MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES
INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

ESTUDO DA ARQUITETURA DE SEGURANÇA DA INFORMAÇÃO EM REDES 5G

Victor de Vasconcelos Carvalho

Relatório de Iniciação Científica do programa PIBIC, orientado pelo Dr. Edesio Paulicena.

INPE
São José dos Campos
2023

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES
INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

ESTUDO DA ARQUITETURA DE SEGURANÇA DA INFORMAÇÃO EM REDES 5G

Victor de Vasconcelos Carvalho

Relatório de Iniciação Científica do programa PIBIC, orientado pelo Dr. Edesio Paulicena.

INPE
São José dos Campos
2023

AGRADECIMENTOS

Gostaria de agradecer aos meus familiares, principalmente meus pais, Maria Barros de Vasconcelos Carvalho e Analdi Serrão de Carvalho, que me auxiliaram em todos os aspectos, compartilhando sua experiência e mostrando caminhos para a resolução dos problemas no dia a dia, que me permitiram chegar até aqui.

Agradeço também ao meu coorientador, Edésio Paulicena, por todo o suporte que me concedeu. Agradeço também a Andréa, que sempre comparece em nossas reuniões e somou com apontamentos valiosos.

Deixo aqui, minha gratidão a minha namorada, que me acompanhou e ajudou concluir esse projeto.

Por fim, exponho minha gratidão ao CNPq pelo suporte financeiro durante esse período, que possibilitou meu desenvolvimento na área acadêmica.

RESUMO

Este trabalho de pesquisa tem como tema o estudo da arquitetura de segurança da informação em redes 5G. Possui oito meses de duração até o presente momento, portanto, a pesquisa ainda segue em progresso. A finalidade deste trabalho é verificar os níveis de segurança dos elementos que compõem o núcleo da arquitetura do 5G. A verificação é realizada usando testes em um ambiente virtual. Com a chegada do 5G, torna-se evidente o aumento na complexidade da estrutura da rede, elevando o nível das possíveis ameaças e vulnerabilidades. Como consequência, serviços oferecidos poderão ser afetados, como por exemplo, a comunicação em larga escala entre dispositivos IoT. Ademais, o 5G possibilita uma troca de informações rápida e abrangente, o que significa que uma quantidade significativa de dados pessoais será transmitida por essas redes. Por meio deste trabalho, será possível verificar os níveis de segurança dos protocolos utilizados pelo 5G, verificar os serviços fornecidos e acompanhar a qualidade dos mesmos. Este trabalho foi desenvolvido em etapas, sendo elas, o estudo da arquitetura 5G, incluindo a evolução do sistema de telecomunicações; implementação de um ambiente virtual para alocar o simulador de redes 5G e o estudo da arquitetura para a verificação prática dos níveis de segurança da informação. Diante de tal exposto, neste momento foi iniciada a terceira fase do projeto, pela qual será realizada a verificação dos níveis de segurança adotando testes que serão realizados durante a comunicação entre as partes que integram o núcleo do 5G, além de verificar os resultados obtidos utilizando analisadores de tráfego.

Palavras-chave: 5G. Segurança da informação. IoT. Virtualização.

Lista de abreviaturas

3GPP	3rd Generation Partnership Project
5G-GUTI	5G-Global Unique Temporary Identity
AMF	Access and Mobility Management Function
AMPS	Analog Mobile Phone System
ASK	Amplitude Shift Keying
AUSF	Autentication Server Function
BASK	Binary Amplitude Shift Keying
Beamforming	Direcionamento de sinal para dispositivos específicos
BFSK	Binary Frequency Shift Keying
BPSK	Binary Phase Shift Keying
CN	Core Network
CRC	Cyclic Redundancy Check
DCI	Downlink Control Information
Downlink	Transmissão de dados no sentido torre-usuário
EDGE	Enhanced Data Rates for GSM Evolution
FDD	Frequency Division Duplex
FSK	Frequency Shift Keying
gNB	Estação Rádio Base
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HSDPA	High-Speed Downlink Packet Access
HDUPA	High-Speed Uplink Packet Access
IMEISV	International Mobile Equipment Identity Software Version
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
LTE	Long Term Evolution
MIB	Master Information Block
MIMO	Multiple Input Multiple Output
mmWave	millimeter Wave

