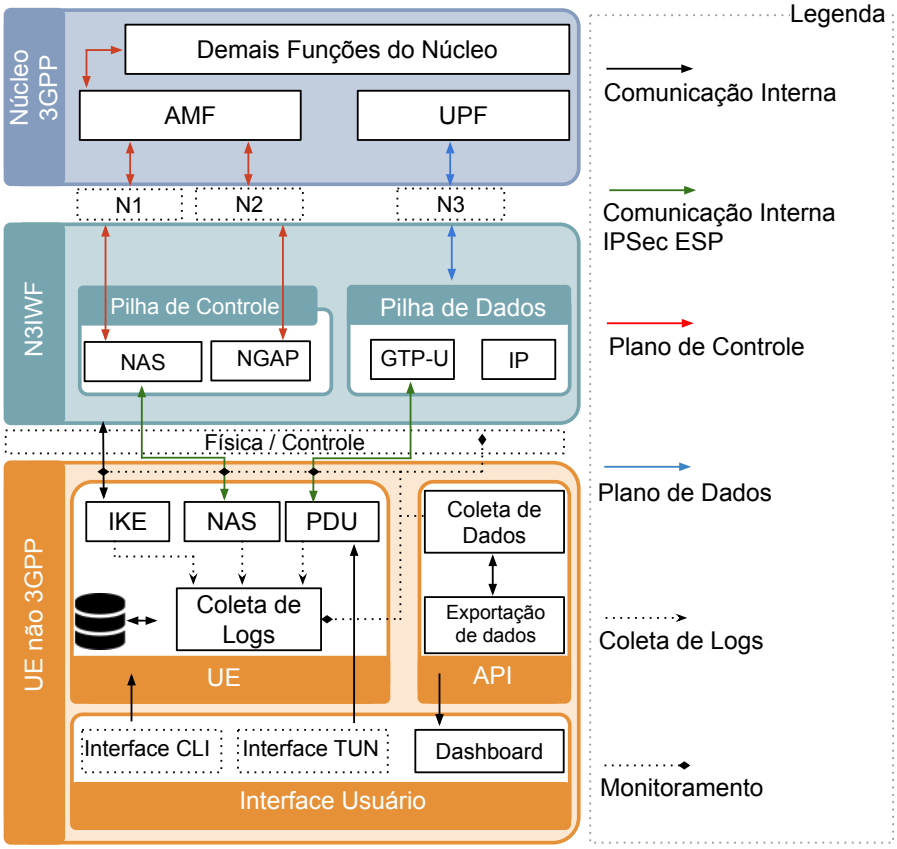

Figura 4.2: Módulos da arquitetura convergente para acesso ao núcleo 5G a partir de redes não 3GPP *não confiáveis*.

O módulo UE *não* 3GPP [1] ilustrado na base da Figura 4.2, é um produto desta tese. Trata-se do primeiro artefato de software capaz de consumir os microsserviços

[1] https://github.com/LABORA-INF-UFG/UE-non3GPP

disponibilizados pela N3IWF e estabelecer a conectividade com o núcleo 5G, através de tecnologias de comunicação sem fio não 3GPP. Esse componente é o elemento crítico da arquitetura convergente. Ele viabiliza o acesso pelo caminho *não confiável* via N3IWF, através de um conjunto de procedimentos que estão distribuídos em seus componentes internos, ilustrados na Figura 4.3.

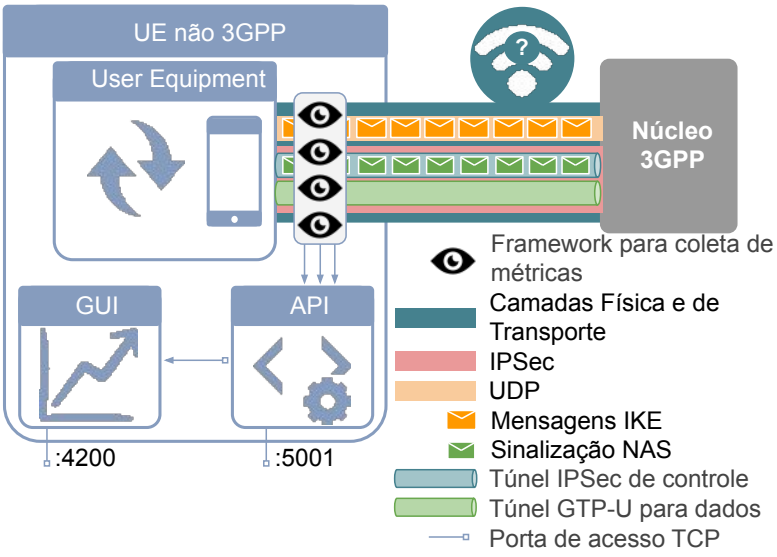

Figura 4.3: Componentes internos do UE não 3GPP, considerando o acesso *não confiável* ao núcleo 5G através da N3IWF.

A comunicação entre o UE não 3GPP e o núcleo 5G é sustentada pelas camadas física e de transporte, que lidam com a transmissão dos dados. A segurança dessa comunicação é garantida pelo uso de IPSec, que estabelece túneis seguros para proteger, tanto o plano de controle (utilizado para sinalização NAS), quanto o plano de dados do usuário. Para a transmissão de mensagens de controle, como a troca de chaves, o protocolo *User Datagram Protocol* (UDP) é empregado, possibilitando a negociação dessas chaves através de IKE. A sinalização NAS é responsável pela troca de mensagens de controle que tratam de processos como registro, autenticação e autorização junto ao núcleo 5G. As mensagens NAS trafegam através de um túnel IPSec dedicado ao controle, enquanto os dados do usuário são transmitidos por meio de um túnel *General Packet Radio Service Tunneling Protocol for the User Plane* (GTPU), que encapsula os pacotes de dados para garantir uma transmissão segura. Todos estes procedimentos, são executados pelo componente interno *User Equipment*, ilustrado em detalhes na Figura 4.4,

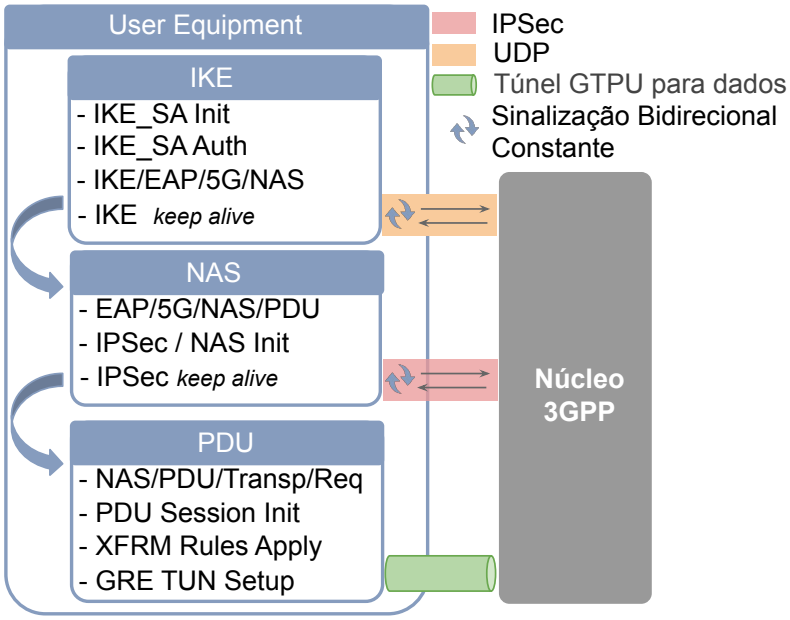

Figura 4.4: Elementos internos do UE não 3GPP responsáveis por processamento IKE, NAS e estabelecimento de sessão PDU.

Além de viabilizar o acesso *não confiável* ao núcleo 5G, o UE não 3GPP incorpora um *framework* específico para o monitoramento das interfaces de rede. Esse *framework* é responsável por coletar métricas importantes de redes não 3GPP, fornecendo ao operador de infraestrutura informações valiosas para análise e monitoramento. Conforme ilustra a Figura 4.5, as métricas coletadas são expostas por meio de uma API, permitindo que outros sistemas ou aplicativos acessem e utilizem esses dados. O acesso à API e ao *dashboard* é viabilizado por portas de acesso *Transmission Control Protocol* (TCP) parametrizadas.

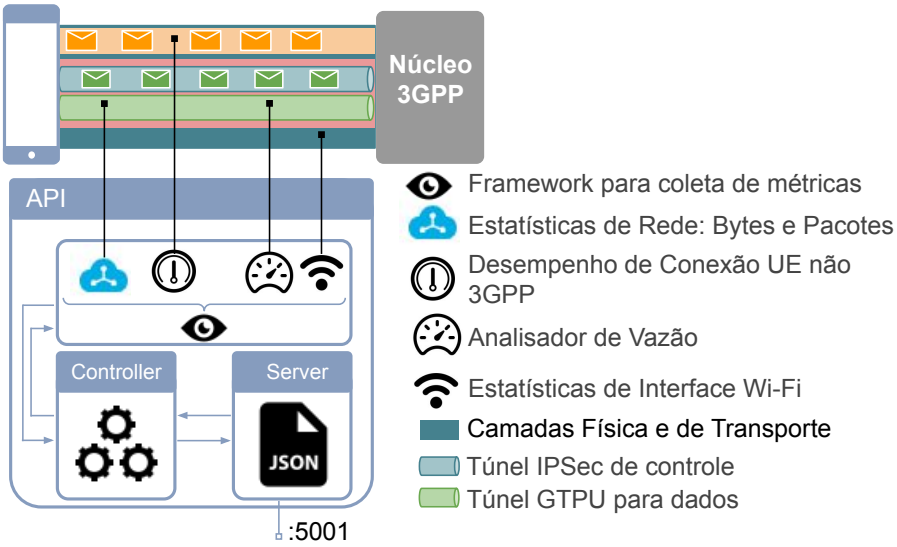

Figura 4.5: Componentes da API de coleta de métricas do UE não 3GPP.

No acesso *não confiável*, não é possível assegurar que o ponto de acesso sem fio possa garantir que a comunicação com o UE aconteça de acordo com os padrões estabelecidos pelo 3GPP para segurança e autenticação, por este motivo, esse modo é caracterizado como *não confiável*. Por essa razão, o UE deve executar um conjunto adicional de procedimentos com o objetivo de estabelecer um canal seguro diretamente com o núcleo 3GPP e realizar sua sinalização de controle exclusivamente através desse canal. Conforme ilustrado na Figura 4.6, o caminho para a convergência com o núcleo 5G, no contexto de acesso *não confiável*, é viabilizado pela N3IWF. Essa função possui um conjunto de microsserviços que, quando consumidos de maneira adequada, viabilizam a comunicação com o núcleo 5G, através de redes de acesso não 3GPP. Implementações de código aberto de núcleo 5G 3GPP, como, por exemplo, *free5GC* [free5GC 2022], já disponibilizam a N3IWF desde a versão 3.0.0, lançada em julho de 2021.

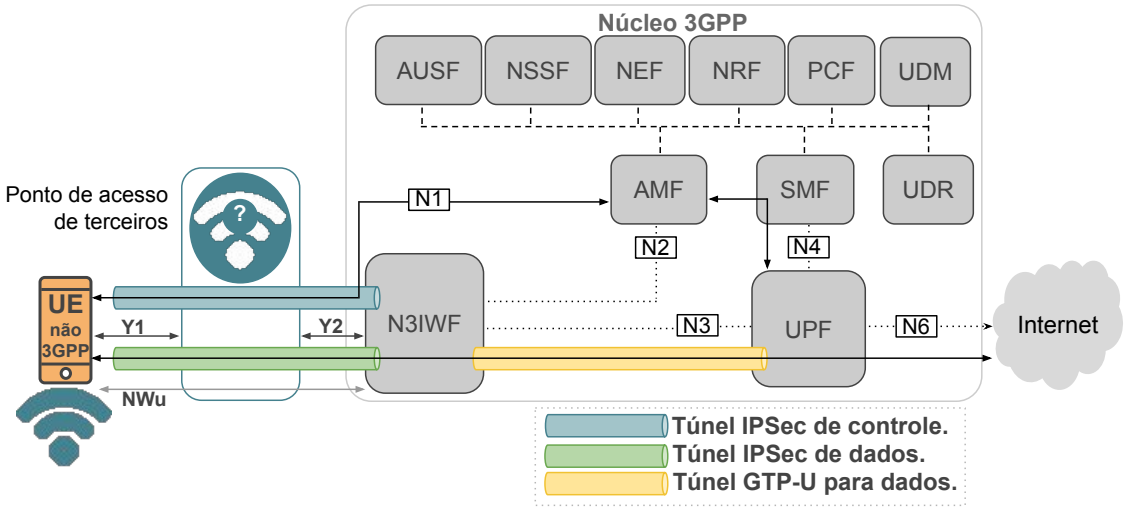

Figura 4.6: Interfaces e túneis de comunicação *IPSec* para o trafego de dados e sinalização do Plano de Controle no acesso não-3GPP *não confiável* através de N3IWF.

Embora o UE não 3GPP tenha implementado boa parte dos procedimentos de registro e autenticação necessários para o acesso ao núcleo 5G, o escopo desta tese não inclui o acesso *confiável* através da TNGF. Isso se deve à ausência de uma implementação de código aberto funcional da TNGF, o que impossibilita a realização de testes e a demonstração do funcionamento desse tipo de acesso não 3GPP *confiável*. Já o acesso *não confiável* é definido através da N3IWF, que expõe um conjunto de microsserviços que, ao serem consumidos de forma adequada, podem habilitar a interligação ao núcleo 5G através de redes de terceiros.

O acesso ao núcleo 5G através de N3IWF somente pode ser realizado por UEs aptos a realizar sinalização NAS [3GPP TS-24.501 2024-04]. Diferentemente das arquiteturas anteriores para interligação de redes não confiáveis e o núcleo, os procedimentos de registro e autenticação são semelhantes ao acesso 3GPP, onde a AMF registra o UE e a AUSF autentica o UE utilizando *Extensible Authentication Protocol - Authentication and Key Agreement* (EAP-AKA)/*5G Authentication and Key Agreement* (5G-AKA). Diferentemente de um acesso 3GPP realizado por um UE tradicional conectado através de uma BS, no acesso não 3GPP *não confiável* o UE deve executar um conjunto de procedimentos adicionais, sendo caracterizado, no contexto deste trabalho, como um UE não 3GPP. Durante a execução dos procedimentos iniciais, especificamente antes do encerramento do procedimento de registro, um enlace do tipo *IPsec Security Association* (IPSec-SA) é configurado entre o UE não 3GPP e a N3IWF para assegurar que as mensagens de mobilidade NAS e a gestão de sessões aconteçam através de um canal seguro. A partir dessa associação segura inicial, o UE não 3GPP deve estabelecer sessões de PDU utilizando o canal IPSec-SA através de mensagens de gestão de sessões do tipo NAS, trocadas com

a SMF através da AMF e da N3IWF. A topologia apresentada na Figura 4.6 ilustra que não existe interligação direta entre N3IWF e AMF. Todos os fluxos de dados envolvidos nos procedimentos de troca de mensagens entre o UE não 3GPP e a SMF transitam obrigatoriamente por N3IWF e AMF. Durante o estabelecimento de uma sessão PDU, a N3IWF realiza uma série de procedimentos, configurando outras associações seguras do tipo IPSec-SA, derivadas do canal IPSec-SA construído inicialmente, antes do encerramento do procedimento de registro. Esses canais derivados são utilizados para o tráfego de diversos fluxos de QoS, contendo métricas da sessão PDU e do túnel GTPU, estabelecido entre a N3IWF e a UPF, com o objetivo de prover acesso ao UE não 3GPP à rede de dados.

Os procedimentos contidos nos microsserviços da N3IWF, que viabilizam o acesso *não confiável*, podem ser agrupados em dois grupos: (i) procedimentos voltados para a estruturação do plano de controle e (ii) procedimentos voltados para a estruturação do plano de dados do usuário. Esses procedimentos são executados por meio de interfaces de rede e utilizam um conjunto de protocolos de comunicação para garantir a segurança dos canais. Cada um desses elementos será descrito com mais detalhes a seguir.

4.2 Interfaces

Conforme ilustra a Figura 4.6, um conjunto de interfaces interliga os componentes envolvidos no acesso não 3GPP *não confiável* através da N3IWF. Cada uma dessas interfaces possui responsabilidades específicas:

- **NWu** - Interface que representa o ponto de referência entre o UE não 3GPP e a N3IWF. É através dessa interface que os túneis IPSec entre o UE não 3GPP e a N3IWF são estabelecidos. É por meio desses túneis que o tráfego relacionado à sinalização do Plano de Controle e o tráfego do Plano de Dados do Usuário entre o UE não 3GPP e o núcleo 5G trafegam com segurança, através de um ponto de acesso *não confiável* não 3GPP.
- **Y1** - Ponto de referência entre o UE não 3GPP e a rede de acesso *não confiável*, através da qual o enlace com a N3IWF será estabelecido.
- **Y2** - Ponto de referência entre a rede de acesso *não confiável* e a N3IWF, através do qual será transportado o tráfego de dados da interface *NWu*.
- **N1** - Ponto de referência que conecta o UE não 3GPP e a AMF, através da N3IWF.
- **N2** - Ponto de referência que conecta a N3IWF à AMF, responsável pelo tráfego de dados associados aos procedimentos de autenticação e autorização do UE não 3GPP junto às demais funções do núcleo 5G. Esta interface também é responsável pelo intercâmbio de dados necessários para o estabelecimento dos túneis IPSec para

comunicação segura e pelo tráfego que gerencia a mobilidade e a sessão do UE não 3GPP.

- **N3** - Ponto de referência entre a N3IWF e a UPF. Esta interface é responsável pelo tráfego de dados entre o UE não 3GPP e o núcleo 5G. A interface N3 é o caminho através do qual os pacotes de dados que partem do UE não 3GPP são encaminhados para a UPF, que, por sua vez, direciona esses pacotes para o destino apropriado. A interface N3 também é responsável por prover suporte a políticas de QoS, que são gerenciadas pela UPF. São essas políticas que garantem que os requisitos de QoS para diferentes tipos de tráfego de dados sejam atendidos, priorizando o tráfego de acordo com as necessidades da aplicação ou serviço que está sendo consumido. A interface N3 também coopera com a AMF em procedimentos associados ao gerenciamento da mobilidade e da continuidade da sessão de dados quando o UE não 3GPP se move entre diferentes pontos de cobertura da rede, com o objetivo de manter os túneis que conectam o UE não 3GPP ao núcleo 5G ativos, possibilitando a reconfiguração dinâmica quando necessário.

De maneira resumida, o conjunto de procedimentos executados através das interfaces NWu, Y1, Y2, N1, N2 e N3 é responsável por garantir que o tráfego associado ao Plano de Dados de Usuário possa ser transmitido de maneira segura entre o UE não 3GPP e o núcleo 5G, através de uma infraestrutura de rede *não confiável* [3GPP TR-23.501 2021-12-23], bem como garantir que todos os procedimentos de sinalização associados ao Plano de Controle aconteçam de forma coesa. No contexto do acesso não 3GPP *não confiável*, as interfaces são apenas pontos de acesso. Para que toda a infraestrutura de comunicação se estabeleça, é necessário que os procedimentos executados através dessas interfaces ocorram de acordo com um conjunto de protocolos bem estabelecidos.

4.3 Estruturação do plano de controle

A N3IWF provê suporte às seguintes funcionalidades para estruturar o canal de comunicação, através do qual a sinalização do plano de controle é realizada:

- Suporte ao estabelecimento de túnel IPSec entre a N3IWF e o UE não 3GPP, através da interface NWu, usando protocolos IKE-v2. A interface NWu facilita a troca de mensagens de controle e dados, enquanto o protocolo IKE-v2, através de suas capacidades de negociação de chaves e autenticação mútua, garante a integridade e a confidencialidade das informações trocadas. Este processo envolve uma série de etapas, incluindo a negociação inicial dos parâmetros de segurança,

a autenticação das partes envolvidas e, por fim, o estabelecimento do canal de comunicação propriamente dito.

- Estabelecimento de túnel para sinalização IPSec-SA, encarregado de proteger as mensagens de sinalização do tipo NAS que transitam entre o UE não 3GPP e a AMF. Esse túnel IPSec-SA assegura que todas as mensagens de sinalização, relevantes para o controle e a gestão da conexão entre o UE não 3GPP e o núcleo da rede 5G, sejam criptografadas e autenticadas, prevenindo interceptações, modificações e ataques maliciosos. A proteção das mensagens NAS é crucial, pois essas contêm informações sensíveis relativas à autenticação, autorização e controle de mobilidade do UE não 3GPP.
- Estabelecimento de túnel de comunicação IPSec-SA, derivado a partir do túnel IPSec-SA de sinalização e controle, com o objetivo de proteger o tráfego de dados da sessão PDU entre o UE não 3GPP e a UPF. O tráfego de dados da sessão PDU transporta informações utilizadas para a operação e os serviços de rede, tornando relevante que essas informações também transitem através de um canal seguro.
- Encerramento da interface N2 através dos protocolos *Next-Generation Application Protoco* (NGAP) e *Stream Control Transmission Protocol* (SCTP) em direção à AMF. O uso de NGAP sobre o SCTP garante que as mensagens de controle sejam transmitidas de forma segura e ordenada, beneficiando-se de características do SCTP, como, por exemplo, garantia de entrega, resiliência a falhas e a manutenção de múltiplos fluxos de dados independentes.
- Retransmissão de sinalização NAS através da interface N1, para controle de taxas de *uplink* e *downlink* entre o UE não 3GPP e a AMF. A interface N1 é relevante para a troca de mensagens de controle NAS, que são responsáveis por gerenciar aspectos como a autenticação, autorização, configuração de sessão e mobilidade dos UEs. Através da retransmissão dessas mensagens, a rede assegura que os comandos e as informações críticas relacionadas às taxas de *uplink* e *downlink* sejam corretamente entregues e processadas, garantindo uma alocação eficiente dos recursos de rede e a QoS necessária.
- Construção e transmissão de mensagens NAS para executar as operações de autenticação e registro do UE não 3GPP e autorizar o seu acesso ao núcleo 5G. As mensagens NAS asseguram que o UE seja corretamente identificado e autorizado a acessar o núcleo 5G. O processo começa quando o UE não 3GPP envia uma solicitação de registro ao núcleo 5G via N3IWF. Em seguida, a N3IWF encaminha a mensagem para a AMF, que gerencia a autenticação do UE não 3GPP com o núcleo 5G. Após a autenticação ser validada, a N3IWF retransmite a confirmação ao UE não 3GPP, finalizando o registro e autorizando seu acesso.
- Construção e transmissão de mensagens NAS para estabelecer a sessão de PDU.

A sessão de PDU permite o transporte de dados do UE não 3GPP para o núcleo 5G e vice-versa. Nesse processo, a N3IWF cria uma mensagem de solicitação de estabelecimento de sessão de PDU, que contém informações como o tipo de conexão solicitada e os parâmetros de QoS. A N3IWF envia essa mensagem encapsulada à AMF, que a encaminha para a SMF. A SMF, por sua vez, aloca os recursos necessários e responde com a aceitação ou rejeição da sessão de PDU, que é então transmitida de volta ao UE não 3GPP pela N3IWF.