MCS	Modulation and Coding Scheme
NAS	Network Access Stratum
NEF	Network Exposure Function
NF	Network Function
NGAP	NG Application Protocol
NRF	Network Repository Function
NSA NR	Non-Standalone New Radio
NSSF	Network Slice Selection Function
OFDM	Orthogonal Frequency Division Multiplexing
PBCH	Physical Broadcast Channel
PCF	Policy Control Function
PDSCH	Physical Downlink Shared Channel
PDU	Protocol Data Unit
Preâmbulo	sinal curto e aleatório enviado antes dos dados reais em uma transmissão
PSK	Phase Shift Keying
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RACH	Random Access Channel
RAN	Radio Access Network
RAN Sharing	Radio Access Network Sharing
RA-RNTI	Random Access Radio Network Temporary Identifier
Roaming	Envio e recebimento de dados fora da área de cobertura
RRC	Radio Resource Control
SA NR	Standalone New Radio
SBA	Service-Based Architecture
SC-FDMA	Single-Carrier Division Multiple Access
SMF	Session Management Function
SMS	Short Message Service
SUCI	Subscriber Concealed Identifier

SUPI	Subscription Identifier Concealing Function
TDD	Time Division Duplex
UDM	Unified Data Management
URLLC	Ultra-Reliable Low-Latency Communications
EU	User Equipment
UPF	User Plane Function
Uplink	Transmissão de dados no sentido usuário-torre

1 INTRODUÇÃO

1.1 O que é a rede 5G?

A rede 5G é a quinta geração de tecnologia móvel, proporcionando velocidades de internet significativamente mais rápidas, menor latência e maior capacidade de conexão para suportar um grande número de dispositivos simultâneos. Com essas melhorias, o 5G abre portas para novas aplicações, como realidade aumentada, IoT e automação industrial avançada, além de viabilizar a expansão de serviços baseados em nuvem, permitindo acesso rápido e eficiente a aplicativos e dados armazenados remotamente. Essa evolução promete revolucionar a forma como nos comunicamos, trabalhamos e interagimos com a tecnologia.

> 5G é a próxima geração de tecnologia sem fio programada para chegar em 2020. Uma vez aqui, o 5G deve ajudar as redes sem fio a fornecer mais largura de banda, maiores velocidades de dados e menor latência para muitos outros dispositivos eletrônicos. É também um dos tópicos mais sensacionalistas da tecnologia com entusiastas prometendo que será a porta de entrada para carros autônomos, realidade virtual e Internet das Coisas (IEEESPECTRUM,2020).

1.1 Porque estudar a segurança em redes 5G?

Com a implantação das redes 5G, a infraestrutura de comunicação se torna mais complexa, o que traz consigo um aumento potencial nas ameaças e vulnerabilidades à segurança da informação. Além da complexidade, há uma troca de informações mais rápida e abrangente na rede, o que implica na transmissão significativa de dados pessoais, e representa um risco adicional de comprometimento da segurança desses dados. Identificar e abordar vulnerabilidades se torna ainda mais crucial para garantir a proteção adequada dos sistemas e informações em meio a essa evolução tecnológica.

2 FUNDAMENTAÇÃO TEÓRICA

Esta seção do documento tem como propósito apresentar a base teórica fundamental para a compreensão aprofundada e a condução eficiente da pesquisa em foco. O exame detalhado das teorias relevantes permitirá uma contextualização adequada do problema em estudo, oferecendo uma visão clara das perspectivas existentes e estabelecendo o quadro conceitual que orientará as etapas subsequentes da pesquisa.

2.1 Estudo de arquitetura da rede 5G

Para compreendermos a arquitetura de segurança na rede 5G, faz se necessário o conhecimento de todas as partes envolvidas no processo de transmissão de dados na rede,

tendo início desde o primeiro contato do usuário na rede até a conexão massiva de de dados dos usuários na rede.

2.1.1 A evolução do sistema de telefonia móvel.

1G

O ano de 1980 marcou a criação e os primeiros testes do sistema de telefonia móvel, uma inovação que teve suas raízes no Japão. Cerca de quinze anos depois, por volta de 1995, essa revolução alcançava o Brasil, inaugurando assim a primeira geração de conexões sem fio para dispositivos móveis. Esse período ficou conhecido como a era do AMPS (Sistema de Telefone Móvel Analógico), caracterizado pelo uso exclusivo de sinais analógicos. Durante essa fase inicial, o foco era principalmente a transmissão de voz, possibilitando chamadas em movimento, apesar da ausência de segurança integrada ou roaming. O sistema operava em um ambiente totalmente analógico, sem os recursos de criptografia e autenticação presentes nas gerações subsequentes (SBRISSIA Helena, 2021).

2G

Na segunda metade da década de 90, a tecnologia de telefonia móvel chegou ao Brasil, trazendo consigo avanços significativos. Com base em tecnologia digital, essa nova era ofereceu maior segurança no espaço aéreo e introduziu capacidade de armazenamento em Kbytes. Dividida em três fases: GSM, GPRS e EDGE. Tais fases trazem consigo mudanças substanciais ao cenário da comunicação móvel. A fase GSM, fruto da colaboração entre países europeus, estabeleceu um padrão unificado de telefonia, viabilizando a popularização dos smartphones e reduzindo custos. O surgimento do SMS e do Sim Card também marcou essa fase.

Com a chegada do GPRS, os pacotes de dados passaram a ser tarifados conforme o volume transferido, não mais pelo tempo de conexão, permitindo o acesso à web pelo celular de maneira realmente utilizável. O sistema EDGE, por sua vez, evoluiu o GPRS, aumentando a velocidade de conexão em três vezes, embora mantivesse o alcance de sinal. No entanto, mesmo com melhor taxa de transferência, a latência permaneceu elevada (SBRISSIA Helena, 2021).

3G

A partir de dezembro de 2007, o Brasil testemunhou uma nova fase na evolução das redes móveis. Com taxas de download de 2Mbps para usuários parados e 384Kbps para usuários em movimento. Essa transformação foi dividida em três etapas distintas: HSDPA, HSUPA. A fase HSDPA trouxe consigo uma diminuição significativa no delay

do downlink, elevando a velocidade para 14Mbps. Com um protocolo que reduz a latência e amplia a taxa de download da rede, essa tecnologia se destacou em distâncias curtas, embora tenha se concentrado principalmente no aprimoramento da taxa de downlink.

Na sequência, a fase HSUPA entrou em cena, trazendo uma redução do delay no uplink. Complementando as taxas de downlink do HSDPA, essa fase melhorou as taxas de uplink, atingindo até 5.76Mbps. Assim como o HSDPA, o HSUPA também se destacou em distâncias mais curtas, contribuindo para uma experiência de comunicação móvel mais eficiente e veloz (SBRISSIA Helena, 2021).

4G

No final de 2012, uma transformação marcante atingiu o cenário das telecomunicações brasileiras com a chegada do LTE (Long Term Evolution), também conhecido como 4G. Essa evolução representou uma mudança abrangente, direcionando-se completamente ao transporte de pacotes de dados, revolucionando a forma como as comunicações móveis eram conduzidas. Um conceito utilizado em redes 4G foi a divisão da infraestrutura através do uso de RAN Sharing (Radio Access Network Sharing), permitindo uma utilização mais eficiente dos recursos, pois compartilham a infraestrutura de acesso ao rádio, ou seja, torres de celular, estações base e outros componentes. Ademais, o 4G inaugurou novos serviços, como aplicativos e serviços de streaming que mudaram a maneira como as pessoas interagiam e se comunicavam digitalmente.

A rede 4G trouxe consigo um modelo de células de cobertura interconectadas que se conectam a uma central, originando o sistema celular moderno. Opera também em diferentes faixas de frequência, com alocações bem definidas em TDD (Time Division Duplex) e FDD (Frequency Division Duplex). O TDD opera com os canais de uplink e downlink compartilhando a mesma frequência, com a transmissão e recepção alternando em intervalos de tempo distintos. Já o FDD os canais de uplink e downlink operam em frequências separadas, o que possibilita a transmissão e recepção de dados de forma contínua e simultânea (SBRISSIA Helena, 2021).

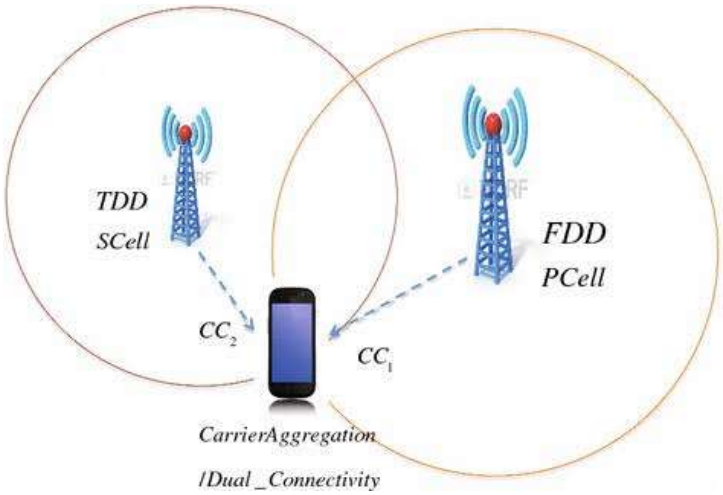
A chegada do 4G levou ou surgimento de novas tecnologias para atender a demanda da rede:

- Carrier agregation
- MIMO
- OFDMA
- SC-FDMA.