- Controle de sinalização, relacionada às sessões de PDU e QoS com a SMF através da interface N2, retransmitida pela AMF. A N3IWF encapsula as mensagens de sinalização NAS provenientes do UE não 3GPP e as envia para a AMF, que repassa essas mensagens para a SMF. A SMF é responsável por estabelecer e controlar os parâmetros de QoS das sessões de PDU, garantindo que a qualidade do serviço solicitada seja atendida. Durante a sessão de PDU, a N3IWF retransmite qualquer modificação nas políticas de QoS ou nos recursos alocados, permitindo ajustes dinâmicos no fluxo de dados, conforme necessário, para assegurar que o UE não 3GPP mantenha a qualidade de conexão adequada.
- Procedimento de escolha da AMF. Quando o UE não 3GPP se conecta à rede, a N3IWF precisa selecionar a AMF adequada para gerenciar as operações de mobilidade e sessão do UE. Esse procedimento começa com a N3IWF enviando uma solicitação inicial ao núcleo 5G, que inclui informações sobre a identidade do UE e o contexto de rede. A rede responde com uma lista de AMFs disponíveis, levando em consideração critérios como a localização geográfica do UE, as capacidades da AMF e a carga da rede. A N3IWF então escolhe a AMF mais adequada e a informa sobre a conexão do UE não 3GPP, estabelecendo a interface de comunicação N2 entre a N3IWF e a AMF selecionada, que será responsável por controlar o UE não 3GPP durante sua sessão na rede 5G.

4.4 Estruturação do plano de dados do usuário

Para estabelecer o Plano de Dados do Usuário em um contexto de acesso *não confiável* ao núcleo 5G, a N3IWF provê suporte às seguintes funcionalidades:

- Término da interface N3 usando protocolo GTPU em direção a UPF.
- Reenvio de pacotes do Plano de Dados do Usuário, associados a *uplink* e *downlink* entre o UE não 3GPP e UPF.
- Encapsulamento e desencapsulamento de pacotes IPSec e GTPU.
- Marcação de pacotes de *uplink* do Plano de Dados do Usuário através da interface N3.

- Aplicação de QoS correspondente à marcação de pacotes de *uplink* através da interface N3.

Os microsserviços disponibilizados na N3IWF executam procedimentos que estão intrinsecamente associados às suas interfaces (e.g., N1, N2, N3, NWu, Y1 e Y2) e aos protocolos envolvidos. Cada interface e protocolo desempenha uma responsabilidade na garantia da estruturação de canais para uma comunicação segura e eficiente, para os planos de dados e de controle, entre o UE não 3GPP e o núcleo 5G. Desde a etapa inicial, em que se faz a seleção e descoberta da rede de acesso, passando pelos procedimentos de registro, autenticação e autorização, até o estabelecimento de sessões PDU, todos esses procedimentos dependem de uma integração coesa de múltiplos protocolos, algoritmos clássicos de criptografia e interfaces, que são discutidos com mais detalhes a seguir.

4.5 Protocolos

O acesso *não confiável* apresenta desafios específicos de segurança e autenticação, que são endereçados através do uso de IPSec para o estabelecimento dos túneis seguros ilustrados na Figura 4.6. Nesse sentido, as interfaces NWu, Y1, Y2, N1 e N2 atuam em conjunto com diferentes protocolos para que determinados procedimentos possam ser executados, habilitando a conexão *não confiável* através de uma rede de acesso não 3GPP e o núcleo 5G. Para compreender o relacionamento entre as interfaces e a pilha de protocolos envolvidos, os procedimentos foram separados por etapas, agrupando as interfaces, os respectivos protocolos e os procedimentos envolvidos em cada uma delas.

Registro e autenticação

As interfaces Y1 e Y2, em conjunto com o protocolo IP de uma WLAN *não confiável*, atuando nas camadas física - *Physical Layer* (L1) e de dados - *Data Link Layer* (L2), são responsáveis por viabilizar o acesso entre o UE não 3GPP e a N3IWF. Através da interface NWu, os protocolos IKE e EAP-5G executam os procedimentos de conexão inicial entre o UE não 3GPP e o núcleo 5G. Durante as etapas de registro inicial e autenticação do UE não 3GPP, a interface N2, que interliga a N3IWF e a AMF, atua em diferentes procedimentos nas camadas L1 e L2, utilizando os protocolos IP, SCTP, NGAP e NAS [3GPP TS-24.501 2024-04]. Esses procedimentos estão associados à troca de mensagens de sinalização de controle, garantindo que o UE não 3GPP seja autenticado e autorizado corretamente através da interface N1. O gerenciamento de mobilidade e controle de sessão do UE não 3GPP também é realizado através das interfaces N1 e N2, que coordenam as ações com a AMF, conforme ilustra a Figura 4.7.

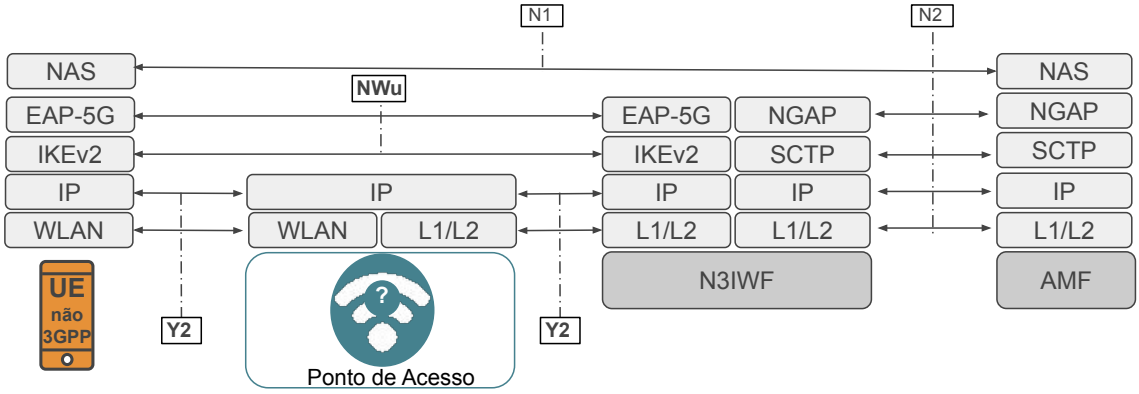

Figura 4.7: Protocolos de comunicação envolvidos nos procedimentos de registro e autenticação no acesso não 3GPP *não confiável* através de N3IWF.

Sessão PDU

Ao final dos procedimentos de registro e autenticação, são executados procedimentos complementares com o objetivo de estabelecer o túnel IPSec do Plano de Dados do Usuário. É a execução correta desses procedimentos que garante que a comunicação dos dados do usuário ocorra de maneira segura e eficiente, protegendo a integridade e a confidencialidade das informações transmitidas. As interfaces e protocolos envolvidos são ilustrados na Figura 4.8 e envolvem o UE não 3GPP, o ponto de acesso *não confiável*, a N3IWF e a UPF.

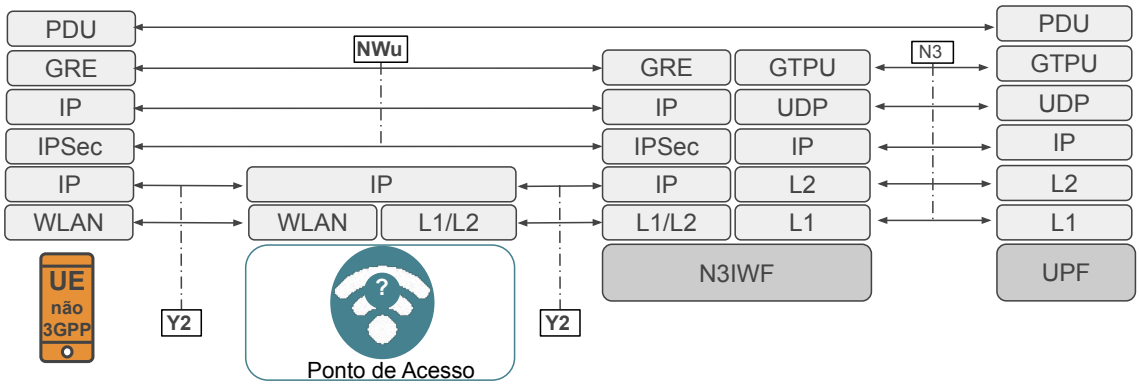

Figura 4.8: Protocolos de comunicação envolvidos nos procedimentos de construção do Plano de Dados do Usuário no acesso não-3GPP *não confiável* através de N3IWF.

Conforme ilustra a Figura 4.8, a pilha de protocolos no UE não 3GPP tem início com o ponto de acesso *não confiável* nas camadas L1 e L2, que habilitam a conectividade inicial com a rede sem fio *não confiável*. Acima dessas camadas, há o protocolo IP, seguido do IPSec, que fornece a segurança necessária para o tráfego dos pacotes do plano de dados do usuário. O protocolo IPSec encapsula os pacotes IP

originais, adicionando camadas de segurança. Acima do IPSec, o protocolo IP é usado novamente para rotear os pacotes através da rede. Finalmente, através de *Generic Routing Encapsulation* (GRE) e PDU, os dados são encapsulados e transportados até o destino. No ponto de acesso *não confiável*, a pilha de protocolos também começa com as camadas L1 e L2, que se conectam diretamente à camada IP. A rede de acesso *não confiável* facilita a comunicação entre o UE não 3GPP e a N3IWF, assegurando que os pacotes encapsulados por IPSec possam ser transmitidos de forma segura. A N3IWF também possui procedimentos vinculados às camadas L1 e L2 para se comunicar com a rede de acesso *não confiável*. Acima dessas camadas, o protocolo IP é utilizado para rotear os pacotes. O IPSec é novamente empregado para desencapsular os pacotes recebidos do UE não 3GPP, garantindo a segurança dos dados. Acima do IPSec, o protocolo IP é usado mais uma vez para o roteamento interno. Os pacotes são encapsulados pelo GRE e finalmente encaminhados à UPF via GTPU, através da interface N3.

De forma resumida, a execução dos procedimentos de Registro e Autenticação e a estruturação do Plano de Dados do usuário em um cenário envolvendo a conexão de um UE não 3GPP a um núcleo 5G através da N3IWF, utilizando um ponto de acesso *não confiável*, envolvem uma série de protocolos e procedimentos para garantir a segurança e a integridade dos dados transmitidos. As pilhas de protocolos no UE não 3GPP, ponto de acesso *não confiável*, N3IWF, AMF e UPF, ilustradas nas Figuras 4.7 e 4.8, foram estruturadas para encapsular, proteger e transmitir os pacotes de dados do usuário, empregando mecanismos como IPSec, EAP-5G e GTPU. Em um acesso 3GPP através de uma BS, esses procedimentos adicionais são desnecessários, visto que todos os elementos da infraestrutura são controlados pelo operador da rede e seguem as diretrizes 3GPP, o que não ocorre quando considera-se a integração a partir de outras tecnologias de comunicação sem fio. Nas seções a seguir, são apresentados os diagramas de sequência dos principais procedimentos envolvendo os protocolos e as interfaces, detalhando as etapas críticas e as interações necessárias para suportar o acesso ao núcleo 5G, através de uma rede de acesso *não confiável*.

Procedimentos para estruturação do plano de controle no acesso *não confiável*

Nesta seção, são detalhados os procedimentos envolvidos no acesso ao núcleo 5G através de uma rede de acesso não 3GPP *não confiável*. O fluxo segue uma sequência que se inicia com a descoberta e seleção da rede de acesso, através da qual o UE não 3GPP se conecta ao N3IWF. Em seguida, ocorrem os procedimentos de registro, autenticação e autorização, que viabilizam o acesso do UE não 3GPP ao núcleo 5G. Finalmente, os procedimentos relacionados ao estabelecimento de sessões PDU são executados,

permitindo que o UE não 3GPP transmita e receba dados através da rede 5G. Cada um desses procedimentos é detalhado a seguir.

Descoberta e seleção da rede de acesso *não confiável*

O primeiro procedimento executado por um UE não 3GPP é a descoberta da rede de acesso *não confiável*, seguido pelo procedimento de escolha da N3IWF, que pode ser observado no início do fluxo de procedimentos ilustrado na Figura 4.9. A descoberta e seleção da rede de acesso *não confiável* são realizadas através de *Access Network Discovery and Selection Policy* (ANDSP) [ETSI TS-24.526 2020]. A ANDSP é composta por dois componentes, o *Non-3GPP Access Networks* (N3AN) e a WLAN Selection Policy (WLANSP) [3GPP TR-24.526 2024-04-02]. A WLANSP contém um conjunto de políticas que orientam o UE na seleção da rede WLAN mais adequada, com base em critérios predefinidos, tais como a força do sinal, a carga da rede e as preferências do usuário. Seguindo essas políticas, o UE consegue identificar e conectar-se à WLAN disponível, estabelecendo um endereço IP local necessário para os procedimentos iniciais de comunicação. As informações de configuração fornecidas pelo N3AN disponibilizam ao UE dados sobre os nós de rede não 3GPP disponíveis. Esses dados incluem uma lista priorizada de *Public Land Mobile Network*s (PLMNs), que abrangem tanto a *Home Public Land Mobile Network* (HPLMN) quanto outras PLMNs às quais o UE pode se conectar. Para cada PLMN, as informações de configuração do N3AN especificam o N3IWF preferido dentro do PLMN, utilizando parâmetros de preferência e *Fully Qualified Domain Name*s (FQDNs) para facilitar a descoberta e a seleção da N3IWF mais adequada. Além disso, um UE pode ser pré-configurado com identificadores de N3IWF [ETSI TS-24.526 2020], incluindo FQDNs ou endereços IP específicos, que permitem ao UE priorizar a seleção da N3IWF, independentemente dos parâmetros de preferência.

Registro, autenticação e autorização

Após estabelecer conexão com a rede de acesso *não confiável* e determinar qual N3IWF será utilizada para viabilizar os procedimentos de conexão com o núcleo 5G, o UE não 3GPP inicia os procedimentos de registro, autenticação e autorização, necessários para estruturar os canais de comunicação seguros, tanto para os planos de dados, quanto para os de controle. Esses procedimentos começam com a transmissão de mensagens NAS, partindo do UE não 3GPP em direção à N3IWF, que atua como um intermediário entre o UE não 3GPP e o núcleo 5G. Os procedimentos de registro, autenticação e autorização, ilustrados na Figura 4.9, estão enumerados, e cada uma das etapas é descrita em detalhes a seguir:

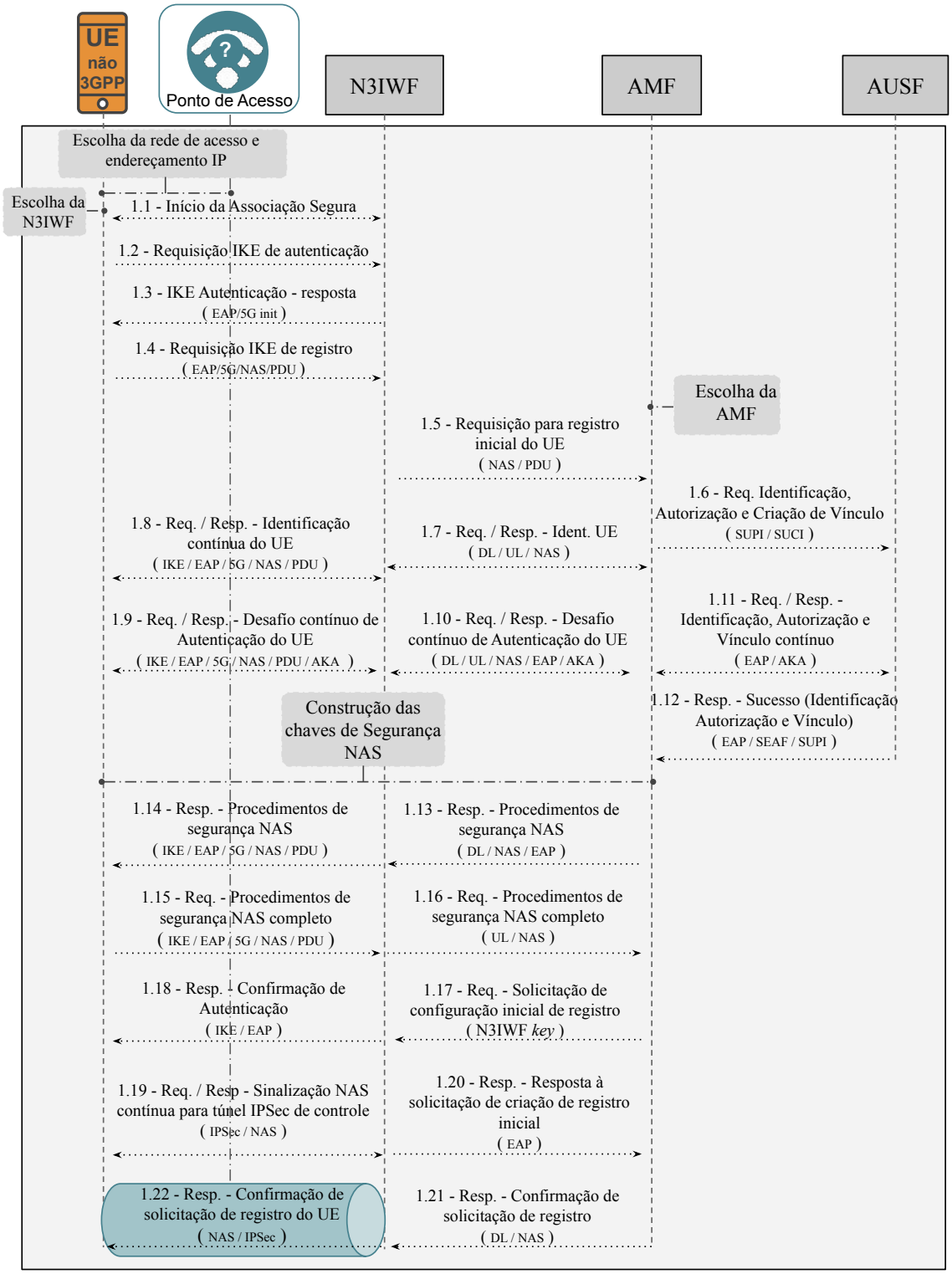

Figura 4.9: Sequência de procedimentos para registro, autenticação e autorização do UE não 3GPP e o núcleo 5G.

- **1.1** - O UE não 3GPP dá início a um procedimento de troca de mensagens com a N3IWF selecionada, utilizando o protocolo IKE-v2. O objetivo deste procedimento

de troca de mensagens é estabelecer uma associação inicial do tipo *Internet Key Exchange Security Association* (IKE-SA). A partir dessa primeira associação segura, todas as mensagens IKE subsequentes são criptografadas e têm sua integridade protegida através da utilização da IKE-SA, previamente estabelecida.

- **1.2** - O UE não 3GPP envia a solicitação de autenticação do tipo IKE-*AUTH* [Kozierok 2005] sem parâmetros de autenticação, indicando apenas o uso de EAP-5G. A solicitação de autenticação IKE pode também incluir parâmetros de notificação para indicar o suporte ao *IKEv2 Mobility and Multihoming Protocol* (MOBIKE) e um parâmetro adicional solicitando acesso à chave pública do certificado da N3IWF.
- **1.3** - A N3IWF responde com uma mensagem de autenticação IKE, incluindo um pacote do tipo *EAP-Request/5G-Start*, informando ao UE não 3GPP que inicie o envio de mensagens NAS. A resposta de autenticação IKE também inclui a chave pública da N3IWF, caso esta tenha recebido o parâmetro de solicitação de acesso à chave pública, encaminhado no procedimento 1.2.
- **1.4** - O UE não 3GPP envia a solicitação de autenticação IKE, incluindo um pacote *EAP-Request/5G-Start* com a solicitação de registro NAS e parâmetros da rede de acesso não confiável que está sendo utilizada, e.g., *Globally Unique AMF Identifier* (GUAMI), identificador da PLMN selecionada e *Network Slice Selection Assistance Information* (NSSAI) solicitado. Todas as mensagens NAS subsequentes entre o UE não 3GPP e a N3IWF são encapsuladas dentro de pacotes EAP/5G-NAS.
- **1.5** - A N3IWF seleciona um AMF com base nos parâmetros da rede de acesso *não confiável* recebidos e nas diretrizes de política local, encaminhando a solicitação de registro recebida do UE não 3GPP para o AMF selecionado dentro de uma mensagem inicial do UE não 3GPP através da interface N2, conforme ilustrado na Figura 4.6. Todas as mensagens NAS trocadas entre o UE não 3GPP e o AMF são retransmitidas de forma transparente pela N3IWF, que passa a atuar como um *gateway* entre esses dois elementos. O AMF pode solicitar o *Subscription Concealed Identifier* (SUCI) do UE não 3GPP através de uma mensagem de solicitação de identidade NAS. Esta solicitação é respondida pelo UE não 3GPP com uma mensagem de resposta de identidade NAS.
- **1.6 a 1.11** - A AMF seleciona uma AUSF para executar os procedimentos de autenticação do UE não 3GPP com base no SUCI ou no *Subscription Permanent Identifier)* (SUPI). A AUSF, por sua vez, escolhe uma UDM para obter os dados de autenticação e executa o procedimento de autenticação EAP-AKA (Redes 4G) ou 5G-AKA (Redes 5G) com o UE não 3GPP.
- **1.12** Após a autenticação bem-sucedida, a AUSF envia uma chave de *ancoragem* de segurança do tipo *Security Anchor Function* (SEAF) para o AMF, que *deriva* as

chaves de segurança NAS e a chave de segurança da N3IWF.

- **1.13** A AMF encapsula a mensagem de sucesso EAP recebida do AUSF dentro da mensagem de segurança NAS e a envia ao UE não 3GPP para que o mesmo ative a estrutura de segurança baseada em NAS.
- **1.14 a 1.16** - O UE não 3GPP também *deriva* a chave SEAF, as chaves de segurança NAS e a chave da N3IWF, enviando em seguida uma mensagem NAS sinalizando a conclusão dos procedimentos de segurança para a AMF.
- **1.17 a 1.18** - A AMF envia, em seguida, uma mensagem NGAP de solicitação de configuração de contexto inicial à N3IWF, incluindo a chave N3IWF. Esta ação desencadeia o envio de uma mensagem EAP de sucesso da N3IWF para o UE não 3GPP, concluindo a sessão EAP-5G.
- **1.19** - Uma associação segura do tipo IPSec é estabelecida entre o UE não 3GPP e a N3IWF utilizando a chave pública N3IWF em modo túnel, com a alocação de um endereço IP interno para o UE não 3GPP e um endereço IP NAS para a N3IWF. Todas as mensagens NAS subsequentes entre o UE não 3GPP e a N3IWF são encapsuladas dentro do túnel IPSec de sinalização estabelecido.
- **1.20** - A N3IWF notifica a AMF que o contexto do UE não 3GPP foi criado, enviando uma resposta de configuração de contexto inicial do tipo NGAP.
- **1.21 a 1.22** - Finalmente, a AMF envia uma mensagem indicando o *aceite de registro* NAS para a N3IWF, incluindo a NSSAI permitida para o tipo de acesso do UE não 3GPP. A N3IWF encaminha essa mensagem ao UE não 3GPP, através da associação de segurança IPSec de sinalização estabelecida.

Após a execução dos procedimentos de registro, o UE não 3GPP passa a suportar a sinalização NAS com o núcleo 5G para as funções de mobilidade e gerenciamento de sessão, através da interface N1, conforme ilustrado na Figura 4.6. Múltiplas instâncias N1 devem existir para um UE não 3GPP conectado a um núcleo 5G através de uma rede de acesso *não confiável*. Para um UE não 3GPP conectado simultaneamente à mesma PLMN por meio de um acesso 3GPP e uma rede de acesso *não confiável*, o registro é realizado com um único AMF utilizando um *5G Globally Unique Temporary Identifier* (5G-GUTI) comum, mas a UDM gerencia procedimentos de registro independentes para cada acesso [TR-21.916 2024]. Para um UE não 3GPP atendido por diferentes PLMNs, o UE não 3GPP é registrado com dois AMFs distintos. Para um UE não 3GPP registrado no núcleo 5G através de uma rede de acesso *não confiável*, a mudança de ponto de acesso não deve levar o UE não 3GPP a realizar um novo procedimento de registro, ou seja, não suporta a atualização de registro de mobilidade em acesso não 3GPP.