A rede LTE utiliza a modulação OFDMA (Ortogonal Frequency Division Multiple Access) para downlink, que se trata de uma técnica de modulação e acesso ao espectro de frequência na rede, através da divisão do espectro de frequência em subcanais menores e espaçados de maneira ortogonal para evitar interferências e permitindo alocação individual de espectro. E para uplink, a técnica usada é SC-FDMA (Single Carrier Frequency Division Multiple Access). Utiliza um único sinal de portadora para transmitir dados de um usuário específico. Quanto ao uplink, possui vantagens em relação ao OFDMA, uma vez que distribui a energia do sinal de maneira mais uniforme ao longo do espectro de frequência.

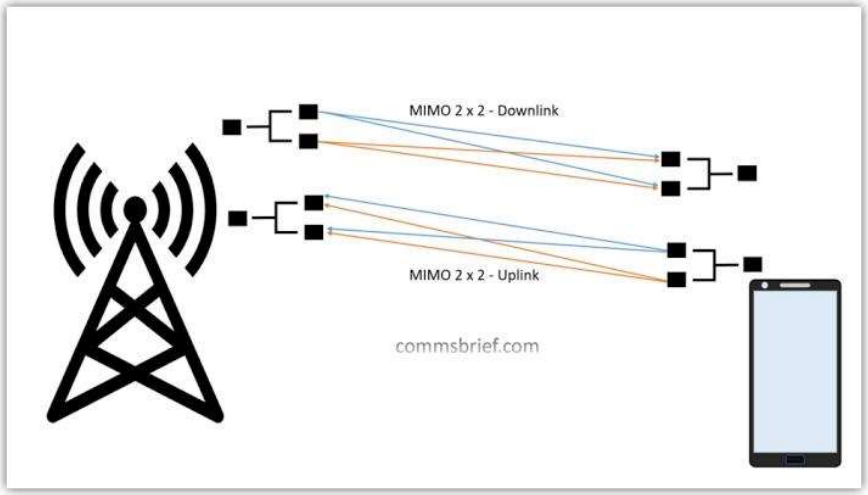
Carrier Agregation é uma tecnologia usada na comunicação sem fio para aumentar a taxa de dados por usuário, por meio da qual vários blocos de frequência são atribuídos ao mesmo usuário.

Representação de funcionamento do Carrier Agregation



O MIMO (Multiple-Input Multiple-Output) usa várias antenas conectadas no mesmo dispositivo que operam em conjunto para minimizar erros, otimizar a velocidade de dados e melhorar a capacidade de transmissão.

Representação do MIMO



2.1.1 O que é o 5G?

Como citado anteriormente, seu nome está relacionado a quinta geração de serviços da telecomunicação, trazendo mudanças para comunicação, frequência da rede e capacidade de transportar informações. Tem por objetivo expandir a conexão para o maior número de dispositivos possíveis, envolvendo redes móveis, carros, eletrodomésticos, educação, indústria entre outros.

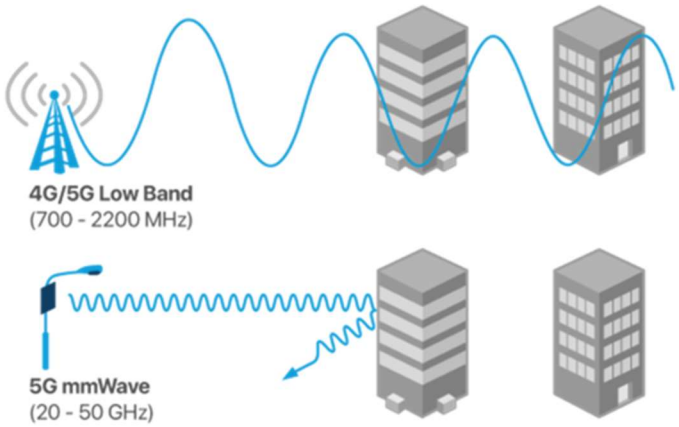
Quanto aos benefícios, a rede 5G conta com uma latência ultrabaixa, transferência de dados a estimados 20Gbps, implementação de SBA (Serviços Baseados em Nuvem) e utiliza um espectro de onda maior que as gerações anteriores.

Houve também o surgimento de novas tecnologias para atender a demanda da rede.