4.6 Transição de estados para o gerenciamento de registro e de autenticação

Um UE não 3GPP que executa com sucesso os procedimentos de registro, autenticação e autorização em um núcleo 5G por meio de uma rede de acesso *não confiável*, tem seu estado de acesso não 3GPP modificado para *Registered Mode* (RM-REGISTERED), tanto no UE não 3GPP, quanto na AMF. Isso significa que o UE pode iniciar ou receber sessões de comunicação (como chamadas, mensagens ou dados) e está em conformidade com os procedimentos de mobilidade e rastreamento de área definidos pela rede.

Assim que a associação segura IPSec, ilustrada no procedimento 1.19 da Figura 4.9, é concluída, o estado do UE não 3GPP é alterado para *Connection Management - Connected Mode* (CM-CONNECTED). Neste estado, o UE está conectado à rede e tem um canal de comunicação ativo estabelecido, podendo enviar e receber dados em tempo real, além de possibilitar à rede saber sua localização exata. É importante destacar que um UE não 3GPP não estabelece conexões simultâneas através da interface NWu para acessar o núcleo 5G. A conexão através da interface NWu é liberada somente em três possíveis situações: (*i*) como resultado de um procedimento explícito de *desregistro* por parte do UE não 3GPP; (*ii*) através de um procedimento de liberação por parte da rede de acesso *não confiável*; ou (*iii*) por meio de um procedimento de liberação partindo da N3IWF, que pode ser determinado por um mecanismo de detecção de conexões inativas presente no protocolo IKE.

Quando uma ação de liberação da conexão através da interface NWu ocorre, o UE não 3GPP tem seu estado modificado para *Connection Management - Idle Mode* (CM-IDLE), e um temporizador de *desregistro* é iniciado [ETSI TS-123.501 2018-09]. Este estado indica que o UE não tem um canal de comunicação ativo com a rede. Embora o UE ainda esteja registrado na rede (em RM-REGISTERED), este UE não está atualmente transmitindo ou recebendo dados ativamente. A localização precisa do UE não é mais conhecida pela rede, contudo, mensagens de notificação ainda podem ser enviadas ao dispositivo quando necessário.

Considerando a interface N2 que interliga a N3IWF e a AMF, um UE não 3GPP com uma conexão ativa através desta interface tem seu estado alterado para CM-CONNECTED no AMF. A conexão através da N2 pode ser liberada como resultado de um procedimento explícito de *desregistro* ou pode ser desencadeada pela N3IWF em decorrência da liberação da conexão através da interface NWu. Quando ocorre a liberação da conexão através da interface N2, o UE não 3GPP transita para o estado de CM-IDLE no AMF, que inicia um temporizador de *desregistro* da rede. Quando a AMF libera a interface N2, a N3IWF deve liberar todos os recursos associados ao UE não 3GPP, incluindo a conexão de acesso não 3GPP com o UE não 3GPP e seus recursos associados

à conexão através da interface N3 com a UPF [ETSI TS-123.501 2018-09].

Quando um UE não 3GPP entra em estado CM-IDLE, inicia-se um conjunto de procedimentos com o objetivo de solicitar o restabelecimento da conexão para sinalização NAS e o restabelecimento do plano de usuário para as sessões de PDU vinculadas ao acesso não 3GPP [ETSI TS-123.501 2018-09]. Se o estado for RM-REGISTERED, tanto no UE não 3GPP quanto na AMF, a transição para o estado de *Deregistered Mode* (RM-DEREGISTERED) ocorre como resultado de um procedimento explícito de *desregistro* ou do *desregistro* realizado ao expirar o temporizador.

Conexões com o núcleo 5G estabelecidas através de uma rede de acesso *não confiável* não fornecem suporte à execução de procedimentos de atualização periódica de registro do UE com o núcleo [ETSI TS-123.501 2018-09]. A atualização periódica de registro é um mecanismo utilizado pelo UE para informar periodicamente ao núcleo 5G sobre sua presença e status, podendo desencadear transições de estado. A execução deste procedimento ajuda a manter o UE registrado na rede e a garantir que ele possa ser alcançado para comunicação e dados. No entanto, quando um UE está conectado ao núcleo 5G através de uma rede de acesso *não confiável*, essa rede de acesso pode introduzir incertezas em termos de latência, perda de pacotes e interferências, podendo impactar na *periodicidade* de envio das mensagens de atualização de registro.

O processo de transição e gerenciamento de estados é responsável por garantir a integridade e a segurança das conexões com o núcleo 5G, permitindo uma gestão eficiente dos recursos de rede e assegurando a continuidade dos serviços fornecidos ao UE não 3GPP. O controle preciso desses estados garante que as conexões sejam mantidas, somente enquanto necessárias e que os recursos sejam liberados de forma adequada para otimizar o desempenho da rede.

4.7 Estruturação da sessão PDU - Acesso *não confiável*

Após os procedimentos de registro, autenticação e autorização, são executados os procedimentos para o estabelecimento da sessão PDU entre o UE não 3GPP e o núcleo 5G. Todos os procedimentos envolvidos no estabelecimento da sessão de PDU são executados com o uso de sinalização NAS, através da associação segura IPSec estabelecida entre o UE não 3GPP e a N3IWF, descrita na Seção 4.5. A sessão de PDU é estruturada a partir de um conjunto de procedimentos, envolvendo microsserviços disponibilizados nas funções N3IWF, AMF, SMF, UPF, UDM e PCF.

A iteração entre cada uma das funções, bem como a ordem de execução dos procedimentos envolvidos, são ilustrados na Figura 4.10. Detalhes de cada um dos procedimentos são discutidos a seguir:

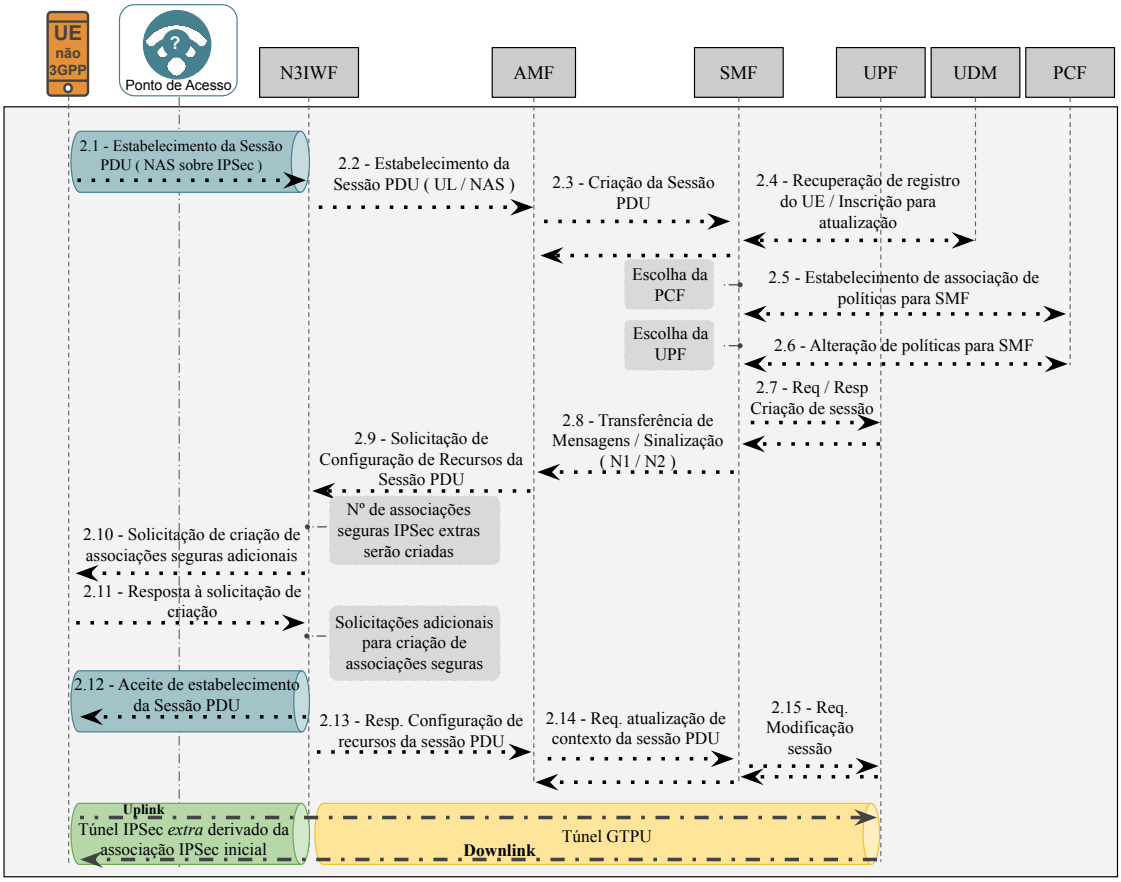

Figura 4.10: Sequência de procedimentos para o estabelecimento da sessão PDU.

- **2.1 a 2.2** - Inicialmente, o UE não 3GPP encaminha uma solicitação de estabelecimento de sessão PDU à N3IWF utilizando a associação segura IPSec para a sinalização NAS. Após receber essa solicitação, a N3IWF a encaminha de forma transparente à AMF em uma mensagem NAS de *uplink*. A N3IWF atua como um intermediário, retransmitindo as solicitações do UE não 3GPP para a AMF, que é responsável por gerenciar a sessão PDU. Este mecanismo de encaminhamento transparente assegura que a solicitação original do UE não 3GPP seja preservada e processada corretamente pela AMF, facilitando a configuração eficiente e segura das sessões de dados junto ao núcleo 5G.
- **2.3 a 2.8** - No núcleo 5G, são executados procedimentos semelhantes aos que seriam realizados durante o estabelecimento de uma sessão PDU em um acesso 3GPP *convencional*. Em outras palavras, os procedimentos 2.3, 2.4, 2.5, 2.6, 2.7 e 2.8, ilustrados na Figura 4.10, são comuns tanto em um acesso 3GPP quanto em um acesso não 3GPP. Esses procedimentos incluem a autenticação do UE não 3GPP, a configuração de recursos de rede e a alocação de perfis de QoS necessários para suportar a sessão de dados, sendo devolvidos à AMF por intermédio da SMF.

- **2.9** - A AMF envia uma mensagem de solicitação de configuração de recursos de sessão PDU através da interface N2 à N3IWF com o objetivo de estabelecer, junto à rede de acesso *não confiável*, os recursos necessários para a sessão PDU. Essa mensagem contém diversos parâmetros relevantes para a configuração da sessão. São especificados os perfis de QoS e os identificadores de fluxo de QoS, que determinam as prioridades e os parâmetros de desempenho para o tráfego de dados. Em seguida, o identificador da sessão PDU é incluído, servindo como um rótulo único para a sessão, facilitando a gestão e o monitoramento dos fluxos de dados. Além disso, a mensagem contém as informações do túnel GTPU, que especificam os detalhes necessários para o roteamento do tráfego de dados de *uplink* dentro da infraestrutura da rede. Por fim, a mensagem inclui a aceitação do estabelecimento da sessão PDU NAS, que confirma a aprovação do estabelecimento da sessão PDU pela camada NAS e permite a continuação do processo de configuração. Com base em um conjunto de políticas internas, algumas configurações específicas e os perfis de QoS recebidos, a N3IWF determina quantas associações seguras IPSec *derivadas* da associação inicial são estabelecidas. A N3IWF define os perfis de QoS associados a cada uma dessas associações seguras adicionais que são estabelecidas.
- **2.10** - A N3IWF envia uma solicitação IKE para a criação de uma associação segura filha, com o objetivo de estabelecer a primeira associação segura IPSec derivada para a sessão PDU. Essa solicitação inclui diversos parâmetros para a configuração adequada da sessão, como, por exemplo, os identificadores de fluxo de QoS, que são essenciais para definir os parâmetros de QoS associados ao tráfego de dados encapsulado pela associação IPSec filha. Esses identificadores de QoS garantem que o tráfego seja tratado conforme os requisitos de qualidade previamente definidos, como prioridade, latência e largura de banda. Além disso, a solicitação contém o identificador da sessão PDU, que serve como um identificador único para a sessão, facilitando a gestão e o monitoramento dos fluxos de dados associados a essa sessão específica. Esse identificador é fundamental para a organização e o rastreamento das sessões dentro da infraestrutura de rede. A solicitação inclui o endereço IP do plano de dados do usuário, associado à IPSec filha, o que é necessário para o roteamento adequado do tráfego de dados entre o UE não 3GPP e o núcleo 5G.
- **2.11** - Após aceitar a solicitação enviada pela N3IWF, o UE não 3GPP envia uma resposta de criação de associação segura IPSec filha. Uma vez recebido o *aceite*, a N3IWF procede com o estabelecimento de associações seguras IPSec filhas adicionais, conforme determinado pelas políticas e configurações pré-definidas. Cada uma dessas associações filhas estabelecidas é associada a um ou mais identificadores de fluxo de QoS, que definem os parâmetros de qualidade de serviço para os diferentes tipos de tráfego de dados. Esses identificadores são relevantes para garan-

tir que o tráfego encapsulado pelas associações IPSec receba o tratamento adequado em termos de prioridade, largura de banda e latência, conforme os requisitos específicos de cada aplicação ou serviço que está utilizando o acesso viabilizado pelo UE não 3GPP. Além disso, cada associação IPSec filha é vinculada a um endereço IP do plano de dados do usuário, que é atribuído pela UPF, responsável por atender as requisições do UE não 3GPP, e utilizado para o roteamento eficiente e seguro dos dados entre o UE não 3GPP e a infraestrutura da rede 5G. Esse processo de associação permite que o tráfego de dados seja gerido de forma organizada e segura, garantindo que cada fluxo de dados siga o caminho apropriado e receba o tratamento de QoS correspondente.

- **2.12** - Após o estabelecimento de todas as associações seguras IPSec filhas, a N3IWF encaminha a mensagem de *aceite*, relacionada ao estabelecimento da sessão PDU, para o UE não 3GPP através da associação de segurança IPSec de sinalização, construída pelos procedimentos ilustrados na Figura 4.9. Este procedimento é responsável por habilitar o início da transmissão de dados de *uplink*. A mensagem de aceite do estabelecimento da sessão PDU confirma que todos os recursos necessários foram configurados com sucesso e que a sessão está pronta para operar. A utilização da associação IPSec de sinalização para o encaminhamento desta mensagem garante que as informações de controle sejam transmitidas de maneira segura e íntegra, protegendo contra possíveis interceptações e modificações durante o processo de comunicação. Ao receber esta mensagem, o UE não 3GPP é notificado de que pode iniciar a transmissão de dados de *uplink*, assegurando que todos os parâmetros de QoS e de segurança estão devidamente configurados e operacionais. Este fluxo de trabalho garante a robustez e a eficiência da comunicação na rede 5G, permitindo que os usuários desfrutem de um serviço de alta qualidade com segurança aprimorada.
- **2.13 a 2.15** - A N3IWF envia uma resposta de configuração de recursos da sessão PDU, através da interface N2, para a AMF. Esta resposta inclui informações sobre o túnel GTPU, permitindo a execução de procedimentos adicionais, semelhantes aos do estabelecimento de sessão PDU em um acesso 3GPP *convencional*, conforme ilustrado na Figura 4.10. Este processo é responsável por habilitar o início da transmissão de dados de *downlink*. A inclusão das informações do túnel GTPU na resposta é fundamental para a configuração correta dos caminhos de dados no núcleo 5G, assegurando que o tráfego de *downlink* seja roteado de maneira eficiente e segura para o UE não 3GPP. A resposta enviada pelo N3IWF à AMF confirma que todos os recursos necessários para o *downlink* estão configurados e prontos para uso. Este procedimento coordena a configuração dos túneis GTPU, que são responsáveis pelo transporte de pacotes de dados entre o núcleo 5G e o UE não

3GPP, garantindo que os dados de *downlink* possam ser transmitidos com segurança e com a QoS apropriada.

A execução coordenada dos procedimentos descritos anteriormente garante que todos os recursos e parâmetros necessários para uma comunicação eficiente, segura e de alta qualidade entre UE não 3GPP e o núcleo 5G, através de uma rede de acesso *não confiável*, sejam configurados corretamente. As especificações 3GPP descrevem fluxos com procedimentos detalhados, com o objetivo de garantir a segurança, eficiência e qualidade das comunicações na rede 5G, especialmente em cenários que envolvem acessos não 3GPP [ETSI TS-123.501 2018-09, 3GPP TR-23.501 2021-12-23, TR-21.916 2024]. A capacidade da N3IWF de gerenciar e alocar recursos de forma dinâmica e precisa permite uma operação robusta e confiável da rede, atendendo aos diversos requisitos de usuários e diferentes tipos de aplicações. Ao seguir um processo semelhante ao estabelecido para acessos 3GPP, o núcleo 5G assegura que tanto os acessos 3GPP quanto os acessos não 3GPP possam operar de maneira integrada e eficiente.

4.8 Encerramento da sessão PDU

O encerramento do plano de dados do usuário de uma sessão PDU existente é resultante do encerramento da conexão através da interface NWu, desencadeando, como consequência, a finalização de todas as associações seguras IPSec e do túnel GTPU da interface N3. A conexão do plano de dados de usuário de diferentes sessões PDU pode ser desativada de forma independente quando um UE não 3GPP está no estado CM-CONNECTED. No entanto, se uma sessão PDU for uma sessão do tipo *sempre ativa* (e.g., *always-on PDU session*, ideal para serviços que requerem baixa latência e disponibilidade imediata, como serviços de IoT e aplicações críticas em tempo real), a SMF não deve desativar a conexão do plano de dados de usuário dessa sessão devido à inatividade. A liberação de sessões PDU através do acesso não 3GPP não implica a liberação da conexão através da interface N2 [3GPP TS-23.502 2024-03].

Dispositivos conectados ao núcleo 5G através de um acesso não 3GPP *não confiável* não possuem suporte a *paging*. Portanto, quando o AMF recebe uma mensagem correspondente a uma sessão PDU para um UE não 3GPP em estado CM-IDLE para acesso, um procedimento de solicitação de serviço acionado pela rede pode ser executado sobre o acesso 3GPP, independentemente do estado do UE para o acesso 3GPP. Além disso, um procedimento de solicitação de serviço acionado pela rede sobre o acesso não 3GPP pode ser realizado para um UE não 3GPP em estado CM-IDLE para acesso 3GPP e em estado CM-CONNECTED para acesso não 3GPP na AMF, quando o *paging* sobre o acesso 3GPP não é realizado [3GPP TS-23.502 2024-03].

A desativação independente das conexões de plano de dados de usuário para diferentes sessões PDU permite uma gestão mais eficiente dos recursos de rede, especialmente em cenários onde múltiplas sessões PDU coexistem e possuem diferentes requisitos de atividade. A manutenção das sessões *sempre ativas* assegura que serviços críticos, ou que necessitam de alta disponibilidade, permaneçam operacionais, mesmo em períodos de inatividade aparente. A limitação de *paging* em redes de acesso não confiáveis é compensada por mecanismos de solicitação de serviço acionados pela rede, garantindo que a comunicação com o UE não 3GPP possa ser restabelecida de maneira eficiente [3GPP TS-23.502 2024-03]. Este procedimento é particularmente importante para assegurar a continuidade do serviço e a responsividade da rede, mesmo quando o UE não 3GPP está em diferentes estados de conectividade para acessos 3GPP e não 3GPP.

Plano de dados do usuário

Após a conclusão do estabelecimento da sessão PDU e a criação das associações seguras IPSec derivadas do plano de dados do usuário entre UE não 3GPP e N3IWF, o UE não 3GPP pode iniciar o envio de tráfego de *uplink* e *downlink* para a sessão. Este tráfego, que pode envolver vários fluxos de QoS, é transmitido através da rede de acesso *não confiável*, utilizando as IPSecs derivadas, bem como o túnel GTPU que interliga N3IWF e a UPF [3GPP TS-23.502 2024-03]. Este canal de comunicação é ilustrado no final da Figura 4.10.

A criação bem-sucedida das associações seguras IPSec filhas garante que o tráfego de dados entre o UE não 3GPP e o N3IWF seja protegido contra interceptações e adulterações, garantindo a integridade e a confidencialidade dos dados transmitidos. Cada fluxo de QoS, definido pelos identificadores de fluxo, é tratado de acordo com seus requisitos específicos de prioridade, latência e largura de banda, proporcionando uma experiência de serviço consistente e de alta qualidade [3GPP TS-23.502 2024-03]. Implementações de N3IWF, como a disponibilizada pelo free5GC [free5GC 2022], são estruturadas sob o sistema operacional Linux [Linux Foundation 2024] e fazem uso intenso das interfaces XFRM no contexto de tráfego seguro [XFRM Linux Kernel 2024]. O XFRM é um subsistema do *kernel* Linux que implementa a camada de transformação IPSec. As interfaces XFRM são usadas para configurar e gerenciar a política de segurança e os estados de IPSec entre o UE não 3GPP e o N3IWF.

O túnel GTPU, que interliga N3IWF e UPF, facilita o roteamento eficiente do tráfego de dados, assegurando que os pacotes de dados sejam encaminhados corretamente dentro da infraestrutura da rede 5G. Este mecanismo de tunelamento permite a integração transparente do tráfego proveniente da rede de acesso *não confiável* com o núcleo da rede 5G, mantendo a consistência e a eficiência na entrega dos serviços.

A combinação das associações seguras IPSec e do túnel GTPU estabelece uma infraestrutura robusta e segura para a transmissão de dados na rede 5G, permitindo que o UE não 3GPP utilize diversos serviços e aplicações com garantias de qualidade de serviço e segurança, mesmo ao operar em ambientes de rede não confiáveis.

Tráfego de *uplink*

O tráfego de *uplink* parte do UE não 3GPP em direção à UPF. Quando o UE não 3GPP precisa executar tráfego de *uplink*, ele deve determinar o identificador de fluxo de QoS associado à PDU, utilizando as regras de QoS da sessão PDU correspondente. Em seguida, o UE não 3GPP deve encapsular a PDU dentro de um pacote GRE, incluindo o valor do identificador de QoS no cabeçalho do pacote GRE. Posteriormente, o UE não 3GPP deve encaminhar o pacote GRE para a N3IWF através da associação segura IPSec filha, associada ao identificador de QoS, encapsulando o pacote GRE em um pacote IPSec no modo túnel, com o endereço IP de origem sendo o endereço IP do UE não 3GPP e o endereço de destino sendo o endereço IP do plano de dados do usuário, fornecido pela UPF e relacionado à associação segura IPSec filha [3GPP TS-24.501 2024-04, 3GPP TS-23.502 2024-03].

Quando o N3IWF recebe a PDU de *uplink*, ela *desencapsula* o cabeçalho IPSec e o cabeçalho GRE para determinar o identificador do túnel GTPU correspondente à sessão de PDU. A N3IWF deve, então, encapsular a PDU de *uplink* dentro de um pacote GTPU, incluindo o valor do identificador de QoS no cabeçalho do pacote GTPU, e encaminhar o pacote GTPU para a UPF através da interface N3, permitindo a continuidade do tráfego de dados na rede 5G [3GPP TS-24.501 2024-04, 3GPP TS-23.502 2024-03].

Tráfego de *downlink*

O tráfego de *downlink* parte da UPF em direção ao UE não 3GPP. Quando a N3IWF recebe um PDU de *downlink* da UPF através da interface N3, ela *desencapsula* o cabeçalho GTPU e utiliza o identificador de fluxo de QoS e o identificador da sessão PDU presentes no cabeçalho GTPU para determinar qual é a associação segura IPSec filha apropriada para enviar o PDU de *downlink* através da interface NWu para o UE não 3GPP [3GPP TS-24.501 2024-04, 3GPP TS-23.502 2024-03].