- Ondas milimétricas (mmWave).
- Células menores.
- MIMO massivo.
- Beamforming

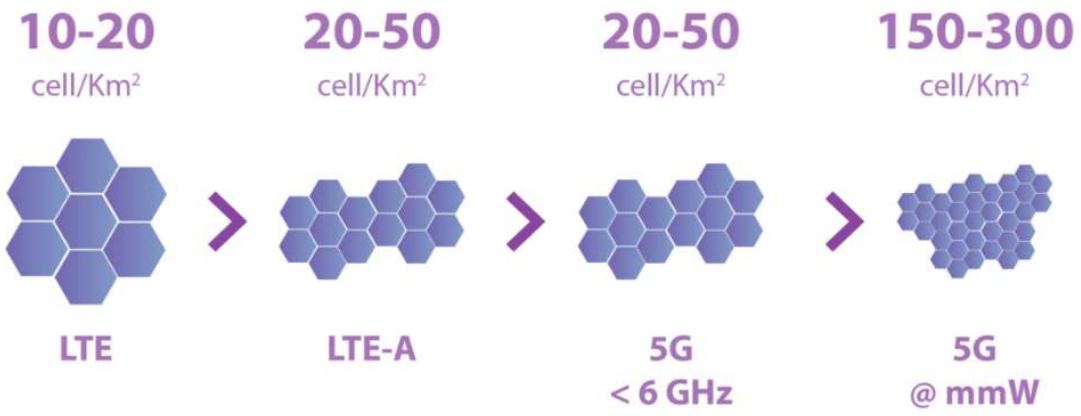
As Ondas milimétricas utilizadas em redes 5G atuam entre 24Ghz e 60Ghz de frequência. Essa faixa é significativamente mais alta do que as faixas utilizadas em gerações anteriores que operam entre 2.4Ghz e 5Ghz. Devido à alta frequência, as ondas milimétricas possuem podem transportar uma quantidade significativamente maior de dados. No entanto característica trás desafios para a implantação do 5G, uma vez que a alta frequência possui uma propagação menor, portanto, são mais suscetíveis a obstáculos físicos.

Representação das ondas milimétricas (mmWave)



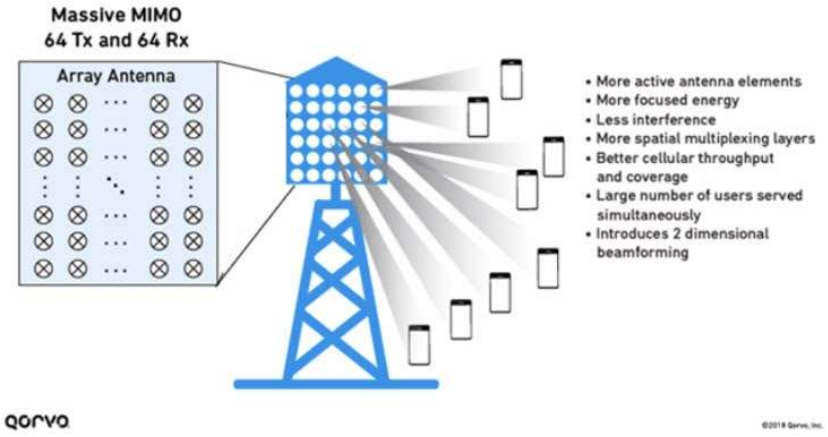
Devido a limitação de alcance do mmWave, as redes que utilizam tal tecnologia necessitam de um número maior de antenas para garantir uma cobertura de rede adequada. Por isso, o 5G utiliza o uso de células menores de cobertura para promover um melhor alcance e qualidade de sinal para os usuários. A cobertura de sinal por células menores possui como benefício uma maior capacidade de dispositivos conectados por km², o que promove um sinal de qualidade em áreas com maior densidade populacional, além de proporcionar o massivo IoT que é buscado pelo 5G.