Após determinar a associação IPSec adequada, a N3IWF encapsula o PDU de *downlink* dentro de um pacote GRE, incluindo o valor do identificador de QoS no cabeçalho do pacote GRE. A N3IWF pode incluir, também, um indicador QoS do tipo *reflexivo* no cabeçalho GRE, que será utilizado pelo UE não 3GPP para habilitar a QoS *reflexiva*, ajustando a qualidade do serviço com base no tráfego recebido [3GPP TS-24.501 2024-04, 3GPP TS-23.502 2024-03]. A QoS *reflexiva* é um mecanismo

que permite que UEs ajustem automaticamente a QoS para os fluxos de *uplink*, com base nas características dos fluxos de *downlink*. Isso é particularmente útil para garantir que a QoS aplicada aos dados enviados esteja alinhada com a QoS dos dados recebidos, sem necessidade de configuração manual ou sinalização adicional [3GPP TS-23.502 2024-03].

Em seguida, a N3IWF encaminha o pacote GRE, contendo o PDU de *downlink*, para o UE não 3GPP através da associação IPSec vinculada ao identificador de QoS. Este encaminhamento é realizado encapsulando o pacote GRE em um pacote IP em modo túnel, onde o endereço de origem é o endereço IP do plano de dados do usuário, disponibilizado pela UPF, e o endereço de destino é o endereço IP do UE não 3GPP [3GPP TS-24.501 2024-04, 3GPP TS-23.502 2024-03].

A arquitetura apresentada ao longo deste capítulo demonstra uma abordagem viável para a integração de tecnologias de comunicação sem fio não 3GPP com o núcleo 5G. Fundamentada nos lançamentos mais recentes do 3GPP, a arquitetura utiliza funções críticas, como a N3IWF, para viabilizar o caminho de acesso *não confiável*. Com a integração entre diferentes interfaces e protocolos, a arquitetura assegura que o tráfego de dados seja transmitido de maneira eficiente, mesmo em ambientes de rede *não confiáveis*. Ao basear-se nas especificações mais recentes do 3GPP, a arquitetura promove uma maior flexibilidade na conectividade, assegurando, ainda, que a solução esteja alinhada com as tendências e demandas atuais do mercado, oferecendo um alto nível de interoperabilidade e desempenho.

Este capítulo forneceu uma análise abrangente da arquitetura convergente proposta por esta tese, abordando a integração de tecnologias de comunicação sem fio não 3GPP com o núcleo 5G. Através de diagramas e descrições detalhadas, foram explorados os principais componentes e interfaces que sustentam a integração entre o UE não 3GPP e a N3IWF. Foram discutidos os desafios de segurança, autenticação e qualidade de serviço, com a introdução de soluções que garantem a comunicação confiável entre o UE não 3GPP e o núcleo 5G. A arquitetura apresentada não apenas considera a estruturação de planos de controle e dados, mas também aborda a implementação de mecanismos como túneis IPSec para assegurar a transmissão segura de dados. O desenvolvimento de um UE não 3GPP foi destacado como uma contribuição inovadora desta tese, permitindo o acesso seguro ao núcleo 5G a partir de redes não confiáveis, algo que até então não tinha sido realizado de forma prática. Além disso, foram detalhados os procedimentos de registro, autenticação, autorização e estabelecimento de sessões PDU, ressaltando a importância da coleta de métricas para monitoramento de redes não 3GPP. No próximo capítulo, será apresentada uma implementação de protótipo, que visa validar a arquitetura convergente. Este protótipo permite uma análise prática dos conceitos teóricos abordados, fornecendo informações adicionais sobre seu desempenho e possíveis melhorias. A implementação detalhada inclui a configuração dos componentes principais, testes de integração e resul-

tados obtidos, oferecendo uma visão abrangente de como a arquitetura pode ser aplicada em cenários reais.

CAPÍTULO 5

Protótipo de arquitetura convergente

Este capítulo apresenta a implementação de um protótipo para a arquitetura convergente, com o objetivo de validar a viabilidade da integração entre tecnologias de comunicação sem fio não 3GPP e o núcleo 5G. Neste capítulo, são expostos os componentes essenciais e as etapas envolvidas na construção desse protótipo, destacando as funcionalidades específicas que foram desenvolvidas, os desafios enfrentados durante o processo, e as soluções implementadas. O foco principal reside na criação de artefatos de software que permitam o acesso ao núcleo 5G por meio de redes de acesso não 3GPP, garantindo flexibilidade e segurança na comunicação entre dispositivos que operam em diferentes padrões de rede. Além disso, este capítulo visa fornecer uma base prática para futuras implementações e aprimoramentos na área de telecomunicações, criando um alicerce para a aplicação e teste de novas soluções que busquem aprimorar a convergência de tecnologias de rede em um ambiente pós-5G.

5.1 Definição do núcleo 5G

A arquitetura convergente é composta por elementos que possuem algum tipo de implementação de código aberto (e.g., funções do núcleo 5G, como UPF, SMF, AMF e N3IWF) e por componentes que, embora especificados, ainda não foram implementados. Para a estruturação do protótipo da arquitetura convergente, a escolha das tecnologias e ferramentas foi feita com base na robustez, flexibilidade e suporte das soluções de código aberto disponíveis. Entre as implementações de núcleo 5G de código aberto mais relevantes atualmente, destacam-se o *free5GC* [free5GC 2022], *Open5GS* [Open5GC 2019], *MAGMA* [Linux Foundation 2023], *Open Air Interface Core* [Open Air Interface 2023] e *SRSRAN* [srsRAN 2023].

Cada uma das soluções de núcleo 5G, consideradas no escopo desta tese, possui características específicas e foi avaliada de acordo com os critérios descritos na Tabela 5.1. A escolha pelo *free5GC* deve-se, principalmente, à existência da implementação da N3IWF, já disponível desde a versão 3.0 [free5GC 2022]. Além disso, o *free5GC* é amplamente reconhecido por sua arquitetura modular, que facilita a integração de novos

componentes e a realização de testes personalizados. Em comparação, o *Open5GS*, embora seja robusto e amplamente utilizado, ainda carece de uma implementação madura da N3IWF. Da mesma forma, o *MAGMA*, apesar de ser uma plataforma poderosa para redes de acesso distribuído, não oferece suporte tão extensivo para funcionalidades específicas do núcleo 5G, como a N3IWF. As soluções *Open Air Interface Core* e *SRSRAN* são mais voltadas para o desenvolvimento e testes de camadas físicas e de rádio, sendo menos adequadas para as necessidades específicas de um núcleo de rede centralizado. Portanto, a escolha pelo *free5GC* foi fundamentada na sua capacidade de atender diretamente aos requisitos do protótipo, oferecendo uma implementação funcional e extensível das funções essenciais do núcleo 5G, incluindo a N3IWF.

Tabela 5.1: Critérios para escolha do núcleo 5G para compor protótipo de arquitetura convergente

5GC	N3IWF	Atividade	Modularidade	Documentação
free5GC	●	●	●	●
MAGMA	○	◓	◓	◓
Open5GS	○	●	◓	●
Open Air Interface Core	○	◓	◓	●
SRSRAN	○	◓	○	◓

A Tabela 5.1 ilustra os critérios que foram considerados na escolha do núcleo 5G para compor o protótipo de arquitetura convergente. Além da existência da implementação da N3IWF, foram considerados o nível de atividade por parte da comunidade de desenvolvedores de projetos de código aberto, no que diz respeito à frequência de *commits* e ao tempo de resposta a *Issues* [1], à maturidade da arquitetura utilizada na estruturação do projeto, no que diz respeito à possibilidade de modularização e extensão dos microsserviços, e, finalmente, o volume e a qualidade da documentação disponível para dar suporte ao desenvolvimento de novas funcionalidades e à utilização da solução.

5.2 Implementação do acesso não confiável ao núcleo 5G

Após definir qual implementação de núcleo 5G utilizar na estruturação do protótipo da arquitetura convergente, o passo seguinte está associado à implementação do artefato de software responsável por provisionar os procedimentos de registro, autenticação e estruturação da sessão de PDU. O acesso ao núcleo é viabilizado pelo UE não 3GPP. Este elemento da arquitetura foi desenvolvido inicialmente em linguagem Go[2] [Google 2022]

[1] Em um projeto de código aberto, uma *Issue* é um item de rastreamento usado para documentar e gerenciar tarefas, *bugs*, solicitações de funcionalidades e discussões relacionadas ao desenvolvimento do software.

[2] https://github.com/LABORA-INF-UFG/UE-non3GPP

para plataformas Linux. O desenvolvimento em Go permite um processamento eficiente e uma fácil integração com sistemas Linux.

Inicialmente, a arquitetura do UE não 3GPP foi projetada para se conectar ao núcleo da rede 5G através da função N3IWF, considerando o caminho não 3GPP *não confiável*. O UE não 3GPP implementa todos os procedimentos e protocolos necessários para estabelecer os canais de comunicação, incluindo os procedimentos de configuração inicial do túnel IPSec, os procedimentos associados à autenticação, utilizando EAP e a negociação de chaves de segurança.

O desenvolvimento em Go [Google 2022] envolveu a criação de módulos para gerenciar as diferentes etapas da conexão com a N3IWF. Esses módulos incluem a inicialização do dispositivo, a execução dos procedimentos de registro e autenticação, e a manutenção do túnel IPSec para a transmissão de dados. Cada módulo foi projetado para ser extensível, permitindo futuras adaptações e melhorias. A escolha pelo Go se mostrou vantajosa, devido à seu desempenho e capacidade de gerenciamento de concorrência, essenciais para garantir que o UE não 3GPP possa lidar com múltiplas conexões e tráfego de dados simultaneamente. Além disso, a possibilidade de implantar uma versão do UE não 3GPP implementado em Go em uma plataforma baseada em Linux de baixo custo, como, por exemplo, em um Veículo Aéreo não Tripulado (VANT) ou alguma plataforma de hardware de computação embarcada executando mais próximo da borda (e.g., Raspberry Pi), é bastante promissora. Essas plataformas, além de serem significativamente mais baratas do que implantar BSs para ampliar a cobertura da rede 5G, oferecem flexibilidade e escalabilidade na infraestrutura de rede. Utilizando Go, que é eficiente em termos de desempenho e gerenciamento de concorrência, tem-se a possibilidade de utilizar o UE não 3GPP em ambientes de borda, onde os recursos de hardware são limitados. A modularidade e extensibilidade dos artefatos de software desenvolvidos permitem que essas soluções se adaptem facilmente às necessidades específicas de cada aplicação, proporcionando uma infraestrutura de comunicação econômica e eficiente. Isso é especialmente importante para cenários como os de VANTs, que frequentemente operam em áreas remotas ou de difícil acesso, e para hardware de computação embarcada, que pode ser utilizado em projetos de baixo custo para expandir a cobertura e capacidade da rede 5G.

A implementação do UE não 3GPP, devidamente integrada com as funcionalidades do free5GC [free5GC 2022], viabiliza a estruturação do protótipo da arquitetura convergente. A implementação dos procedimentos de segurança envolve a utilização de protocolos como IKE-v2 e EAP-5G, juntamente com algoritmos de criptografia robustos como *Advanced Encryption Standard with a 256-bit key in Cipher Block Chaining* (AES-CBC) e *Hash-based Message Authentication Code Secure Hash Algorithm 1-96* (HMAC-SHA1-96). Bibliotecas utilitárias como **`netlink`** para configuração de rede e **`github.com/free5gc/nas`** para manipulação de mensagens NAS complementam

as diretrizes especificadas pelo 3GPP e foram utilizadas durante a etapa de implementação. O acesso ao código-fonte, bem como a toda a documentação do UE não 3GPP, foi devidamente disponibilizado em um repositório GitHub [3], sendo um dos entregáveis desta tese.

Todo o processo de desenvolvimento do UE não 3GPP foi conduzido com base em boas práticas de engenharia de software, especialmente no que diz respeito à parametrização, visando tornar a solução mais flexível e apta a adaptações futuras. A configuração é parametrizada a partir de arquivos *YAML Ain't Markup Language* (YAML), o que facilita o uso e a customização conforme as necessidades específicas. Essa abordagem promove a reutilização e a modularidade do código, além de simplificar a manutenção e a atualização, possibilitando ajustes rápidos e eficientes sem a necessidade de alterações complexas no código-fonte. A responsabilidade de cada um dos parâmetros configuráveis é detalhada nas seções a seguir, proporcionando uma compreensão de como cada aspecto do sistema pode ser ajustado para atender aos requisitos específicos de operação e desempenho.

5.3 Parâmetros de configuração para acesso não 3GPP ao núcleo 5G

A configuração do UE não 3GPP é realizada de forma desacoplada, possibilitando maior flexibilidade e facilidade na utilização. Os parâmetros de configuração são utilizados nos procedimentos de autenticação, registro e estabelecimento de sessão de PDU. Os parâmetros contidos no arquivo de configuração **`config/config.yaml`** foram agrupados em tabelas, seguindo como critério, a responsabilidade de cada um deles durante a estruturação do acesso não 3GPP *não confiável*. A Tabela 5.2 apresenta os parâmetros utilizados nos procedimentos de autenticação do UE não 3GPP no núcleo 5G. Os valores atribuídos a cada um dos parâmetros são utilizados para gerar os vetores de autenticação necessários para os procedimentos de registro e estruturação dos canais de comunicação segura.

A Tabela 5.3 detalha os parâmetros utilizados nos procedimentos de identificação e registro do UE não 3GPP no núcleo 5G. Os valores atribuídos a cada um dos parâmetros da tabela são responsáveis por identificar o UE dentro de uma rede móvel, e estão diretamente relacionados aos tipos de procedimentos de autenticação que serão executados pelo núcleo.

[3] https://github.com/LABORA-INF-UFG/UE-non3GPP

Tabela 5.2: Parâmetros de autenticação do UE não 3GPP no núcleo 5G

Parâmetro	Descrição
permanentkeyvalue	O valor atribuído a este parâmetro é a chave permanente do usuário, utilizada em conjunto com o valor de sequência (**sequencenumber**) e os parâmetros de operadores (**opcvalue** e **opvalue**) para gerar os vetores de autenticação, após a execução dos procedimentos de registro. Este valor é essencial para o correto funcionamento dos procedimentos de segurança da autenticação baseada em *Authentication and Key Agreement* (AKA) e deve ser equivalente ao valor armazenado na coleção **authenticationSubscription** da base de dados do free5GC [MongoDB Inc 2024].
opcvalue e **opvalue**	Os valores contidos nestes parâmetros são utilizados para derivar a chave de autenticação. O **opcvalue** (Operator Code) é um valor derivado da **opvalue** (Operator Key) e da chave permanente. Ambos são utilizados para calcular os vetores de autenticação.
sequencenumber	O valor contido neste atributo é utilizado para sincronizar o UE não 3GPP e o núcleo da rede 5G durante o procedimento de autenticação. Ele garante que as tentativas de autenticação sejam protegidas contra ataques de repetição.

Tabela 5.3: Parâmetros para identificação e registro do UE não 3GPP no núcleo 5G

Parâmetro	Descrição
msin	O *Mobile Station Identification Number* (MSIN) é um identificador exclusivo de um UE dentro de uma determinada rede móvel. Ele é combinado com o código de rede para formar o *International Mobile Subscriber Identity* (IMSI), usado durante os procedimentos de registro. O valor contido neste parâmetro deve ser equivalente ao valor armazenado na coleção **authenticationSubscription** da base de dados do free5GC [MongoDB Inc 2024]
hplmn	O HPLMN é composto pelo MCC e pelo MNC. Esses códigos identificam a rede doméstica do UE não 3GPP e são utilizados para autenticação e registro.
ranuengapid e **amfuengapid**	Esses parâmetros identificam de forma única o UE não 3GPP no contexto da rede de acesso e do AMF. São utilizados durante o registro e a manutenção da conexão com o núcleo 5G.
authmngfield	Este campo é utilizado para gerenciar a autenticação do UE não 3GPP, especificando a versão e o tipo de procedimentos de autenticação a serem aplicados.

A Tabela 5.4 descreve os parâmetros de identificação de endereços IP e nomenclatura das interfaces de rede do UE não 3GPP. A nomenclatura das interfaces de rede responsáveis por: (i) encapsular o tráfego de dados entre o UE não 3GPP e o núcleo 5G, e (ii) realizar a sinalização NAS do plano de controle, são definidas tendo como base os valores atribuídos aos seus parâmetros.

Tabela 5.4: Parâmetros de identificação de endereços IP e nomenclatura das interfaces de rede para os planos de dados do usuário e de plano de controle no UE não 3GPP

Parâmetro	Descrição
`localpublicipaddr`	Este é o endereço IP público do UE não 3GPP utilizado para estabelecer a conexão inicial com a N3IWF via IKE. O valor atribuído a este parâmetro é relevante para a configuração e manutenção de túneis seguros.
`localportudpconn`	Este parâmetro contém a porta UDP pública utilizada pelo UE não 3GPP para a conexão IKE com a N3IWF. Esta porta é padrão para comunicações IKE-v2.
`greinterface`	O valor armazenado neste parâmetro será utilizado para nomear a interface GRE, configurada para encapsular o tráfego de dados entre o UE não 3GPP e o núcleo 5G. O nome da interface e o *Maximum Transmission Unit* (MTU) são especificados para garantir uma comunicação eficiente.
`ipsecinterface`	A interface IPSec é utilizada para criar um túnel seguro entre o UE não 3GPP e o N3IWF. O nome da interface, a marcação **`mark`** e o MTU são especificados para a correta configuração e operação da interface de tunelamento.

A Tabela 5.5 descreve parâmetros cujos valores estão associados à identificação de fatias de rede e da sessão PDU do UE não 3GPP. Os valores atribuídos são utilizados durante a execução de procedimentos para gerenciar sessões de dados entre o UE não 3GPP e o núcleo 5G.

Finalmente, os valores atribuídos aos parâmetros da Tabela 5.6 identificam a N3IWF à qual o UE não 3GPP se conecta. Os valores atribuídos ao endereço IP são utilizados para estabelecer a conexão inicial e configurar túneis para uma comunicação segura.

5.4 Parâmetros de configuração da N3IWF

Para que um UE não 3GPP consiga acessar o núcleo 5G por meio de uma rede de acesso *não confiável*, a configuração correta da N3IWF presente no free5GC [free5GC 2022] é essencial. Esta seção tem como objetivo detalhar os passos necessários para configurar a N3IWF. Aspectos fundamentais são abordados, como a configuração

Tabela 5.5: Parâmetros de identificação de fatias de rede e da sessão PDU do UE não 3GPP

Parâmetro	Descrição
snssai	Este é o endereço IP público do UE não 3GPP utilizado para estabelecer a conexão inicial com a N3IWF via IKE. O valor atribuído a este parâmetro é relevante para a configuração e manutenção de túneis seguros.
pdusessionid	Identificador da sessão de PDU, utilizado para gerenciar sessões de dados específicas entre o UE não 3GPP e a rede 5G. Cada sessão possui um ID único.
greinterface	O valor armazenado neste parâmetro é utilizado para nomear a interface GRE, configurada para encapsular o tráfego de dados entre o UE não 3GPP e o núcleo 5G. O nome da interface e o MTU são especificados para garantir uma comunicação eficiente.
dnnstring	O *Data Network Name* (DNN) especifica a rede de dados desejada pelo UE não 3GPP. O valor contido no parâmetro **dnnstring** deve representar uma das redes de dados devidamente configuradas na lista de **snssaiInfos** contida na SMF. Com base no valor contido em **dnnstring** e nos atributos que identificam as fatias de rede, o SMF definirá qual UPF será responsável por estruturar o túnel GTPU para o tráfego de dados. Este parâmetro direciona o tráfego de dados para a rede correta, conforme configurado.

Tabela 5.6: Parâmetros de identificação da N3IWF no UE não 3GPP

Parâmetro	Descrição
ikebindaddress	Este parâmetro contém o endereço IP da N3IWF utilizado para a comunicação IKE. É importante para estabelecer a conexão inicial e configurar os túneis para comunicação segura.
ikebindport	Porta IKE da N3IWF, utilizada para a comunicação IKE-v2. Esta é a porta padrão para operações de IKE.
ipsecifaceprotocol	Protocolo utilizado pela interface IPSec, normalmente UDP, para o transporte seguro de dados.

dos parâmetros de rede, autenticação e tunelamento, destacando as interações cruciais entre o N3IWF e os demais componentes do núcleo 5G, como a AMF e a UPF. A configuração das demais funções de rede que compõem o free5GC está fora do escopo deste trabalho. Entretanto, o repositório GitHub [4] contendo os experimentos desta tese, foi estruturado com base em Ansible [RedHat 2024], contemplando a configuração de

[4] https://github.com/LABORA-INF-UFG/TESE_CJAM_2024

todos os componentes do núcleo 5G. O Ansible [RedHat 2024] é uma ferramenta de automação que permite gerenciar a infraestrutura como código, facilitando a definição, provisionamento e manutenção de ambientes de forma automatizada e reproduzível.

A configuração correta da N3IWF é um pré-requisito para possibilitar o acesso não 3GPP *não confiável*. O processo envolve a definição precisa de parâmetros de configuração que devem estar alinhados com os valores esperados pelo núcleo 5G, garantindo a interoperabilidade entre as diversas tecnologias envolvidas. A seguir, cada parâmetro do arquivo de configuração da N3IWF é detalhadamente analisado, explicando sua função e destacando sua relevância na estruturação dos túneis IPSec para o tráfego de dados e sinalização de controle NAS. Após a implantação do free5GC, o arquivo de configuração da N3IWF pode ser localizado em **`n3iwf/config/n3iwfcfg.yaml`**.

Identificadores da N3IWF

- **`GlobalN3IWFID`** - Identifica globalmente a N3IWF dentro da rede.
  - **`PLMNID`** - *Public Land Mobile Network ID*, composto por:
    - **`MCC`** - Código do país, deve corresponder ao valor do MCC contido no atributo **`hplmn`** do arquivo de configuração do UE não 3GPP, apresentado na Seção 5.3.
    - **`MNC`** - Código da rede móvel, deve corresponder ao valor do MNC contido no atributo **`hplmn`** do arquivo de configuração do UE não 3GPP, apresentado na Seção 5.3.
  - **`N3IWFID`** - Identificador único da N3IWF na PLMN.
- **`Name`** - Nome atribuído a instância da N3IWF, usado para identificação em *logs* e monitoramento durante a execução dos procedimentos registro, autenticação e autorização.
- **`SupportedTAList`** - Lista de áreas de rastreamento suportadas por esta instância de N3IWF.
  - **`TAC`** - Código da área de rastreamento, identificando a área específica atendida.
  - **`BroadcastPLMNList`** - Lista de redes PLMN que podem ser transmitidas nesta área.
    - **`PLMNID`** - Correspondente aos valores MCC e MNC descritos anteriormente.
    - **`TAISliceSupportList`** - Lista de slices de rede suportados:
      - **`SNSSAI`** - A *Single Network Slice Selection Assistance Information* (S-NSSAI) é usada para identificar uma fatia de rede específica. O

Slice/Service Type (SST) e o *Slice Differentiator* (SD) são valores hexadecimais que especificam a fatia de serviço e o diferenciador de fatia, respectivamente. Deve corresponder ao valor contido no atributo **`snssai`** do arquivo de configuração do UE não 3GPP, apresentado na Seção 5.3.

Endereços IP e interfaces de acesso

- **`AMFSCTPAddresses`** - Lista de endereços IP da interface N2 no AMF para conexão NGAP através de uma porta previamente configurada. Por padrão a porta para sinalização NGAP é a 38412 [ETSI TS-138.412 2018].
- **`IKEBindAddress`** - Endereço IP da interface Nwu IKE na N3IWF, utilizado para inicialização e gerenciamento de chaves de segurança. Deve corresponder ao valor contido no atributo **`ikebindaddress`** do arquivo de configuração do UE não 3GPP, apresentado na seção 5.3.
- **`IPSecInterfaceAddress`** - Endereço IP da interface IPSec, ponto de extremidade do túnel IPSec do lado da N3IWF.
- **`UEIPAddressRange`** - Faixa de endereços IPs que são alocados aos UEs não 3GPP dentro do túnel IPSec, garantindo que cada UE não 3GPP tenha um endereço IP exclusivo para a comunicação.
- **`IPSecInterfaceMark`** - Identificador de marcação da interface IPSec, utilizado para identificação e roteamento dentro das políticas de segurança através de XFRM [XFRM Linux Kernel 2024] para controle de estados de IPSec no *kernel* Linux.
- **`GTPBindAddress`** - Endereço IP da interface N3 *General Packet Radio Service Tunneling Protocol* (GTP) na N3IWF, utilizado para encaminhamento de pacotes de dados GTP.
- **`NASTCPPort`** - Porta TCP onde o processo de sinalização NAS ocorre, permitindo a sinalização controle de mensagens NAS entre UE não 3GPP e N3IWF.
- **`FQDN`** - Nome de domínio totalmente qualificado da N3IWF, utilizado nas requisições internas da arquitetura SBA para identificação e autenticação.

Identificadores de segurança

- **`PrivateKey`** - Caminho para o arquivo da chave privada, utilizada para criptografia e autenticação de mensagens.
- **`CertificateAuthority`** - Caminho para o arquivo da autoridade certificadora, necessário para validar certificados.
- **`Certificate`** - Caminho para o arquivo do certificado da N3IWF, utilizado para estabelecer conexões seguras.

Os parâmetros de configuração são críticos para assegurar a correta operação e segurança das comunicações entre o UE não 3GPP e o núcleo 5G. Parâmetros como **`PLMNID`**, **`vIKEBindAddress`**, **`IPSecInterfaceAddress`** e **`PrivateKey`** são diretamente envolvidos na autenticação, gerenciamento de chaves e estabelecimento de túneis IPSec. A coerência desses parâmetros com os valores configurados no UE não 3GPP é essencial para garantir que as chaves AKA sejam corretamente derivadas e que os túneis IPSec sejam estabelecidos com sucesso, permitindo o tráfego seguro de dados e sinalização NAS entre o UE não 3GPP e o núcleo 5G.

A configuração detalhada dos parâmetros do UE não 3GPP e da N3IWF é fundamental para assegurar uma integração eficiente e segura com o núcleo 5G, permitindo a comunicação através de redes de acesso não confiáveis. Compreender a função de cada parâmetro e a importância da coerência entre os valores configurados no UE não 3GPP e na N3IWF é relevante para a implementação bem-sucedida de soluções de rede avançadas.

5.5 Estatísticas das interfaces de rede no acesso *não confiável*

A implementação de um serviço de API para coleta de métricas no protótipo da arquitetura convergente proporciona uma visão detalhada do desempenho e do status da rede, permitindo uma melhor gestão e monitoramento. Adicionalmente, uma API para coleta de métricas das interfaces de rede do UE não 3GPP é uma contribuição relevante para pesquisas científicas no âmbito das telecomunicações, especialmente considerando a aplicação de IA em telecomunicações e a notória demanda por *datasets* para o treinamento desses modelos. A implementação do UE não 3GPP possui um mecanismo de coleta de métricas que define algumas rotas de API para coletar e retornar informações sobre o status da rede, vazão e o estado das conexões do UE não 3GPP. A seguir, as funções e procedimentos envolvidos são detalhadas, bem como os protocolos, algoritmos e bibliotecas utilitárias utilizados.

Rotas de API

As rotas de API são configuradas utilizando o *Gin Web Framework* [Team 2024], que facilita a criação de roteadores HTTP eficientes. O serviço de API define quatro principais *handlers* para coletar diferentes tipos de métricas:

- **`controller.NewNetworkStatustHandler`** - Configura a rota para coleta do status da rede.

- **`controller.NewNetworkThroughputHandler`** - Configura a rota para monitoramento da taxa de transferência da rede.
- **`controller.NewNetworkThroughputHandler`** - Configura a rota para obter informações sobre a conexão do UE não 3GPP.
- **`controller.NewWiFiMetricstHandler`** - Configura a rota para obter informações sobre a conexão do UE não 3GPP em um cenário onde os túneis para os planos de dados de usuário e plano de controle foram estabelecidos através de um enlace utilizando Wi-Fi.

Cada uma dessas rotas está associada a uma função específica que processa as requisições e retorna os dados coletados. O escopo de implementação do protótipo contempla a parametrização das rotas, usando uma API para escolher qual interface de rede do UE não 3GPP é alvo da coleta de métricas (por exemplo, *GRETUN* para o plano de dados do usuário ou IPSec para sinalização do plano de controle).

Monitorando o status das interfaces de rede

A função **`controller.GetNetworkStatus`**, implementada no UE não 3GPP, coleta o status de uma interface de rede específica durante um intervalo de tempo previamente definido.

1. **Parâmetros da requisição** - A função recebe o nome da interface de rede (**`interface`**) e o intervalo (**`interval`**) como parâmetros da *Uniform Resource Locator* (URL). O nome da interface pode ser o nome associado à interface do túnel IPSec do plano de dados do usuário ou à interface do túnel IPSec do plano de controle. O nome das interfaces é definido dinamicamente, tomando como base os parâmetros **`ipsecinterface`** como definidos para a interface do plano de controle e **`greinterface`** como definidos para a interface do plano de dados do usuário. Ambos os parâmetros estão presentes no arquivo de configuração do UE não 3GPP apresentado na Seção 5.3. O parâmetro **`interval`** é um valor numérico inteiro que representa o tempo, em segundos, em que a métrica deve ser coletada na respectiva interface de rede.
2. **Coleta de métricas** - Utilizando o *Gin Web Framework* [Team 2024], a função coleta estatísticas de rede como *bytes* recebidos (**`BytesRecv`**), *bytes* enviados (**`BytesSent`**), pacotes recebidos (**`PacketsRecv`**) e pacotes enviados (**`PacketsSent`**). Essas estatísticas são coletadas repetidamente a cada segundo durante o intervalo de tempo especificado pelo parâmetro **`interval`**.
3. **Resposta JSON** - As métricas coletadas são armazenadas em uma lista de **`StatusValue`** e retornadas como resposta JSON.

Monitorando a taxa de transferência das interfaces de rede

A função **`controller.GetNetworkThroughput`**, implementada no UE não 3GPP, monitora a taxa de transferência de uma determinada interface de rede.

1. **Parâmetros da requisição** - A função recebe o nome da interface de rede (**`interface`**) e o intervalo (**`interval`**) como parâmetros da URL.
2. **Coleta e cálculo da taxa de transferência** - A função coleta estatísticas da interface de rede antes e após cada intervalo de um segundo, calculando a diferença em *bytes* recebidos e enviados para determinar a vazão de entrada (**`ThroughputIn`**) e saída (**`ThroughputOut`**).
3. **Resposta JSON** - Os valores de *throughput* são armazenados em uma lista de **`Throughput`** e retornados como resposta JSON.

Monitorando o status de conexão do UE não 3GPP

A função **`controller.GetInfoUE`**, implementada no UE não 3GPP, retorna métricas relacionadas ao estado da conexão do UE não 3GPP e o núcleo 5G.

1. **Coleta de métricas** - Utilizando os parâmetros de conexão do UE não 3GPP, a função coleta tempos de registro (**`RegisterTime`**), tempo para o estabelecimento da sessão de PDU (**`PduTime`**), tempo para o estabelecimento dos canais de segurança (**`SecurityTime`**), tempo de execução dos procedimentos de autenticação (**`AuthTime`**) e tempo para a configuração IPSec (**`IpsecTime`**).
2. **Resposta JSON** - As métricas coletadas são armazenadas em um objeto **`UeStatus`** e retornadas como resposta JSON.

Monitorando métricas das interfaces de rede Wi-Fi

A função **`controller.GetWiFiMetrics`**, implementada no UE não 3GPP, coleta métricas de uma interface de rede Wi-Fi durante um determinado intervalo de tempo e retorna essas informações em formato JSON.

1. **Parâmetros da requisição** - A função recebe o nome da interface de rede (**`interface`**) e o intervalo (**`interval`**) como parâmetros da URL.
2. **Coleta de métricas** - Durante um intervalo de tempo especificado como parâmetro, a função coleta um conjunto de métricas que incluem informações como o nome da rede, modo de operação, frequência, ponto de acesso, taxa de transmissão, potência de transmissão, qualidade do enlace, nível de sinal e nível de ruído.

3. **Resposta JSON** - As métricas coletadas são armazenadas em uma lista de `WifiMetrics` e retornadas como resposta JSON. Se o enlace entre UE não 3GPP e N3IWF não tiver sido estabelecido através de Wi-Fi, a função registra o erro e retorna uma resposta JSON com um código de status HTTP 400 (*Bad Request*), indicando que houve uma falha no procedimento de coleta.

A implementação do protótipo de arquitetura convergente demonstrou a viabilidade técnica e operacional da integração entre tecnologias de comunicação sem fio não 3GPP e o núcleo 5G, proporcionando um cenário flexível para a comunicação em redes avançadas. As etapas detalhadas de desenvolvimento e configuração mostraram como cada componente e protocolo foi integrado para garantir a segurança, desempenho e interoperabilidade necessários para uma operação eficiente. A escolha do free5GC [free5GC 2022], devido à sua modularidade e suporte robusto para N3IWF, possibilitou a criação de uma plataforma extensível e adaptável para futuras pesquisas e implementações.

A abordagem de desenvolvimento adotada, utilizando linguagens como Go e Kotlin, permitiu uma adaptação eficiente para diferentes plataformas, desde dispositivos Linux de baixo custo até dispositivos móveis Android. A modularidade e a parametrização dos artefatos de software desenvolvidos não só facilitaram a integração e configuração do protótipo, mas também abrem caminhos para personalizações e melhorias futuras. A capacidade de coletar métricas detalhadas de desempenho e status das interfaces de rede reforça a utilidade prática do protótipo, oferecendo uma base sólida para o monitoramento e gestão de redes em cenários reais de aplicação.

A documentação abrangente e a disponibilização do código-fonte no repositório GitHub[5] garantem que o trabalho desenvolvido possa ser replicado, avaliado e aprimorado por outros pesquisadores e profissionais da área. Este protótipo não apenas valida as teorias discutidas, mas também serve como base para avanços significativos na integração de tecnologias não 3GPP com o núcleo 5G, contribuindo para a evolução das telecomunicações e para a implementação de soluções de rede mais eficientes e acessíveis.

Este capítulo apresentou uma análise detalhada da implementação de um protótipo de arquitetura convergente proposta por esta tese, com o objetivo de validar a integração entre tecnologias de comunicação sem fio não 3GPP e o núcleo 5G. O capítulo explorou a escolha do núcleo 5G, destacando as características do free5GC [free5GC 2022], principalmente sua modularidade e suporte robusto à função N3IWF, em comparação com outras soluções de núcleo 5G, implementadas em código aberto. A implementação do acesso não confiável ao núcleo 5G foi explicada em profundidade, incluindo o desenvolvimento do UE não 3GPP. O capítulo também destacou a configuração dos parâmetros

[5] https://github.com/LABORA-INF-UFG/TESE_CJAM_2024

críticos, tanto para o UE não 3GPP quanto para a N3IWF, visando garantir uma comunicação segura e eficiente. As funções de autenticação, tunelamento IPSec e os protocolos de segurança como IKE-v2 e EAP-5G foram implementados para assegurar a integridade e confidencialidade da comunicação. Além disso, o protótipo oferece uma API para coleta de métricas das interfaces de rede, o que reforça sua aplicabilidade em ambientes reais e sua utilidade em pesquisas futuras. O código desenvolvido e documentado foi disponibilizado no GitHub, permitindo que outros pesquisadores repliquem e aprimorem o trabalho. No próximo capítulo, as funcionalidades são apresentadas em casos de uso práticos, demonstrando a operação do UE não 3GPP em vários cenários. Através de exemplos reais, é possível observar a aplicação prática das configurações descritas, bem como avaliar a viabilidade e o desempenho da arquitetura convergente em diferentes contextos de rede.

CAPÍTULO 6

Metodologia e resultados experimentais da integração do UE não 3GPP com núcleo 5G

Este capítulo apresenta os resultados experimentais obtidos a partir da integração do UE não 3GPP com o núcleo 5G, abordando a metodologia aplicada e os resultados práticos alcançados. A implementação do protótipo serviu como base para os experimentos detalhados, proporcionando um ambiente realista para a validação das funcionalidades e da viabilidade da arquitetura convergente. Múltiplos testes em ambientes controlados foram realizados, abrangendo desde a implantação e configuração dos componentes da arquitetura, até a avaliação da conectividade, desempenho de vazão e monitoramento das redes de acesso não 3GPP, como Wi-Fi. Através desses experimentos, foi possível explorar como a integração entre tecnologias 3GPP e não 3GPP pode ser aprimorada, destacando os principais desafios e soluções implementadas. Adicionalmente, alguns dos experimentos foram realizados no âmbito do projeto Brasil 6G [Inatel, MCTI e RNP 2024], cujo principal objetivo é definir os passos necessários para que a futura geração de redes móveis seja capaz de atender às aplicações e casos de uso importantes para o desenvolvimento econômico e social do país.

Para assegurar a robustez dos resultados, adotou-se uma metodologia experimental, envolvendo múltiplos testes em ambientes controlados. Cada experimento foi projetado para avaliar aspectos específicos da integração, incluindo o passo a passo da implantação do protótipo, a validação da conectividade dos componentes após a implantação, a latência de comunicação, a coleta de métricas das interfaces de rede, a estabilidade das conexões e a eficiência na transmissão de dados. A utilização de ferramentas de monitoramento e coleta de métricas permitiu uma análise detalhada dos parâmetros de desempenho. Os resultados apresentados neste capítulo fornecem uma visão abrangente do desempenho do UE não 3GPP, quando integrado ao núcleo 5G através de redes de acesso *não confiáveis*, destacando os principais desafios enfrentados e as soluções implementadas para superá-los. A análise dos dados coletados nos experimentos permitiu uma compreensão profunda dos benefícios e limitações da arquitetura convergente, além de oferecer *insights* para futuras melhorias e pesquisas na área de telecomunicações.

6.1 Metodologia de implantação e configuração dos componentes

Nesta seção, a metodologia de implantação dos componentes da arquitetura convergente é detalhada. A Figura 6.1 ilustra a topologia utilizada, utilizando três *Virtual Machine*s (VMs): a primeira para o provisionamento do UE não 3GPP, a segunda para o provisionamento da N3IWF, e a terceira dedicada à execução das demais funções de rede que compõem o núcleo 5G.

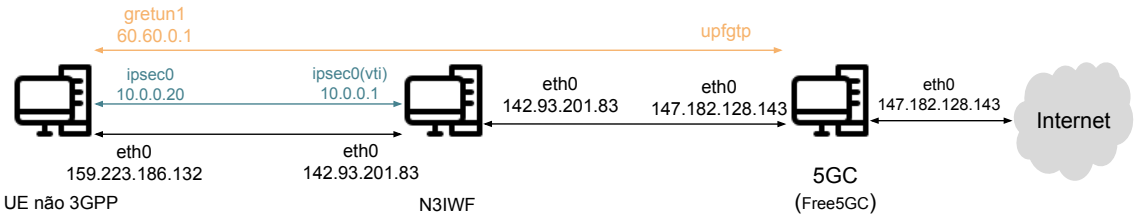

Figura 6.1: Topologia de rede utilizada na implantação do protótipo da arquitetura convergente.

Os endereços IPs ilustrados em cada uma das interfaces de rede *eth0* das VMs são dinâmicos e ilustram o momento exato da execução do experimento. As interfaces *ipsec0* e *gretun1* são construídas dinamicamente, através da execução dos procedimentos de registro, autenticação e autorização e através da execução dos procedimentos para o estabelecimento da sessão de PDU. Os IPs atribuídos a cada uma dessas interfaces possuem endereços diretamente relacionados aos parâmetros de configuração das demais funções de rede do núcleo 5G. Por exemplo, o endereço IP da interface *ipsec0*, atribuída ao UE não 3GPP, é obtido a partir de procedimentos internos da N3IWF, considerando a faixa de valores atribuída ao parâmetro **`UEIPAddressRange`**. O valor atribuído a esse parâmetro determina a faixa de endereçamento IP a ser atribuída a um determinado UE não 3GPP que queira se conectar à N3IWF. Além disso, o endereço IP da interface *gretun1*, também atribuída ao UE não 3GPP, representa o Plano de Dados do Usuário e é obtido através da UPF e devolvido ao UE não 3GPP de forma indireta pela N3IWF, através da execução de procedimentos envolvendo os microsserviços provisionados pelas funções AMF e SMF por meio da interface N2.

A topologia apresentada na Figura 6.1 é uma abordagem que visa garantir uma configuração modular e escalável, onde cada VM desempenha um papel específico no protótipo da arquitetura convergente. A escolha de um ambiente *cloud*, além de demonstrar a característica escalável do protótipo, também está associada à robustez, flexibilidade e suporte de alto desempenho desses ambientes, características essenciais para a implantação de uma arquitetura de rede 5G. Adicionalmente, é necessário garantir

que cada VM esteja devidamente provisionada com os recursos necessários, incluindo sistema operacional, memória e armazenamento suficientes para suportar as operações de rede intensivas. Os requisitos mínimos de cada elemento da topologia estão descritos na Tabela 6.1.

Tabela 6.1: Infraestrutura de Hardware e Software para Implantação do Protótipo

Componente	Sistema Operacional	Memória	Espaço em Disco
5GC	Ubuntu 20.04 (LTS) x64 - kernel >= *5.4.0-122-generic*	8 GB	40 GB
N3IWF	Ubuntu 20.04 (LTS) x64	2 GB	20 GB
UE-não-3GPP	Ubuntu 20.04 (LTS) x64	1 GB	20 GB

O processo de implantação segue uma sequência lógica de passos, começando pela configuração inicial das VMs que compõem a topologia ilustrada na Figura 6.1, pela instalação dos pacotes de software necessários e pela configuração detalhada de cada componente. Para facilitar a replicação do processo de implantação o repositório GitHub [1] foi disponibilizado, descrevendo detalhadamente todo o passo a passo necessário para realizar o provisionamento do protótipo de arquitetura convergente. Este repositório complementa o conteúdo descrito nesta tese, proporcionando instruções claras e detalhadas para cada etapa do processo.

Com o objetivo de reduzir a complexidade de configuração do protótipo, utilizou-se Ansible [RedHat 2024] para automatizar o processo de implantação. A preparação do ambiente, configuração da topologia de rede, instalação de dependências e testes de conectividade são todas automatizadas por meio de *scripts* Ansible, garantindo que cada VM esteja corretamente configurada para desempenhar suas funções durante a execução do protótipo da arquitetura convergente. O guia de implantação no repositório GitHub visa fornecer um roteiro claro e detalhado para a configuração do UE não 3GPP, N3IWF e free5GC [free5GC 2022], facilitando a replicação do ambiente e a validação dos experimentos. Após o provisionamento do UE não 3GPP, N3IWF e free5GC, cada um dos elementos deve ser inicializado na seguinte ordem: (*i*) free5GC, (*ii*) N3IWF e (*iii*) UE não 3GPP. Os procedimentos de inicialização de cada um dos elementos também estão contidos na documentação do repositório GitHub que complementa esta tese.

A inicialização do núcleo 5G consiste na execução de um conjunto coordenado de procedimentos envolvendo cada uma das funções de rede que compõem a arquitetura SBA. Este processo começa com a ativação e configuração das funções de rede, como a UPF, AMF, SMF e outras funções de apoio. Cada função de rede deve se registrar na NRF para permitir que outras funções se encontrem e se comuniquem de maneira eficiente e integrada ao núcleo. A coordenação e a sincronia entre essas funções são cruciais para

[1] https://github.com/LABORA-INF-UFG/TESE_CJAM_2024/tree/main/exp_1

assegurar que a rede possa gerenciar adequadamente as sessões de dados dos usuários, a mobilidade e outros serviços críticos.

Após a inicialização das funções do núcleo 5G, o próximo elemento do protótipo de arquitetura convergente a ser inicializado é a N3IWF. Embora a N3IWF esteja sendo executada de forma isolada em uma máquina dedicada, ela se registra na NRF, de forma similar às demais funções do núcleo. Este registro na NRF é crucial, pois permite que a N3IWF seja descoberta e se comunique com outras funções de rede, integrando-a eficientemente ao núcleo 5G. A Figura 6.2 ilustra o resultado esperado após a inicialização da N3IWF, destacando a execução dos seguintes procedimentos:

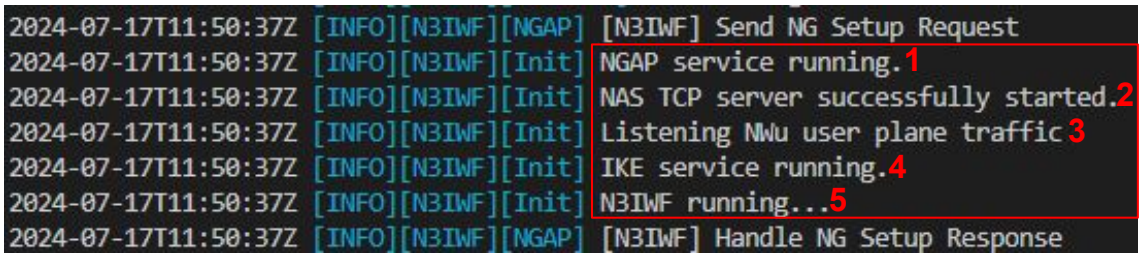

Figura 6.2: Inicialização da N3IWF com destaque para a execução de procedimentos que viabilizam o acesso não 3GPP *não confiável*.

1. ***NGAP service running*** - Indica que o serviço NGAP foi iniciado com sucesso. O NGAP é o protocolo de aplicação usado entre a N3IWF e a AMF para sinalização de controle através da interface N2, para gerenciar conexões e mobilidade dos dispositivos na rede 5G.
2. ***NAS TCP server successfully started*** - Informa que o servidor TCP para sinalização NAS foi iniciado com sucesso. O NAS é responsável pela sinalização entre o UE não 3GPP e o núcleo 5G para gerenciar aspectos de conexão, autenticação, segurança e sessões de PDU.
3. ***Listening NWu user plane traffic*** - Indica que a N3IWF começou a *escutar* o tráfego de dados no plano de usuário através da interface NWu. A interface NWu é utilizada para o transporte de dados entre a N3IWF e o UE não 3GPP, por meio de uma rede de acesso *não confiável*, permitindo que esses dispositivos se conectem e utilizem os serviços do núcleo da rede 5G.
4. ***IKE service running*** - Indica que o serviço IKE foi iniciado com sucesso. O IKE é um protocolo usado para configurar uma associação de segurança IPSec. É essencial para estabelecer canais seguros e criptografados para a transmissão de dados, garantindo a integridade e a confidencialidade da comunicação entre o UE não 3GPP e o núcleo 5G por meio da N3IWF.

5. ***N3IWF running*** - Confirma que a N3IWF está operacional e funcionando corretamente. Isso significa que todos os serviços e componentes essenciais foram inicializados com sucesso e estão prontos para processar tanto o tráfego de sinalização quanto o tráfego de dados dos usuários, integrando dispositivos ao núcleo 5G por meio de uma rede de acesso não 3GPP *não confiável*.