Representação das células de cobertura



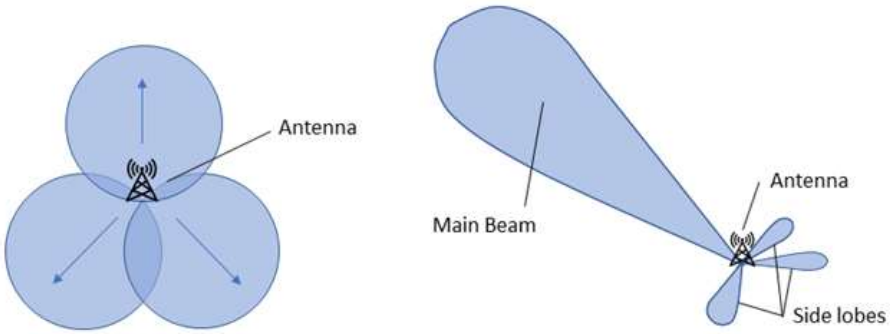
A rede 5G utiliza o MIMO massivo (Multiple Input Multiple Output). Essa tecnologia também é usada na rede 4G, pois envolve o uso de múltiplas antenas implantadas tanto no receptor quanto no transmissor. No 4Gcada torre possui cerca de 12 antenas, já o 5G utiliza centenas de antenas por torre, o que traz um aumento drástico na capacidade de conexão sem fio sem necessitar de mais espectro, uma vez que o sinal pode ser transmitido e recebido por várias trajetórias ao mesmo tempo.

Representação do MIMO massivo



O Beamforming é uma técnica utilizada no 5G para direcionar o sinal de transmissão de uma antena em uma direção específica, de forma a otimizar a intensidade do sinal na direção desejada e minimizar a interferência em outras direções.

Representação de um sinal emitido utilizando Beamforming



Sectored Antenna Array Beamforming Antenna Array

2.1.2 Implementação do 5G a IoT

O 5G catalisa o potencial do IoT ao oferecer uma conectividade excepcionalmente veloz e estável. Essa combinação permite que dispositivos interajam em tempo real, impulsionando a coleta e análise de dados instantâneos. Com uma latência mínima, o 5G amplia a eficiência do IoT, abrindo caminho para avanços revolucionários em áreas como automação industrial, cidades inteligentes e monitoramento de saúde remoto.

2.1.4 Arquitetura do 5G segundo o 3GPP

O 3GPP projeta a implementação do 5G através uma organização física e lógica da rede, com foco em realizar implementações baseadas em nuvem para atingir maiores taxas de transferência e menor latência.

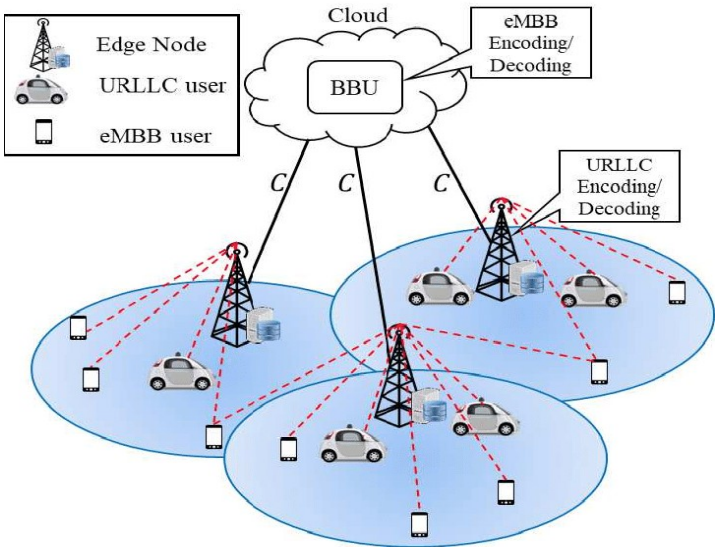
A arquitetura do 5G se divide em:

- RAN (Radio-Access Network).
- CN (Core Network).

2.1.4.1 RAN 5G

A RAN do 5G é uma parte fundamental da infraestrutura de comunicação, é responsável por estabelecer a conexão de comunicação entre dispositivos móveis. A RAN pode fornecer "suporte para serviços avançados de banda larga móvel, suporte para comunicações ultra confiáveis e de baixa latência (URLLC), e implementação de funções em nuvem (3GPP, 2021)". Ela é composta por antenas, estações de base, equipamentos de transmissão e recepção, e tecnologias de processamento de sinal, entre outros componentes.