Após a inicialização das funções do núcleo 5G e da N3IWF, o último elemento do protótipo de arquitetura convergente a ser inicializado é o UE não 3GPP. A Figura 6.3 ilustra o resultado esperado após a inicialização, destacando a execução dos seguintes procedimentos:

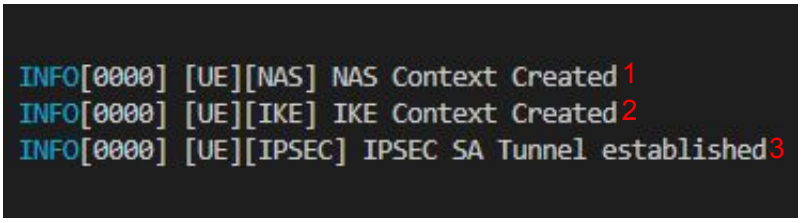

Figura 6.3: Inicialização do UE não 3GPP. Procedimentos de configuração NAS, IKE e *enlace* IPSec.

1. ***NAS Context Created*** - Indica que o UE não 3GPP conseguiu estabelecer um *enlace* com o servidor TCP de sinalização NAS da N3IWF.
2. ***IKE Context Created*** - Indica que o UE não 3GPP conseguiu estabelecer um *enlace* com o serviço IKE da N3IWF.
3. ***IPSEC SA Tunnel establised*** - Indica que o UE não 3GPP conseguiu estabelecer uma associação segura do tipo IPSec-SA com a N3IWF. Os túneis para a sinalização NAS do plano de controle e o túnel GRE para o tráfego do plano de dados do usuário foram estabelecidos, e o UE não 3GPP está operacional e funcionando corretamente.

Após a execução dos procedimentos de inicialização do UE não 3GPP, duas interfaces de rede são construídas: uma para sinalização NAS do plano de controle e outra para o tráfego de dados do usuário. A Figura 6.4 ilustra as interfaces e os respectivos endereços IP atribuídos a cada uma delas.

O endereço IP associado à interface *gretun1* (1) foi atribuído pela UPF, escolhida pela SMF para atender às requisições do UE não 3GPP, tendo como base os parâmetros de configuração **`dnnstring`** e **`snssai`**. Já o endereço IP associado à interface *ipsec0* foi atribuído pela N3IWF, tendo como base o parâmetro **`UEIPAddressRange`**, que define a faixa de endereços IPs que são alocados aos UEs não 3GPP dentro do túnel

```
1   gretun1: flags=209<UP,POINTOPOINT,RUNNING,NOARP>  mtu 1420
            inet 60.60.0.1  netmask 255.255.255.255  destination 60.60.0.1
            inet6 fe80::5efe:a00:14  prefixlen 64  scopeid 0x20<link>
            unspec 0A-00-00-14-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 0  (UNSPEC)
            RX packets 0  bytes 0 (0.0 B)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 6  bytes 336 (336.0 B)
            TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

2   ipsec0-default: flags=193<UP,RUNNING,NOARP>  mtu 1420
            inet 10.0.0.20  netmask 255.255.255.0
            inet6 fe80::42b5:a3fe:1993:84ac  prefixlen 64  scopeid 0x20<link>
            unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 0  (UNSPEC)
            RX packets 31  bytes 1763 (1.7 KB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 38  bytes 2244 (2.2 KB)
            TX errors 0  dropped 6 overruns 0  carrier 0  collisions 0
```

Figura 6.4: Túneis IPSec para sinalização NAS do plano de controle (1) e GRE para o trafego do plano de dados do usuário (2).

IPSec, garantindo que cada UE tenha um endereço IP exclusivo para a comunicação com a N3IWF.

Com a inicialização dos componentes que integram o protótipo da arquitetura convergente, o UE não 3GPP está operacional e apto a realizar comunicação segura através de uma rede de acesso não 3GPP *não confiável*. Este estado operacional (CM-CONNECTED) significa que o UE está autenticado na rede 5G através da N3IWF e que os túneis IPSec foram devidamente estabelecidos. A infraestrutura provisionada neste experimento abrange a interligação entre a N3IWF e as funções do núcleo 5G, como a AMF, UPF e SMF, todas registradas e comunicando-se via NRF, assegurando a coordenação e o gerenciamento adequado do tráfego de sinalização e de dados do UE não 3GPP. No próximo experimento, a conectividade da infraestrutura é testada, avaliando a capacidade do UE não 3GPP em estabelecer sessões de dados, a latência da comunicação, a estabilidade das conexões e a resposta da rede.

6.2 Experimento 1 - Conectividade dos componentes da arquitetura convergente

Após a implantação e configuração dos componentes que integram o protótipo da arquitetura convergente, é importante testar a conectividade da interface de rede *gretun1*. Para testar a conectividade de uma interface de rede em um ambiente Linux [Linux Foundation 2024], várias ferramentas podem ser utilizadas, como, por exemplo, **`ping`** e **`traceroute`**. Testar a conectividade de uma interface de rede é relevante para

garantir que a infraestrutura de rede está funcionando corretamente.

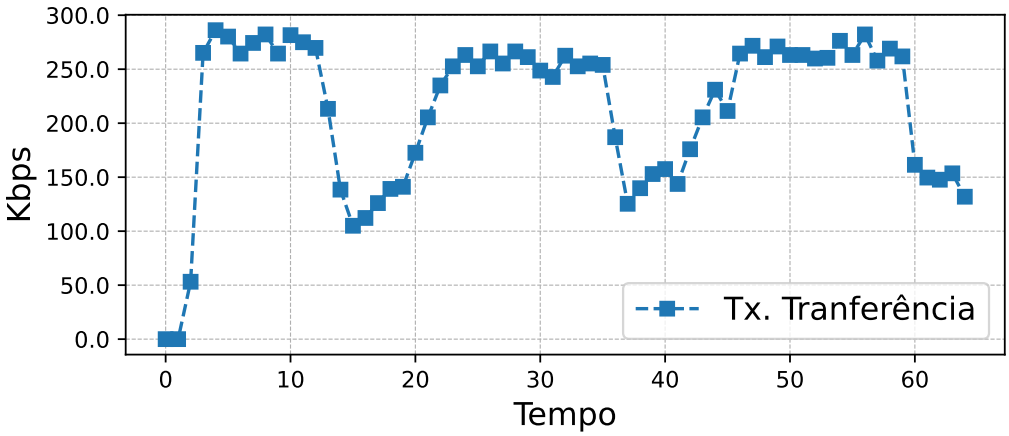

Figura 6.5: Teste de conectividade do UE não 3GPP através do uso de *ping* com inundação de pacotes (*flooding*).

A Figura 6.5 ilustra o resultado de um teste de conectividade executado através do comando **`ping -f -I gretun1 8.8.8.8`**. Quando se utiliza o comando **`ping`** com a opção **`-f`**, habilita o modo de inundação de pacotes (*flooding*), enviando pacotes *Internet Control Message Protocol* (ICMP) ao destino **`8.8.8.8`** o mais rapidamente possível. Esse tipo de teste gera um grande volume de tráfego em um curto período de tempo na interface *gretun1*. O objetivo de usar o **`-f`** é testar a capacidade da interface *gretun1* do UE não 3GPP em lidar com uma carga intensa de pacotes.

Tabela 6.2: Resultados obtidos após o uso de *ping* com inundação de pacotes (*flooding*)

Descrição	Valor
Pacotes transmitidos	30361
Pacotes recebidos	30360
Percentual de pacotes perdidos	0.0032937%
Tempo de execução	64564 ms
RTT (min)	1.786 ms
RTT (méd)	2.725 ms
RTT (max)	27.853 ms

A Tabela 6.2 apresentas os valores estatísticos obtidos com o teste. Os resultados indicam a estabilidade da interface *gretun1* do UE não 3GPP, com praticamente nenhuma perda de pacotes, baixa latência e uma variação mínima nos tempos de resposta. O **`ping`** com *flooding* foi bem sucedido, e a rede conseguiu lidar com a carga intensa de pacotes sem problemas significativos.

A Figura 6.6 ilustra o resultado de um teste de conectividade executado através do comando **`traceroute -i gretun1 8.8.8.8`** (1). O experimento tem como

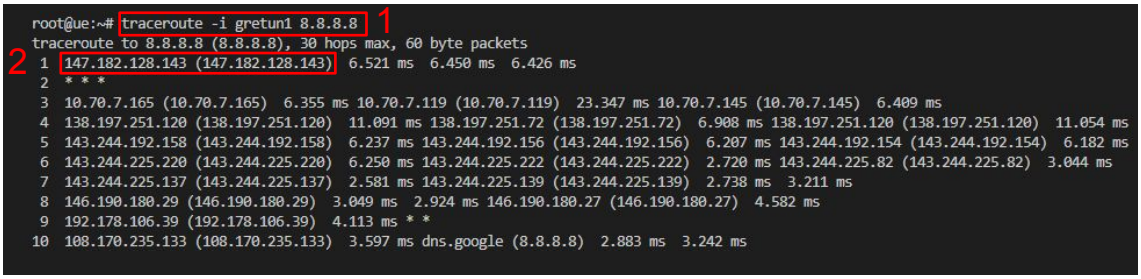

Figura 6.6: Teste de conectividade do UE não 3GPP através do uso de *traceroute*.

objetivo rastrear a rota que os pacotes de dados seguem, partindo da interface *gretun1* do UE não 3GPP até o servidor de *Domain Name System* (DNS) público do Google. É importante observar o endereço IP do primeiro roteador pelo qual os pacotes passam após saírem da interface *gretun1* (2). A topologia apresentada na Figura 6.1 permite observar que o primeiro salto possui o mesmo endereço IP da interface *eth0* que interliga o núcleo 5G à Internet. Todos os endereços IPs atribuídos nas interfaces de rede intermediárias existentes entre *gretun1* no UE não 3GPP e a saída do núcleo 5G não são apresentados. Isso demonstra que os dados estão trafegando através do túnel do plano de dados do usuário e fluindo através do núcleo 5G. Além disso, observa-se que a maior parte dos roteadores respondeu, exceto o segundo salto, que não forneceu resposta, possivelmente, devido a políticas de rede que bloqueiam pacotes ICMP. A latência geral é baixa, indicando uma conexão relativamente rápida.

Os testes de conectividade evidenciam que a interface *gretun1* do UE não 3GPP está operando de forma estável, garantindo uma comunicação de baixa latência com o servidor de destino. Tanto o comando **`ping`** quanto o **`traceroute`** demonstraram a robustez da configuração da rede, com perda de pacotes nula e tempos de resposta consistentes. A estabilidade e a baixa latência observadas reforçam a viabilidade da arquitetura convergente, proporcionando uma base sólida para futuras expansões e otimizações.

6.3 Experimento 2 - Avaliação de desempenho de vazão

Após confirmar a existência de conectividade estável entre os componentes do protótipo da arquitetura, pode-se examinar a capacidade de transmissão de dados do UE através da rede 5G. Para avaliar a capacidade de transmissão, utilizou-se a seguinte estratégia: (*i*) aplicar um tráfego de dados sobre a interface *gretun1* do UE não 3GPP, (*ii*) utilizar o serviço **`controller.GetNetworkThroughput`** da API do UE não 3GPP para monitorar a interface *gretun1* durante um determinado intervalo de tempo e (*iii*) plotar um gráfico com o intervalo de tempo no eixo x e a vazão no eixo y.

Para aplicar o tráfego sobre a interface *gretun1*, utilizou-se o comando **`time curl -L --interface gretun1 -O [url-para-download]`**, onde o marcador `[url-para-download]` deve ser substituído pelo endereço de um arquivo para download. No experimento, utilizou-se a URL de um arquivo do tipo `.tar.gz` com tamanho de aproximadamente 64 Megabytes (MBs). O comando `time` foi combinado com `curl`, direcionado à interface *gretun1* através do parâmetro `-interface`. Como resultado, pode-se observar que 100% do arquivo de 64 MB foi baixado, com um tempo total de 38 segundos.

Alguns segundos antes de executar o teste de vazão, utilizou-se o microsserviço `controller.GetNetworkThroughput`, passando como parâmetro a interface *gretun1* e um intervalo de tempo de 60 segundos. Após o intervalo de tempo especificado, o microsserviço retornou um JSON contendo, para cada intervalo de tempo, uma métrica de vazão da interface *gretun1*. A Figura 6.7 ilustra o resultado obtido a partir do monitoramento da vazão do UE não 3GPP. Inicialmente, os valores de vazão são nulos, e após 3 segundos, os valores passam a oscilar indicando a taxa de transferência em Mbps. A resposta obtida a partir do microsserviço de monitoramento do UE não 3GPP também indica que, após aproximadamente 42 segundos, o tráfego da interface *gretun1* é encerrado.

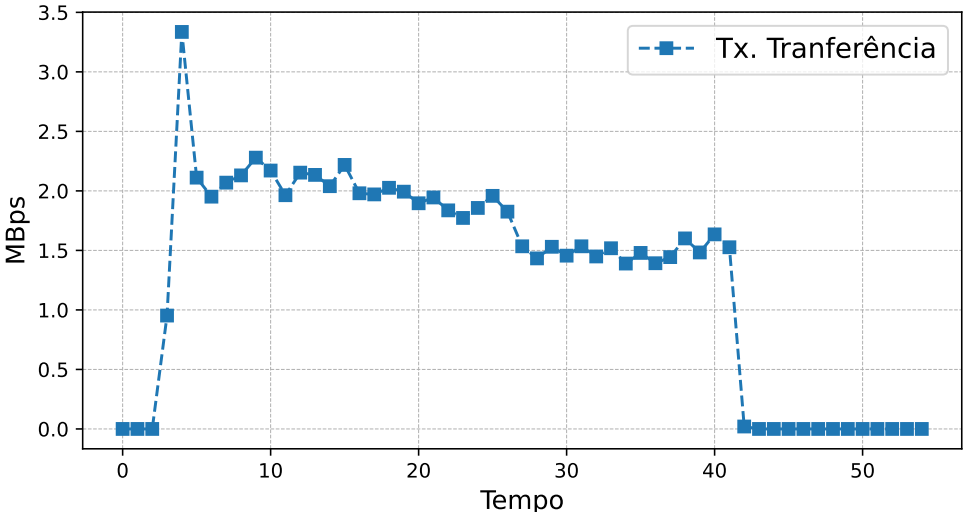

Figura 6.7: Vazão da interface *gretun1* obtida a partir do serviço de API do UE não 3GPP.

Os resultados obtidos com o teste de vazão evidenciam a funcionamento do mecanismo de coleta de métricas implementado no protótipo da arquitetura convergente. A execução do comando `curl` para download de um arquivo, juntamente com a ativação do mecanismo de coleta de métricas na interface *gretun1* do UE, demonstrou que a taxa de transferência, ilustrada na Figura 6.7, se manteve ativa durante um intervalo de tempo equivalente ao intervalo de 38 segundos, obtido com as estatísticas do comando `curl`

no próprio dispositivo. Este alinhamento confirma a funcionalidade da API de coleta de métricas e destaca uma inovação: a capacidade do operador de infraestrutura de acessar métricas de desempenho de um UE conectado através de uma rede de acesso *não confiável*. Em um contexto de convergência de tecnologias de comunicação não 3GPP e o núcleo 5G, essa funcionalidade é especialmente relevante, pois permite ao operador monitorar e otimizar a qualidade do serviço, mesmo quando o UE utiliza redes de acesso não controladas pelo operador da infraestrutura. Esse avanço representa um passo significativo para a integração mais eficiente e eficaz de diferentes tecnologias de comunicação, ampliando o alcance e a robustez das redes convergentes.

6.4 Experimento 3 - Monitoramento de redes não 3GPP

Neste experimento, a capacidade de monitoramento de redes não 3GPP foi investigada, especificamente redes Wi-Fi, dentro de uma infraestrutura 5G, utilizando o mecanismo de coleta de métricas de interface Wi-Fi do UE não 3GPP. O experimento foi realizado utilizando equipamentos físicos, conectados em uma topologia conforme ilustra a Figura 6.8. A Tabela 6.3 descreve a configuração de cada um dos dispositivos físicos utilizados no experimento. O objetivo é demonstrar como essas métricas, coletadas durante o acesso *não confiável* ao núcleo 5G via N3IWF, podem fornecer ao operador da infraestrutura uma visão detalhada e em tempo real sobre o comportamento e a qualidade das conexões em redes não 3GPP. Essa capacidade de monitoramento é essencial para garantir a QoS, identificar potenciais problemas de conectividade e tomar decisões informadas sobre a gestão da infraestrutura de comunicação.

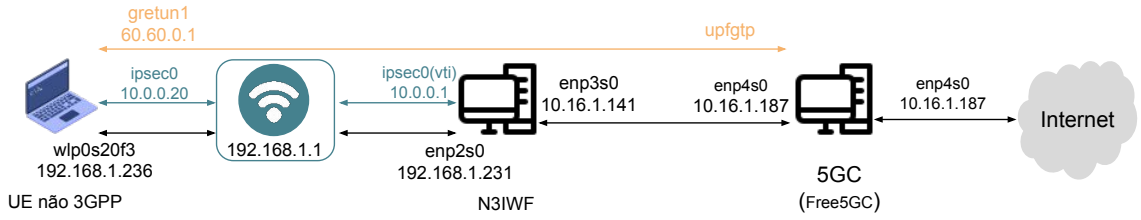

Figura 6.8: Topologia de rede utilizada no experimento de monitoramento de redes não 3GPP por meio de métricas coletadas do UE não 3GPP.

Durante o experimento, os túneis para o Plano de Dados do Usuário e Plano de Controle, entre UE não 3GPP e N3IWF, foram estabelecidos através de um ponto de acesso Wi-Fi, configurado de acordo com os parâmetros descritos na Tabela 6.4. Após implantar os componentes e testar a conectividade, adotou-se a seguinte estratégia: (i) Aplicar tráfego sobre a interface *gretun1* do UE não 3GPP, repetindo o experimento descrito na Seção 6.3, (ii) distanciar progressivamente o posicionamento do UE não 3GPP

Tabela 6.3: Configurações dos dispositivos físicos para o monitoramento de redes não 3GPP

Componente	Tipo de Equipamento	Sist. Operacional	Memória	Processador	Espaço em Disco
5GC	Computador	Ubuntu 20.04 (LTS) x64 kernel >= *5.4.0-122-generic*	4 GB	Intel i7	1 TB
N3IWF	Computador	Ubuntu 20.04 (LTS) x64	4 GB	Intel i5	500 GB
UE não 3GPP	Laptop	Ubuntu 20.04 (LTS) x64	4 GB	Intel i3	256 GB

do ponto de acesso Wi-Fi, registrando as métricas produzidas pela interface e (iii) gerar gráficos a partir das métricas coletadas.

Tabela 6.4: Configurações do ponto de acesso Wi-Fi para o monitoramento de redes não 3GPP

Parâmetro	Descrição
Banda	2.4 GHz
Autenticação	WPA2-PSK
Padrão	802.11
Antenas	3 antenas ajustáveis
Canal	Adaptativo

Durante o experimento, observou-se que, à medida que o UE não 3GPP se distancia progressivamente do ponto de acesso Wi-Fi, a potência do sinal oscila entre -30 dBm e -65 dBm. Esses valores representam a intensidade do sinal recebido pelo UE não 3GPP conectado à rede Wi-Fi. Um valor mais próximo de 0 dBm indica um sinal mais forte, enquanto valores negativos indicam um sinal mais fraco. A oscilação entre -30 dBm e -65 dBm reflete flutuações na qualidade do sinal, decorrentes da movimentação do UE não 3GPP durante a realização do experimento. A redução na potência do sinal pode resultar em impactos significativos na taxa de transferência. Quando o sinal está forte (próximo de -30 dBm), a conexão tende a ser estável e a velocidade de transferência de dados, mais alta. No entanto, quando o sinal enfraquece (próximo de -65 dBm), a conexão pode se tornar instável, resultando em uma taxa de transferência mais lenta, causando possíveis interrupções ou até mesmo quedas de conexão, conforme ilustra a Figura 6.9.

Atualmente, os operadores de redes 5G não têm acesso direto a métricas de redes não 3GPP. Com a introdução de uma API de coleta de métricas do UE não 3GPP, os operadores de redes 5G podem acessar essas informações, permitindo uma visão mais holística da qualidade da conexão do usuário. Esse acesso permite que os operadores identifiquem e solucionem problemas de conectividade de forma mais eficaz, ajustando os recursos da rede e melhorando a experiência do usuário final. Ao ter acesso a parâmetros que possibilitem compreender as flutuações em redes não 3GPP, os operadores de infraestrutura podem tomar decisões mais acertadas sobre como gerenciar o tráfego e

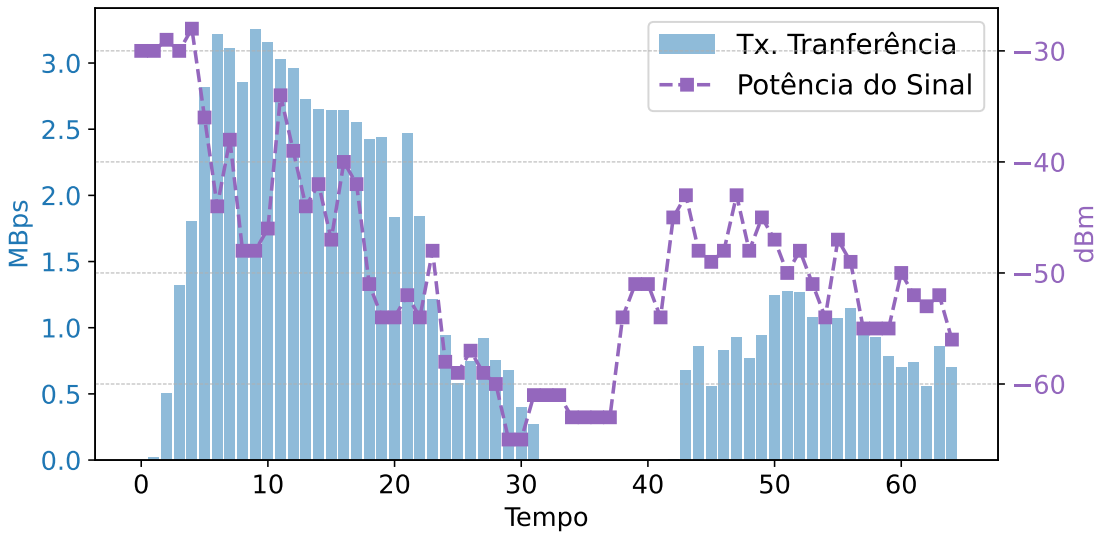

Figura 6.9: Potência do sinal da interface de rede Wi-Fi vs taxa de transferência. Medidas obtidas através da API de coleta de métricas do UE não 3GPP durante aproximadamente 60 segundos.

distribuir recursos, garantindo que as comunicações críticas sejam mantidas com a maior qualidade.

6.5 Experimento 4 - Aplicação de realidade mista

Nos últimos anos, as constantes melhorias no poder de computação reacenderam o interesse em aplicações envolvendo Realidade Virtual (VR). A VR é definida como um ambiente inteiramente gerado por computador que simula espaços, objetos e seres de forma a imitar a realidade percebida pelos cinco sentidos humanos. Dentro desse conjunto, encontram-se a Realidade Aumentada (AR) e a Realidade Virtual Aumentada (AVR) [Bekele et al. 2018]. A AR envolve a sobreposição de elementos visuais e sonoros, que existem apenas virtualmente, sobre a percepção do mundo real, criando uma camada digital integrada à realidade física. Entretanto, a AVR insere elementos do mundo real em um ambiente virtual, enriquecendo a experiência simulada com componentes reais. O termo Realidade Mista (MR) é utilizado para descrever genericamente qualquer aplicação que combine AR e AVR.

Com os avanços recentes nas tecnologias de comunicação, o consumo de aplicações de MR em dispositivos móveis, como *smartphones*, tem se tornado uma tendência crescente. Por exemplo, na navegação, *smartphones* podem utilizar algoritmos para reconhecer objetos no ambiente e sobrepor instruções de navegação diretamente no campo de visão do usuário. No entanto, a execução dessas aplicações em tempo real continua a

representar desafios significativos, principalmente, devido às demandas por alto poder de processamento e baixa latência. Nesse contexto, a computação de borda surge como uma solução promissora, permitindo que dispositivos móveis executem tarefas menos exigentes, enquanto operações mais complexas são processadas no servidor. Esse processo de transferência de operações do dispositivo móvel para um servidor de borda é comumente conhecido como *offloading* [Mach e Becvar 2017].

Considerando um cenário onde uma aplicação MR em um dispositivo móvel exige *offloading*, a arquitetura convergente proposta nesta tese se mostra promissora, pois facilita a conectividade necessária, conforme demonstrado pelos experimentos descritos nas Seções 6.1, 6.2 e 6.3. A especificação do 3GPP sobre aspectos de serviço e sistema [3GPP XR in 5G 2020] cobre mais de 20 casos de uso distintos, que vão desde entretenimento até saúde e educação. Para ilustrar a capacidade do protótipo da arquitetura convergente em atender a um cenário de MR, um experimento utilizando o *Mixed Reality Linköping Egde Offloading* (MR-Leo) [Lindqvist 2019] foi realizado, conforme mostrado na Figura 6.10.

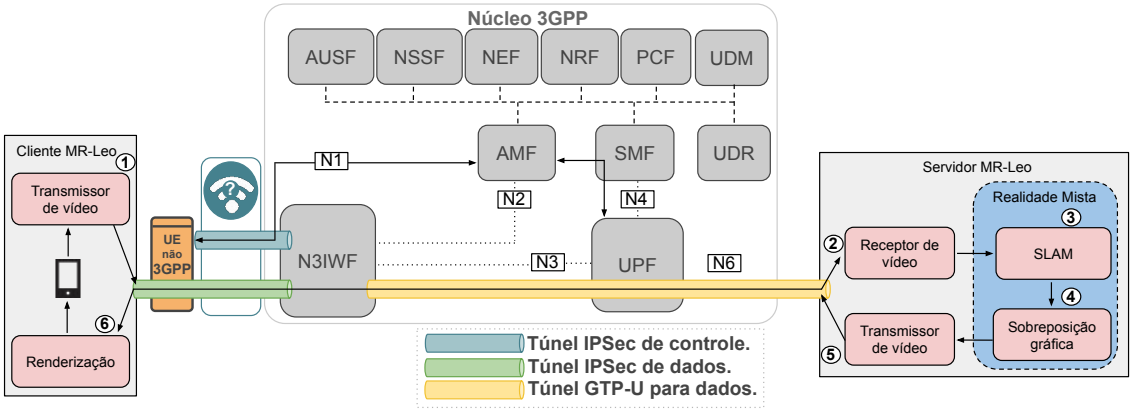

Figura 6.10: Fluxo de funcionamento do MR-Leo integrado ao protótipo da arquitetura convergente através do acesso não confiável.

O MR-Leo é um *framework* de realidade mista que enriquece um fluxo de vídeo utilizando um algoritmo de *Simultaneous Localization and Mapping* (SLAM) conhecido como *Oriented FAST and Rotated BRIEF* (ORB)-SLAM2. O MR-Leo realiza um *offloading* estático, onde as funções de transmissão/recepção de vídeo e renderização são executadas pelo dispositivo móvel, enquanto os demais processos são realizados por um servidor de borda. O experimento ilustrado na Figura 6.10 foi conduzido no âmbito do projeto Brasil 6G [Inatel, MCTI e RNP 2024]. Neste experimento, o servidor MR-Leo foi posicionado na infraestrutura da rede de dados e hospedado em uma máquina virtual dedicada. O cliente MR-Leo é representado por um dispositivo UE, um *smartphone* que executa a aplicação cliente em um dispositivo Android convencional, conectado a um

gateway UE não 3GPP responsável por fornecer conectividade utilizando um acesso *não confiável* através de Wi-Fi para chegar até a N3IWF.

Na Figura 6.10, observa-se que o MR-Leo inicia seu processo com a captura de vídeo pelo dispositivo do usuário, que é enviado ao servidor através do núcleo 5G, utilizando o acesso *não confiável* provido pelo protótipo da arquitetura convergente. No servidor, o vídeo capturado é redirecionado para o módulo de realidade mista, onde o ORB-SLAM2 constrói um mapa Tridimensional (3D) do ambiente. Esse mapa é utilizado para a subsequente sobreposição gráfica, permitindo a inserção de um objeto virtual no quadro de vídeo. Finalmente, a cena enriquecida é retransmitida ao cliente, novamente através do protótipo da arquitetura convergente, e renderizada no dispositivo do usuário.

Do lado do cliente MR-Leo, é necessário informar o endereço IP do servidor para que o vídeo seja transmitido a partir do *smartphone* através do protótipo da arquitetura convergente. A Figura 6.11 ilustra o comportamento esperado da aplicação cliente MR-Leo. No lado direito da figura, é exibida a imagem capturada e enviada pelo UE. Essa transmissão é direcionada ao servidor através do protótipo da arquitetura convergente, onde são adicionadas informações de MR, como contexto ou objetos virtuais.

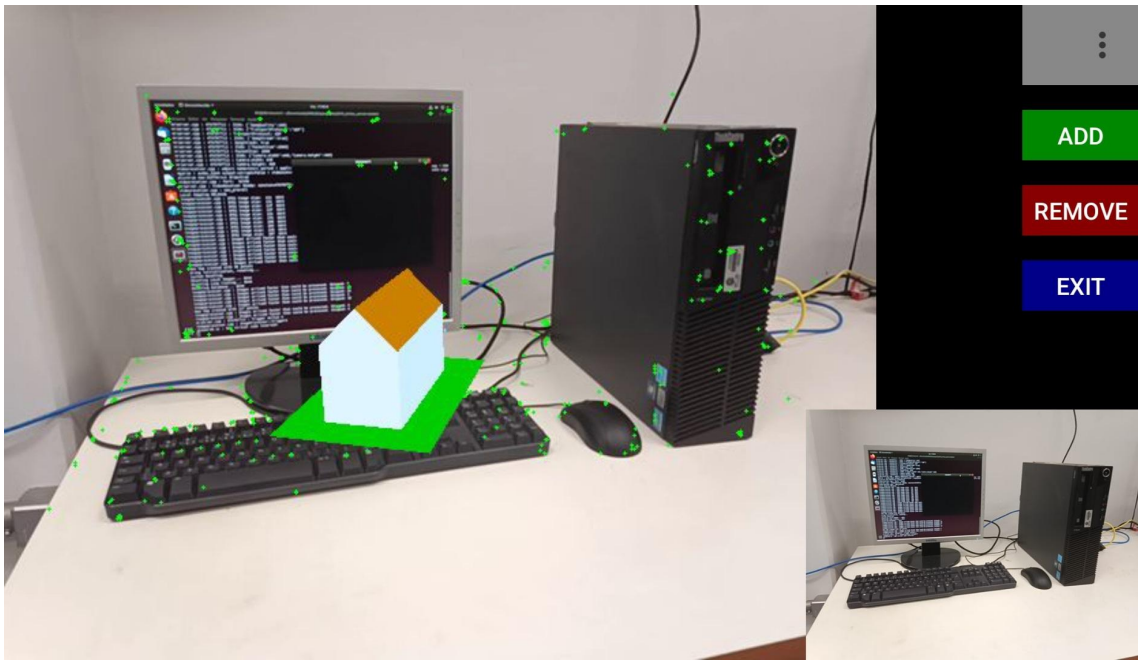

Figura 6.11: Aplicação de Realidade Mista com MR-Leo em operação no lado cliente.

Aplicações de realidade mista (MR) exigem uma experiência de usuário contínua e fluida, tornando a baixa latência um requisito crucial. Qualquer atraso, interrupção ou travamento pode comprometer a imersão e a interatividade. A Tabela 6.5 apresenta a distribuição do tempo total necessário para processar um quadro. Este tempo total é dividido em tempo de enriquecimento e tempo de comunicação / processamento. O tempo

de enriquecimento refere-se ao intervalo necessário para fornecer ao usuário um quadro de vídeo enriquecido com informações adicionais. A análise da Tabela 6.5 revela um tempo médio total de 17,3 ms, dos quais 16,2 ms são dedicados ao enriquecimento. Esses resultados evidenciam a ausência de atrasos significativos na comunicação.

Tabela 6.5: Distribuição do tempo necessário para processar um quadro de vídeo pela aplicação de realidade mista com MR-Leo

Descrição	Tempo
Comunicação e Processamento	1,1 ms
Enriquecimento	16,2 ms
Total	17,3 ms

Os resultados apresentados demonstram um comportamento satisfatório do protótipo da arquitetura convergente em um cenário de uso de uma aplicação de realidade mista (MR). A infraestrutura de comunicação, mesmo com o acesso *não confiável*, mostrou-se promissora ao transmitir os dados em tempo hábil, permitindo o processamento de vídeo no servidor de borda. A distribuição do tempo evidencia a ausência de atrasos significativos na comunicação. Os *point clouds* e o mapeamento são realizados de forma eficiente, e o objeto virtual inserido acompanha o movimento do usuário, posicionando-se corretamente na superfície desejada.

6.6 Experimento 5 - Aplicações prioritárias para o agronegócio

Além do experimento envolvendo a aplicação de realidade mista (MR), descrito na seção 6.5, foram selecionadas algumas aplicações prioritárias para o agronegócio no âmbito do projeto Brasil 6G [Inatel, MCTI e RNP 2024]. A seleção dessas aplicações baseou-se na classificação de *alto impacto* atribuída a cada uma delas em relação às áreas rurais, conforme os estudos produzidos pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) [BNDES e MCTIC].

Com o objetivo de demonstrar a compatibilidade de integração do protótipo de arquitetura convergente com soluções comerciais que empregam diferentes padrões de comunicação, considerou-se que as aplicações prioritárias para o agronegócio utilizariam redes de comunicação diversas. As aplicações de sensoriamento e monitoramento IoT voltadas para o agronegócio frequentemente empregam redes de comunicação LPWAN, conhecidas por seu baixo consumo energético e longo alcance. Entre essas redes, destacam-se *Sigfox* [UnaBiz Pte Ltd 2024], LoRa [Semtech Corp. 2024] e Wi-Fi. O experimento conduzido no âmbito do projeto Brasil 6G é ilustrado na Figura 6.12.

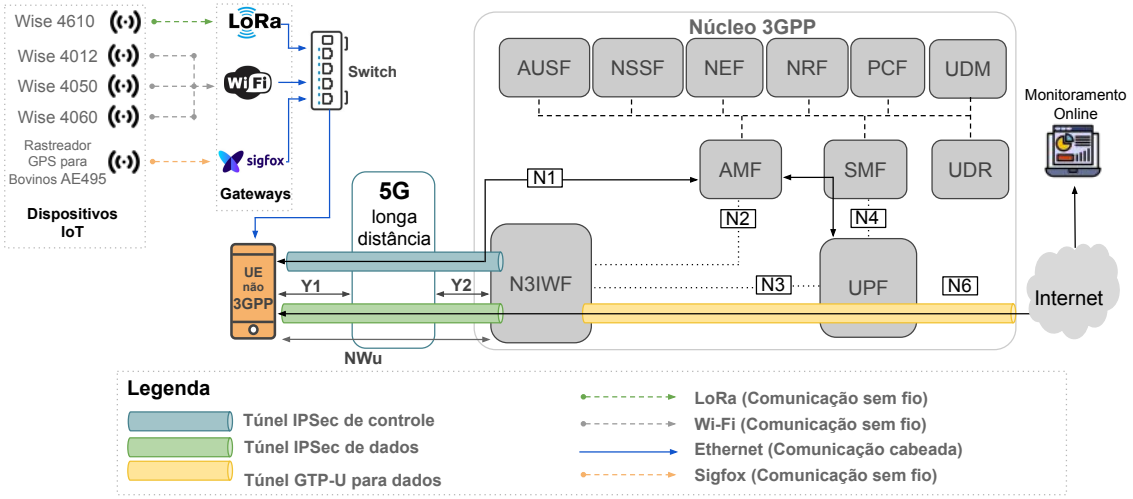

Figura 6.12: Aplicações prioritárias para o Agronegócio com conectividade através de acesso não 3GPP não confiável.

Na Figura 6.12, são apresentados diferentes tipos de dispositivos IoT associados às tecnologias Wi-Fi, LoRa e *Sigfox*. Estes dispositivos transmitem informações para *Gateways*, que estão conectados ao UE não 3GPP através de um equipamento *Switch*. O enlace entre o UE não 3GPP e a N3IWF, responsável pela estruturação dos túneis para os planos de dados do usuário e controle, foi estabelecido por meio de radiocomunicação entre dois transceptores. Um transceptor está posicionado no mesmo computador que executa o UE não 3GPP, enquanto o outro está posicionado no computador que executa a N3IWF. Cada transceptor é composto por um *Software-Defined Radio* (SDR) e uma *Outdoor Unit* (ODU) com antenas, capaz de manter uma taxa de dados média de aproximadamente 100 Mbps a uma distância de até 50 km [Mendes et al. 2020]. No experimento, as informações geradas pelos diferentes dispositivos IoT são transmitidas através do núcleo 5G via acesso *não confiável*, em direção a uma aplicação de monitoramento situada na rede de dados.

Os testes foram conduzidos com foco no monitoramento dos dispositivos IoT que utilizam comunicação via LoRa e Wi-Fi, junto com os respectivos *gateways*. Os dados dos dispositivos são transmitidos à Internet através do protótipo da arquitetura convergente e, em seguida, apresentados em um *dashboard* para visualização das informações coletadas. A aplicação prática da arquitetura no Centro de Referência em Radiocomunicações do Inatel reforça a viabilidade da convergência de tecnologias de comunicação não 3GPP. O UE não 3GPP, em conjunto com a N3IWF, demonstrou ser viável para garantir a conectividade contínua e a integração dos dispositivos IoT, evidenciando que a arquitetura convergente pode suportar de maneira eficaz uma ampla gama de aplicações.

CAPÍTULO 7

Conclusão

O presente documento apresentou uma investigação detalhada sobre a viabilidade da convergência entre tecnologias de comunicação sem fio não 3GPP e o núcleo 5G, com ênfase na arquitetura convergente. A integração dessas tecnologias, facilitada pelo uso do UE não 3GPP e do acesso não confiável através da N3IWF, demonstrou ser uma solução robusta para enfrentar desafios de conectividade em cenários diversos, incluindo áreas rurais e aplicações IoT. A implementação do protótipo funcional desta arquitetura permitiu a validação de diversas hipóteses levantadas ao longo do trabalho. O acesso não confiável, facilitado pelo UE não 3GPP, mostrou-se eficaz na manutenção da conectividade contínua e segura, sendo crucial para o funcionamento de aplicações críticas. Além disso, os túneis IPSec estabelecidos pelo UE não 3GPP são associados a um usuário específico, permitindo ao operador de infraestrutura monitorar conexões individuais e, se necessário, alocar o UE não 3GPP em uma fatia de rede com recursos customizados. Isso é viável porque o túnel de dados pertence a um UE não 3GPP específico, oferecendo flexibilidade na gestão dos recursos de rede.

Neste sentido, a tese responde a primeira pergunta de pesquisa apresentada no Capítulo 1, destacando que os principais requisitos para o desenvolvimento de uma arquitetura de sistema que permita a convergência de tecnologias 3GPP e não 3GPP incluem a integração de diferentes padrões de comunicação de forma coesa, garantindo interoperabilidade, segurança, e eficiência na transmissão de dados. A arquitetura proposta deve adotar tecnologias como virtualização, baixa complexidade, acoplamento reduzido e ser estruturada tendo como base protocolos robustos de segurança, como o IKE e IPSec, para assegurar a comunicação segura entre redes heterogêneas. Já a segunda pergunta, apresentada no Capítulo 1, é respondida ao observar que a arquitetura convergente proposta nesta tese amplia significativamente a observabilidade e o monitoramento da infraestrutura 5G para redes de acesso não 3GPP. Um dos principais avanços desta abordagem é a nova capacidade de monitorar conexões fora da rede 3GPP tradicional. Atualmente, quando um UE se conecta ao núcleo da rede através de um caminho diferente daquele fornecido por uma BS, o controlado da infraestrutura enfrenta limitações em aplicar conceitos de observabilidade a essas conexões. Nesse contexto, o UE não 3GPP introduz mecanismos

de monitoramento de interfaces de rede, permitindo ao operador do sistema obter uma visão abrangente das atividades além dos limites da rede 3GPP. Através da integração do UE não 3GPP e da N3IWF, a arquitetura possibilita a coleta de métricas detalhadas, monitorando não apenas os túneis de controle e de dados, mas também as interfaces associadas ao acesso não confiável. Isso permite ao operador aplicar otimizações, ampliando significativamente a capacidade de monitoramento e gerenciamento da rede, mesmo em cenários que envolvem tecnologias não 3GPP.

Além dos benefícios técnicos, a convergência entre tecnologias não 3GPP e o núcleo 5G oferece vantagens econômicas significativas. A possibilidade de utilizar infraestruturas de comunicação já existentes, como redes Wi-Fi e LoRa, reduz os custos de implantação e operação, tornando a solução acessível para uma ampla gama de usuários e aplicações. Essa economia de recursos é particularmente relevante em contextos como o agronegócio, onde a viabilidade financeira de novas tecnologias é um fator crucial para sua adoção. Além disso, com a capacidade de monitorar e gerenciar conexões fora da rede 3GPP, os operadores podem otimizar a alocação de recursos, maximizando a eficiência operacional e reduzindo os custos associados ao gerenciamento de redes híbridas.

Os resultados obtidos indicam um caminho promissor para o desenvolvimento de futuras redes de telecomunicações, na qual a integração de diferentes tecnologias de comunicação pode proporcionar uma conectividade abrangente e resiliente. A arquitetura convergente apresentada nessa tese pode ser adaptada e expandida para suportar novas tecnologias emergentes, garantindo que as redes 5G e além permaneçam na vanguarda da inovação tecnológica. Com a capacidade de monitoramento além da rede controlada pelo operador, a segurança e a qualidade do serviço são aprimoradas, abrindo novas possibilidades para o desenvolvimento de aplicações que exigem alta confiabilidade e personalização dos recursos de rede.

O estudo também destacou a importância de adotar uma abordagem híbrida para superar as limitações das tecnologias 3GPP, especialmente em áreas onde a cobertura 5G ainda é limitada. A convergência com tecnologias não 3GPP permite preencher essas lacunas, garantindo uma conectividade contínua e eficiente, independentemente do ambiente de operação da rede. A capacidade de monitorar e controlar o tráfego por meio de túneis IPSec associados a usuários específicos oferece uma ferramenta poderosa para os operadores de infraestrutura, permitindo-lhes adaptar as condições de rede às necessidades particulares de cada UE.

Este trabalho contribui para o avanço do conhecimento na área de telecomunicações, oferecendo uma base sólida para futuras pesquisas e desenvolvimentos. A integração de redes não 3GPP com o núcleo 5G, por meio da arquitetura convergente, abre novas oportunidades para inovação e transformação digital, atendendo às crescentes demandas de uma sociedade cada vez mais interconectada e dependente de tecnologias de

comunicação avançadas. A inclusão de ferramentas de monitoramento e gestão para redes de acesso não confiáveis representa um avanço significativo, permitindo uma gestão mais eficaz e segura dos recursos de rede. Este progresso é essencial para o sucesso das futuras implementações de redes, criando condições para um cenário de superconvergência.

7.1 Resultados de divulgação científica

As investigações realizadas durante o desenvolvimento desta tese resultaram em diversos produtos finais, incluindo publicações científicas, repositórios de código, registros de programas de computador junto ao Instituto Nacional de Propriedade Intelectual (INPI), além de outros trabalhos técnicos dentro do escopo da pesquisa. Os resultados estão detalhados nas Tabelas 7.1 e 7.2.

Tabela 7.1: Resultados científicos

ID	Identificação do Trabalho / Local de Publicação / Autores	Tipo	Status
1	**Título:** *FramCo: Frame corrupted detection for the Open RAN intelligent controller to assist UAV-based mission-critical operations* **Local:** Journal of Internet Services and Applications **DOI:** https://doi.org/10.5753/jisa.2024.4036 **Página Oficial:** https://journals-sol.sbc.org.br/index.php/jisa/article/view/4036 **Autores:** **Ciro J. A. Macedo**, Elton Dias, Cristiano Bonato Both, Kleber Vieira Cardoso	Artigo Completo	Publicado
2	**Título:** *Improved support for UAV-based computer vision applications in Search and Rescue operations via RAN Intelligent Controllers* **Local:** XL Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT2022) **DOI:** http://dx.doi.org/10.14209/sbrt.2022.1570817420 **Página Oficial:** https://biblioteca.sbrt.org.br/articles/3601 **Autores:** **Ciro J. A. Macedo**, Elton Dias, Jones José da Silva Júnior, Gustavo Zanatta Bruno, Felipe Hauschild Grings, Antonio M Alberti, Cristiano Bonato Both, Kleber Vieira Cardoso	Artigo Completo	Publicado
3	**Título:** *System Intelligence for UAV-Based Mission Critical with Challenging 5G/B5G Connectivity* **Local:** ITU Journal on Future and Evolving Technologies **DOI:** https://doi.org/10.52953/WWDQ6893 **Página Oficial:** https://www.itu.int/pub/S-JNL-VOL3.ISSUE2-2022-A29 **Autores:** Cristiano Bonato Both, Joao Borges, Luan Gonçalves, Cleverson Nahum, **Ciro J. A. Macedo**, Aldebaro Klautau, Kleber Vieira Cardoso	Artigo Completo	Publicado
4	**Título:** *Soft5G+: Explorando a Softwarização nas Redes 5G* **Local:** XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos **DOI:** https://doi.org/10.5753/sbc.5033.7.3 **Autores:** Cristiano Bonato Both, Kleber Vieira Cardoso, Lucio Rene Prade, Victor Hugo L. Lopes, **Ciro J. A. Macedo**	Cap. Livro	Publicado
5	**Título:** *NWDAF habilitando Inteligência Artificial em operações de busca e salvamento assistidas por VANTs.* **Local:** XXXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - 2021 **Página Oficial:** https://sol.sbc.org.br/index.php/w6g/article/view/17229 **Autores:** **Ciro J. A. Macedo**, Hudson P. Romualdo, Cristiano B. Both, Antonio Oliveira-Jr, Kleber Vieira Cardoso	Artigo Curto	Publicado
6	**Título:** *Implantação e Avaliação de um Protótipo para Filas Inteligentes utilizando um Dispositivo IoTWi-Fi e um Gateway IoT Definido por Software* **Local:** Escola Regional de Informática de Goiás - ERIGO 2019 **Página Oficial:** https://sol.sbc.org.br/9102 **Autores:** Divino Alves Ferreira Júnior, João Paulo Oliveira Cabral, **Ciro J. A. Macedo**, Tércio A.dos Santos Filho, Kleber Vieira Cardoso, Antonio Oliveira-Jr	Artigo Completo	Publicado
7	**Título:** *Experimentos da Proposta de Integração SOFTWAY4IoT e FIWARE-Lab@RNP para Internet das Coisas (IoT)* **Local:** XLI Congresso da Sociedade Brasileira de Computação Workshop do Testbed FIBRE 2021 **DOI:** https://doi.org/10.5753/fibre.2021.15768 **Página Oficial:** https://sol.sbc.org.br/index.php/wfibre/index **Autores:** Antonio Oliveira-Jr, **Ciro J. A. Macedo**, Gabriel M. F. de Almeida, Leonardo Rodrigues, Marcos Abreu, Sand Correa, Kleber Vieira Cardoso	Artigo Completo	Publicado