Representação da RAN

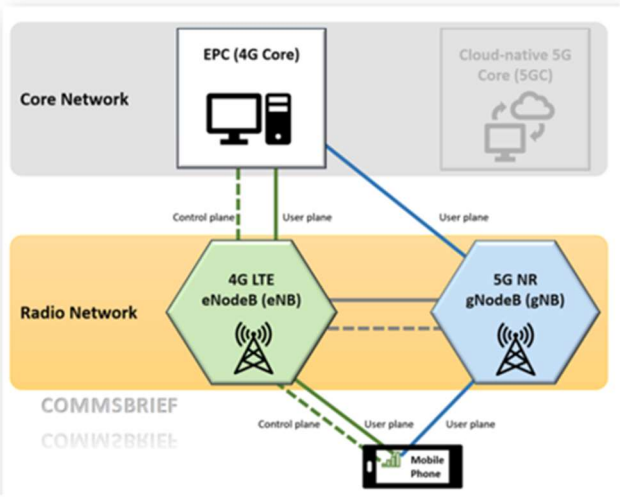


A RAN apresenta dois tipos de arquitetura:

- NSA NR (Non-Standalone New Radio)
- SA NR (Standalone New Radio)

A arquitetura NSA NR é um sistema híbrido, pois opera com dupla conectividade entre o LTE e o NR. Utiliza a conexão entre a RAN do 4G e do 5G, e se conecta com o core do 4G. É um modelo mais econômico, pois aproveita recursos de rede já instalados. É frequentemente utilizado por operadoras para disponibilizar os recursos do 5G, porém não explora seu potencial máximo devido a sua arquitetura híbrida.

Representação da arquitetura Standalone New Radio

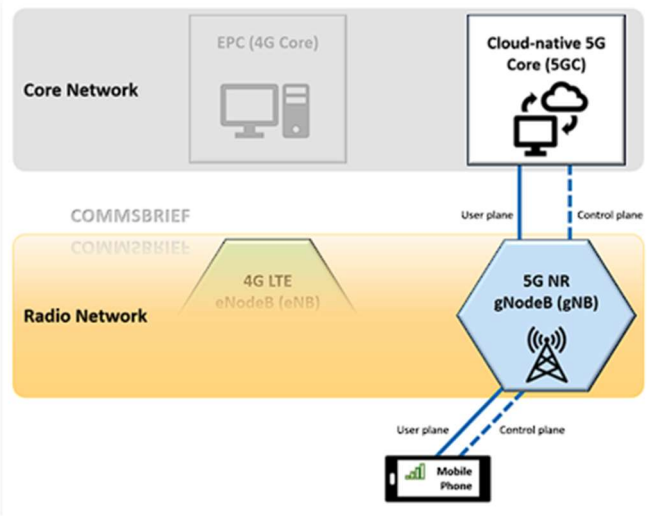


Já a arquitetura SA NR é um sistema autônomo, pois é constituído inteiramente de tecnologias do 5G. Realiza a conexão direta entre a RAN e o CN do 5G. O SA NR possibilita novas funcionalidades, como a Arquitetura Baseada em Serviços (Service Based Architecture, SBA) e o fatiamento de rede (Network slicing).

O network slicing refere-se à capacidade de criar múltiplas "fatias" virtuais em uma única infraestrutura de rede física. Cada fatia é uma porção isolada da rede que pode ser configurada e otimizada de forma independente para atender a requisitos específicos de aplicativos, serviços ou segmentos de clientes. Cada fatia tem sua própria alocação de recursos, topologia, latência, capacidade, segurança e outras características.

A arquitetura baseada em serviços (Service-Based Architecture, SBA) é um formato de design utilizado para as redes 5G. Nesse modelo, a rede é projetada em torno dos serviços que ela oferece, em vez de ser organizada em elementos de rede específicos, como ocorria nas gerações anteriores. Os diferentes componentes de rede são configurados de forma independente, mas estão interconectados e padronizados. Essa característica facilita a adaptação da rede à novos serviços, sem maiores complicações.

Representação da arquitetura Standalone New Radio

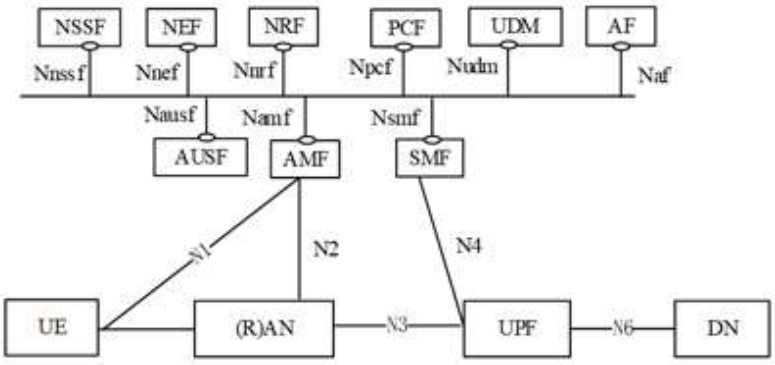


2.1.4.2 Core 5G

O Core do 5G sua arquitetura é alinhada a nuvem, e é responsável por funções não ligadas ao acesso dos recursos de rádio, mas necessárias para o funcionamento da rede, como Segurança, armazenamento de informações do dispositivo, configuração da conexão e disponibilização das funcionalidades de acordo com o contratado.