Tabela 7.2: Resultados técnicos

ID	Identificação do Trabalho / Local de Publicação / Autores	Tipo	Status
3	**Título:** *ORQCGIOT - Orquestrador de Componentes Virtuais para Sistema Corporativo de Gateways IoT* **Local:** INSTITUTO NACIONAL DE PROPRIEDADE INTELECTUAL **Nº Registro:** BR 51 2020 002007 0 **Autores:** ANTONIO OLIVEIRA-JR, **CIRO J. A. MACEDO**, GABRIEL M. F. DE ALMEIDA, KLEBER VIEIRA CARDOSO, MARCOS F. B. DE ABREU, PABLLO F. DE ANDRADE SOUSA, SAND L, CORRÊA	Programa de Computador	Registrado
4	**Título:** *ICSGWIOT - Interface de Comunicação entre Sistema Corporativo de Gateways IoT e Plataforma de Desenvolvimento de Aplicações IoT* **Local:** INSTITUTO NACIONAL DE PROPRIEDADE INTELECTUAL **Nº Registro:** BR 51 2020 002006 2 **Autores:** ANTONIO OLIVEIRA-JR, **CIRO J. A. MACEDO**, GABRIEL M. F. DE ALMEIDA, KLEBER VIEIRA CARDOSO, LEONARDO R. FURTADO, PABLLO F. DE ANDRADE SOUSA, SAND L, CORRÊA	Programa de Computador	Registrado
5	**Título:** *User Equipment for non-3GPP Untrusted Access* **Local:** GITHUB **Página Oficial:** https://github.com/LABORA-INF-UFG/UE-non3GPP **Autor: CIRO J. A. MACEDO**	Repositório de Código	Publicado
5	**Título:** *Proto6G - Implantação dos componentes de software da arquitetura de comunicação desenvolvida no projeto Brasil 6G* **Local:** GITHUB **Página Oficial:** https://github.com/LABORA-INF-UFG/Proto6G-Install **Autor: CIRO J. A. MACEDO**	Repositório de Código	Publicado
6	**Título:** *SAMURAI-IoT-Access - Implantação dos componentes de software que formam núcleo e rede de acesso do projeto Smart 5G Core And MUltiRAn Integration (SAMURAI)* **Local:** GITHUB **Página Oficial:** https://github.com/LABORA-INF-UFG/SAMURAI-IoT-Access **Autor: CIRO J. A. MACEDO**	Repositório de Código	Publicado
10	**Título:** *A Softwarized Perspective of 5G Networks* **Local:** IEEE CONFERENCE ON NETWORK SOFTWARIZATION NETSOFT 2020 **Página Oficial:** https://netsoft2020.ieee-netsoft.org/program/tutorials/ **GitHub:** https://github.com/LABORA-INF-UFG/NetSoft2020-Tutorial4 **Autores:** KLEBER VIEIRA CARDOSO, CRISTIANO BONATO BOTH, LUCIO RENE PRADE,**CIRO J. A. MACEDO**, VICTOR HUGO L. LOPES	Tutorial	Ministrado
8	**Título:** *Soft5G+: Explorando a Softwarização nas Redes 5G* **Local:** XXXVIII SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS **Página Oficial:** https://sol.sbc.org.br/livros/index.php/sbc/catalog/book/50 **Autores:** CRISTIANO BONATO BOTH, KLEBER VIEIRA CARDOSO, LUCIO RENE PRADE, VICTOR HUGO L. LOPES, **CIRO J. A. MACEDO**	Minicurso	Ministrado

7.2 Trabalhos futuros

Alguns pontos relevantes são sugeridos para trabalhos futuros no âmbito da tese. Em primeiro lugar, implementar uma versão em código aberto da TNGF, de modo a viabilizar o acesso confiável, representa uma oportunidade significativa para investigações adicionais. A TNGF, como uma função de rede que possibilita o acesso seguro ao núcleo 5G a partir de redes confiáveis não 3GPP, como o Wi-Fi em ambientes empresariais, pode oferecer uma arquitetura alternativa ou complementar ao caminho da N3IWF. Investigar os mecanismos de segurança, desempenho e interoperabilidade entre diferentes implementações de TNGF pode proporcionar uma compreensão mais abrangente das possibilidades de integração entre redes 5G e não 3GPP.

O acesso através da TWIF também não foi explorado no escopo deste trabalho. A TWIF oferece um caminho adicional para a integração de redes não 3GPP confiáveis, particularmente aquelas baseadas em WLAN, com o núcleo 5G. A investigação sobre como a TWIF pode ser utilizada para melhorar a resiliência, segurança e desempenho de sistemas de comunicação em ambientes urbanos densos ou em cenários industriais pode abrir novos horizontes para o desenvolvimento de arquiteturas mais robustas e escaláveis, adequadas a diferentes casos de uso na era das redes pós-5G.

Outra área promissora para pesquisas futuras é a agregação de observabilidade ao UE não 3GPP. Este trabalho fez contribuições significativas para esse aspecto. Entretanto, explorar mais profundamente como as métricas de desempenho geradas pelo UE não 3GPP podem ser utilizadas para otimizar a operação da rede seria um avanço importante. A incorporação dessas métricas em modelos de IA voltados para a melhoria do desempenho da rede e a gestão dinâmica de recursos pode resultar em redes mais eficientes e adaptativas, capazes de responder proativamente às mudanças no ambiente de rede e às demandas dos usuários. Além disso, a utilização das métricas disponibilizadas pelo UE não 3GPP para alimentar modelos de IA que melhorem o desempenho do núcleo 5G representa uma lacuna significativa a ser abordada. A aplicação de técnicas de aprendizado de máquina e análise preditiva, utilizando dados coletados em tempo real dos dispositivos, pode fornecer *insights* valiosos para a otimização de tráfego, gestão de interferências e até mesmo na prevenção de falhas. A criação de uma camada de IA que interaja diretamente com o núcleo 5G poderia revolucionar a forma como as redes são gerenciadas, elevando o conceito de *softwarização* de redes a um novo patamar.

É importante destacar que embora o UE não 3GPP represente um avanço significativo na integração de tecnologias não 3GPP com o núcleo 5G, ainda apresenta algumas características que limitam sua aplicabilidade em cenários mais complexos. Um dos principais desafios é a ausência de suporte à execução de múltiplos UEs não 3GPP a partir de uma única máquina, o que restringe a capacidade de simulação e

teste em ambientes de maior escala. Além disso, outra limitação está relacionada ao suporte a dispositivos IoT que não possuem a capacidade de executar o UE não 3GPP, o que dificulta a integração plena desses dispositivos em redes 5G. Essas limitações são oportunidades promissoras para pesquisa e desenvolvimento, com potencial para fortalecer ainda mais a convergência entre tecnologias não 3GPP e o núcleo 5G.

Em resumo, as áreas identificadas para trabalhos futuros não apenas preenchem as lacunas deixadas por este estudo, mas representam fronteiras promissoras para o avanço das redes de telecomunicações. A exploração dessas oportunidades de pesquisa tem o potencial de contribuir significativamente para o desenvolvimento de arquiteturas de rede mais robustas, seguras e eficientes, alinhadas às exigências de uma sociedade cada vez mais interconectada e dependente de tecnologias de comunicação avançadas.

Referências Bibliográficas

[3GPP TR-21.101 2009] 3GPP TR-21.101. *4G; Release 8*. 2009. https://www.3gpp.org/specifications/releases/72-release-8. [Último acesso: 8-jul-2024].

[3GPP TR-21.915 2018-12] 3GPP TR-21.915. *Technical Specification Group Services and System Aspects; Release 15 Description*. [S.l.], 2018–12. Version 0.5.0.

[3GPP TR-23.501 2021-12-23] 3GPP TR-23.501. *System architecture for the 5G System*. [S.l.], 2021–12–23. Version 17.3.0.

[3GPP TR-24.526 2024-04-02] 3GPP TR-24.526. *User Equipment policies for 5G System –Stage 3*. [S.l.], 2024–04–02. Version 18.6.0.

[3GPP TS-133.185 2017-10] 3GPP TS-133.185. *TS133.185: 3rd Generation Partnership Project Technical Specification Group Services and Systems Aspects Release 14 Description*. [S.l.], 2017–10. Version 14.1.0.

[3GPP TS-23.502 2024-03] 3GPP TS-23.502. *Technical Specification Group Services and System Aspects; Procedures for the 5G System; Release 18*. [S.l.], 2024–03. Version 18.5.0.

[3GPP TS-24.501 2024-04] 3GPP TS-24.501. *Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3*. [S.l.], 2024–04. Version 18.6.0.

[3GPP XR in 5G 2020] 3GPP XR in 5G. *Extended Reality (XR) in 5G*. [S.l.], December 2020.

[Abdelwahab et al. 2016] Abdelwahab, S. et al. Network function virtualization in 5G. *IEEE Communications Magazine*, v. 54, n. 4, p. 84–91, 2016.

[Aijaz 2020] AIJAZ, A. Private 5G: The Future of Industrial Wireless. *IEEE Industrial Electronics Magazine*, v. 14, n. 4, p. 136–145, 2020.

[al 2024] AL, I. B. et. *Weightless-P System specification*. 2024. https://pro-bee-user-content-eu-west-.s3.amazonaws.com/public/users/Integrators/929cb090-e779-401a-b06c-c629ff6b0fea/

ap-cambridgestartuplimi/Weightless-P_v1.03.pdf. [Último acesso: 30-mar-2024].

[Barb et al. 2022] BARB, G. et al. Analysis of Vegetation and Penetration Losses in 5G mmWave Communication Systems. In: IEEE. *2022 International Symposium on Electronics and Telecommunications (ISETC)*. [S.l.], 2022. p. 1–5.

[Bekele et al. 2018] BEKELE, M. K. et al. A Survey of Augmented, Virtual, and Mixed Reality for Cultural Heritage. *J. Comput. Cult. Herit.*, Association for Computing Machinery, New York, NY, USA, v. 11, n. 2, 2018.

[BNDES e MCTIC] BNDES e MCTIC. *BNDES e MCTIC, Internet das Coisas: um plano de ação para o Brasil*. Disponível em: <https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil>.

[Both et al. 2020] Both, C. B. et al. Soft5G+: explorando a softwarização nas redes 5G. In: ____. [S.l.]: MDPI, 2020. p. 49. ISBN 9786587003337.

[Chen et al. 2015] Chen, T. et al. Software defined mobile networks: concept, survey, and research directions. *IEEE Communications Magazine*, v. 53, n. 11, p. 126–133, 2015.

[Chen et al. 2024] Chen, Y. et al. LoRa Mesh-5G Integrated Network for Trackside Smart Weather Monitoring. *IEEE Transactions on Vehicular Technology*, p. 1–13, 2024.

[Chinchilla-Romero et al. 2023] CHINCHILLA-ROMERO, L. et al. URLLC Achieved Data Rate through Exploiting Multi-Connectivity in Industrial Private 5G Networks with Multi-WAT RANs. In: *2023 IEEE Wireless Communications and Networking Conference (WCNC)*. [S.l.: s.n.], 2023. p. 1–6.

[CLARITY 2022] CLARITY, G. *5G-CLARITY Deliverable D2.4 - Final System Architecture and Its Evaluation*. 2022. https://5gclarity.com/wp-content/uploads/2023/03/5G-CLARITY-D24-Amended.pdf. [Último acesso: 03-jun-2024].

[Cogalan et al. 2022] Cogalan, T. et al. 5G-CLARITY: 5G-Advanced Private Networks Integrating 5GNR, WiFi, and LiFi. *IEEE Communications Magazine*, v. 60, n. 2, p. 73–79, 2022.

[Duan et al. 2020] Duan, W. et al. Emerging Technologies for 5G-IoV Networks: Applications, Trends and Opportunities. *IEEE Network*, v. 34, n. 5, p. 283–289, 2020.

[Ericcson 2024] ERICCSON. *Mobile data traffic outlook*. 2024. https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/mobile-traffic-forecast. [Último acesso: 30-mar-2024].

[Ericsson 2024] ERICSSON, T. L. *Ericsson Mobility Report*. 2024. https://www.ericsson.com/en/reports-and-papers/mobility-report/. [Último acesso: 19-mar-2024].

[ETSI TS-123.501 2018-09] ETSI TS-123.501. *Technical Specification System Architecture for the 5G System ; Release 15 Description*. [S.l.], 2018–09. Version 15.3.0.

[ETSI TS-138.412 2018] ETSI TS-138.412. *5G – NG-RAN – NG signalling transport*. [S.l.], 2018.

[ETSI TS-24.526 2020] ETSI TS-24.526. *3GPP TS 24.526 version 16.4.0 Release 16 – User Equipment (UE) policies for 5G System (5GS); Stage 3*. [S.l.], 2020.

[Felix Richter 2024] Felix Richter. *5G Is Still in the Early Stages of Its Lifecycle*. 2024. https://www.statista.com/chart/9604/5g-subscription-forecast/. [Último acesso: 19-mar-2024].

[Foukas et al. 2017] Foukas, X. et al. Network slicing in 5G: Survey and challenges. *IEEE Communications Magazine*, v. 55, n. 5, p. 94–100, 2017.

[free5GC 2022] FREE5GC. *free5GC*. 2022. [Último acesso: 07-jun-2024]. Disponível em: <https://www.free5gc.org/>.

[Google 2022] GOOGLE. *Go*. 2022. [Último acesso: 24-jun-2024]. Disponível em: <https://go.dev/>.

[IEEE Std 802.11 2016] IEEE Std 802.11. IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, p. 1–3534, 2016.

[Inatel, MCTI e RNP 2024] INATEL; MCTI; RNP. *Brasil 6G*. 2024. [Último acesso: 16-jul-2024]. Disponível em: <https://inatel.br/brasil6g/>.

[ITU-R M.2083-0 2015] ITU-R M.2083-0, R. *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*. 2015. https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf.

[Kaloxylos 2018] Kaloxylos, A. A Survey and an Analysis of Network Slicing in 5G Networks. *IEEE Communications Standards Magazine*, v. 2, n. 1, p. 60–65, 2018.

[Khan et al. 2022] Khan, B. S. et al. URLLC and eMBB in 5G industrial IoT: A survey. *IEEE Open Journal of the Communications Society*, IEEE, v. 3, p. 1134–1163, 2022.

[Khanh et al. 2022] Khanh, Q. V. et al. Wireless communication technologies for IoT in 5G: Vision, applications, and challenges. *Wireless Communications and Mobile Computing*, Hindawi Limited, v. 2022, p. 1–12, 2022.

[Khorov et al. 2018] Khorov, E. et al. A tutorial on IEEE 802.11 ax high efficiency WLANs. *IEEE Communications Surveys & Tutorials*, IEEE, v. 21, n. 1, p. 197–216, 2018.

[Kozierok 2005] KOZIEROK, C. M. *The TCP/IP guide: a comprehensive, illustrated Internet protocols reference*. [S.l.]: No Starch Press, 2005.

[Kunz et al. 2020] KUNZ et al. Non-3GPP Access Security in 5G. *Journal of ICT Standardization*, v. 8, n. 1, p. 41–56, 2020.

[Lagen et al. 2020] LAGEN et al. Cellular and Wi-Fi in Unlicensed Spectrum: Competition leading to Convergence. In: *2020 2nd 6G Wireless Summit (6G SUMMIT)*. [S.l.: s.n.], 2020. p. 1–5.

[Lemes et al. 2022] Lemes, M. T. et al. A Tutorial on Trusted and Untrusted Non-3GPP Accesses in 5G Systems—First Steps Toward a Unified Communications Infrastructure. *IEEE Access*, IEEE, v. 10, p. 116662–116685, 2022.

[Lindqvist 2019] LINDQVIST, J. *Edge Computing for Mixed Reality*. Dissertação (Mestrado) — Linköping University, 2019.

[Linux Foundation 2023] Linux Foundation. *MAGMA*. 2023. [Último acesso: 24-jun-2024]. Disponível em: <https://magmacore.org/>.

[Linux Foundation 2024] Linux Foundation. *Linux Kernel Archives*. 2024. [Último acesso: 15-jul-2024]. Disponível em: <https://www.kernel.org/>.

[Luglio et al. 2022] LUGLIO, M. et al. Performance evaluation of untrusted non-3GPP Access to a 5G Core Network via satellite. In: *2022 International Symposium on Networks, Computers and Communications (ISNCC)*. [S.l.: s.n.], 2022. p. 1–6.

[Mach e Becvar 2017] MACH, P.; BECVAR, Z. Mobile Edge Computing: A Survey on Architecture and Computation Offloading. *IEEE Communications Surveys & Tutorials*, v. 19, n. 3, p. 1628–1656, 2017.

[Mademann 2018] MADEMANN, F. The 5G System Architecture. *Journal of ICT Standardization*, v. 6, n. 3, p. 77–86, 2018.

[Mendes et al. 2020] Mendes, L. L. et al. Enhanced Remote Areas Communications: The Missing Scenario for 5G and Beyond 5G Networks. *IEEE Access*, v. 8, p. 219859–219880, 2020.

[Mikhaylov et al. 2018] Mikhaylov, K. et al. Multi-RAT LPWAN in Smart Cities: Trial of LoRaWAN and NB-IoT Integration. In: *2018 IEEE International Conference on Communications (ICC)*. [S.l.: s.n.], 2018. p. 1–6.

[MongoDB Inc 2024] MongoDB Inc. *MongoDB*. 2024. [Último acesso: 02-jul-2024]. Disponível em: <https://www.mongodb.com/>.

[Navarro-Ortiz et al. 2018] Navarro-Ortiz, J. et al. Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things. *IEEE Communications Magazine*, v. 56, n. 2, p. 60–67, 2018.

[Nguyen et al. 2021] NGUYEN, A. et al. Implementation of a WiFi-based V2V-V2I communication unit for low speed vehicles. In: IEEE. *2021 International Conference on Advanced Technologies for Communications (ATC)*. [S.l.], 2021. p. 79–82.

[Nguyen et al. 2019] Nguyen, T. T. et al. Efficient design of chirp spread spectrum modulation for low-power wide-area networks. *IEEE Internet of Things Journal*, IEEE, v. 6, n. 6, p. 9503–9515, 2019.

[Noor-A-Rahim et al. 2022] Noor-A-Rahim, M. et al. 6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities. *Proceedings of the IEEE*, IEEE, v. 110, n. 6, p. 712–734, 2022.

[Ohrtman 2003] Ohrtman, F. Building 802.11 b Wireless Networks. *New York*, 2003.

[Open Air Interface 2023] Open Air Interface. *OAI-5G Core Network*. 2023. [Último acesso: 24-jun-2024]. Disponível em: <https://openairinterface.org/oai-5g-core-network-project/>.

[Open5GC 2019] OPEN5GC. *Open5GS*. 2019. [Último acesso: 07-jun-2024]. Disponível em: <https://open5gs.org/>.

[OpenSAND 2022] OPENSAND. *OpenSAND*. 2022. [Último acesso: 03-set-2024]. Disponível em: <https://www.opensand.org/>.

[Palattella et al. 2016] Palattella, M. R. et al. Internet of Things in the 5G Era: Enablers, Architecture, and Business Models. *IEEE Journal on Selected Areas in Communications*, v. 34, n. 3, p. 510–527, 2016.

[Penttinen 2021] PENTTINEN, J. T. *5G Second phase explained: The 3GPP Release 16 enhancements*. [S.l.]: John Wiley & Sons, 2021.

[Peralta-Ochoa et al. 2023] PERALTA-OCHOA, A. M. et al. Smart healthcare applications over 5G networks: a systematic review. *Applied Sciences*, MDPI, v. 13, n. 3, p. 1469, 2023.

[RedHat 2024] REDHAT. *Ansible*. 2024. [Último acesso: 02-jul-2024]. Disponível em: <https://www.ansible.com/>.

[Rommer et al. 2019] Rommer, S. et al. *5G Core Networks: Powering Digitalisation*. [S.l.]: Elsevier Science & Technology, 2019. ISBN 9780081030097.

[Roseti 2021] ROSETI, C. Integration of a non-3GPP satellite interface in a 5G multiple access configuration. In: *2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*. [S.l.: s.n.], 2021. p. 01–06.

[Semtech Corp. 2024] Semtech Corp. *What Is LoRa ®*. 2024. https://www.semtech.com/lora. [Último acesso: 29-mar-2024].

[Shafi et al. 2017] Shafi, M. et al. 5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice. *IEEE Journal on Selected Areas in Communications*, v. 35, n. 6, p. 1201–1221, 2017.

[srsRAN 2023] srsRAN. *srsRAN*. 2023. [Último acesso: 24-jun-2024]. Disponível em: <https://www.srslte.com/>.

[Sunny et al. 2021] Sunny, A. I. et al. Low-Cost IoT-Based Sensor System: A Case Study on Harsh Environmental Monitoring. *Sensors*, v. 21, n. 1, 2021. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/21/1/214>.

[Tataria et al. 2021] Tataria, H. et al. 6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities. *Proceedings of the IEEE*, v. 109, n. 7, p. 1166–1199, 2021.

[Team 2024] TEAM, G. *Gin Web Framework*. 2024. [Último acesso: 16-jul-2024]. Disponível em: <https://gin-gonic.com/>.

[Tebe et al. 2022] Tebe, P. I. et al. 5G-enabled medical data transmission in mobile hospital systems. *IEEE Internet of Things Journal*, IEEE, v. 9, n. 15, p. 13679–13693, 2022.

[Torroglosa-Garcia et al. 2020] Torroglosa-Garcia, E. M. et al. Enabling Roaming Across Heterogeneous IoT Wireless Networks: LoRaWAN MEETS 5G. *IEEE Access*, v. 8, p. 103164–103180, 2020.

[Toskala e Poikselkä 2020] TOSKALA, A.; POIKSELKÄ, M. 5G Architecture. *5G Technology: 3GPP New Radio*, Wiley Online Library, p. 67–86, 2020.

[TR-21.916 2024] TR-21.916, G. *Release 16*. 2024. https://www.3gpp.org/ftp/Specs/archive/21_series/21.916/21916-g20.zip. [Último acesso: 29-mai-2024].

[UnaBiz Pte Ltd 2024] UnaBiz Pte Ltd. *What is Sigfox 0G Technology*. 2024. https://www.sigfox.com/what-is-sigfox/. [Último acesso: 29-mar-2024].

[Vassis et al. 2005] Vassis, D. et al. The IEEE 802.11 g standard for high data rate WLANs. *IEEE network*, IEEE, v. 19, n. 3, p. 21–26, 2005.

[Weightless 2024] Weightless. *Open Weightless*. 2024. https://www.openweightless.org/. [Último acesso: 30-mar-2024].

[XFRM Linux Kernel 2024] XFRM Linux Kernel. *XFRM Linux Kernel*. 2024. [Último acesso: 15-jul-2024]. Disponível em: <https://docs.kernel.org/networking/xfrm_sync.html>.

[Xiao 2005] XIAO, Y. IEEE 802.11 n: enhancements for higher throughput in wireless LANs. *IEEE Wireless Communications*, IEEE, v. 12, n. 6, p. 82–91, 2005.

[Yadav et al. 2023] YADAV et al. A Flexible Architecture for Broadcast Broadband Convergence in Beyond 5G. In: *2023 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. [S.l.: s.n.], 2023. p. 1–6.

[Yang et al. 2022] Yang, C. et al. Using 5G in smart cities: A systematic mapping study. *Intelligent Systems with Applications*, Elsevier, v. 14, p. 200065, 2022.

[Yasmin et al. 2017] Yasmin, R. et al. On the integration of LoRaWAN with the 5G test network. In: *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. [S.l.: s.n.], 2017. p. 1–6.

[Zampognaro et al. 2024] ZAMPOGNARO, F. et al. Local Edge-Services through N3IWF in 5G Networks. In: *2024 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*. [S.l.: s.n.], 2024. p. 19–24.

[Zhang et al. 2020] Zhang, C. C. et al. Routing and Packet Scheduling in LORAWANs-EPC Integration Network. In: *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*. [S.l.: s.n.], 2020. p. 1–6.