Para o seu funcionamento, o core 5G utiliza a arquitetura baseada em serviços da RAN. Os elementos da arquitetura são definidos em termos de "Network Function" (NF's), tais elementos são responsáveis por conectar as diferentes funções da rede. As funcionalidades suportadas são acessíveis via API (Interface de Programação da Aplicação).

Diagrama do núcleo do 5G



2.1.4.2.1 NF's do 5G

AMF (Access and Mobility Management Function) é o componente responsável pelo acesso e gerenciamento de mobilidade, fazendo a conexão inicial com o usuário (User Equipment, UE) e atuando como intermediário na solicitação com as demais NF's do

core. Oferece suporte a conexões de sinalização criptografadas, permitindo que o dispositivo se registre, seja autenticado e se mova pelas diferentes células na rede.

SMF (Session Management Function) gerencia as sessões dos equipamentos conectados à rede, estabelecendo, modificando e liberando as sessões individuais dos usuários. O SMF aloca um endereço de IP para cada usuário conectado, realiza a conexão indiretamente através da AMF e coleta dados de uso para implementar as funções da UPF (User Plane Function).

AUSF (Authentication Server Function) é responsável pela autenticação de equipamentos através das credenciais de acesso fornecidas pelo UDM (Unified Data Management). Realiza a autenticação através de criptografia para garantir o tráfego seguro de informações e o roaming (Manter a conectividade em movimento). O AUSF se comunica com o AMF, que solicita tais recursos de autenticação.

UPF (User Plane Function) é um elemento de encaminhamento de pacotes que processa e encaminha os dados do usuário. Executa políticas de rede, como: filtragem de pacotes, redirecionamento de tráfego e aplicação de limite de taxa de dados. Aplica recursos de qualidade e serviço, usado pela rede de transporte para fazer o gerenciamento de mobilidade da rede em caso de congestionamento. A UPF é controlada pelo SMF.

UDM (Unified Data Management) atua gerenciando os dados dos usuários na rede de forma centralizada e é responsável pelos protocolos de segurança. Realiza o registro, autenticação do usuário, aplicação de regras de acesso, autorização, etc. Interage diretamente com o AMF.

NSSF (Network Slice Selection Function) faz a seleção da rede dependendo do tipo de serviço solicitado e direciona para outra entidade de controle.

NEF (Network Exposure Function) realiza a troca de informações entre a interface do usuário e outros serviços.

PCF (Police Control Function) controla o tráfego de dados do usuário para que não exceda a capacidade que foi negociada com o portador.

NRF (Network Repository Function) realiza a listagem de todas as NF’s da rede e acompanha todos os serviços do núcleo, pois, cada NF precisa ser configurada individualmente com o endereço do NRF. É consultado por todas as outras NF’s.

2.1.5 Criptografia

Criptografia é a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser

decodificados ao formato original com o uso de uma chave de descriptografia específica. A criptografia permite a comunicação segura e privada entre duas ou mais partes, mesmo que a mensagem seja interceptada por terceiros.

2.1.5.1 Pilares da criptografia

A criptografia dispõe de três pilares fundamentais na sua composição

A confidencialidade é a premissa que garante a privacidade e a proteção dos dados contra acessos indevidos. Esse pilar visa assegurar o sigilo total de informações específicas, evitando que ações maliciosas exponham seu conteúdo. As medidas de confidencialidade devem ser persistentes e prevalecer em todo o tratamento das informações, e devem ser empenhadas principalmente na transmissão dos dados e em seu destino.

A disponibilidade visa manter os dados ativos e disponíveis para serem usados sempre que necessário. Entre as características da disponibilidade destacam-se a pontualidade, que pressupõe o desimpedimento dos dados no tempo necessário, e a robustez, que garante capacidade suficiente de acesso simultâneo para todos os usuários autorizados.

A integridade está associada à confiança e consistência dos dados. O foco maior está em garantir que as informações se mantenham exatas, sem erros e livres de alterações não autorizadas, para que possam ser empregadas de maneira segura. A integridade pode ser comprometida de várias maneiras. Por isso, cada vez que os dados são replicados ou transferidos, é preciso se certificar de que eles permanecerão intactos e inalterados.

2.1.5.2 Tipos de criptografia

Existem muitas formas diferentes de realizar a criptografia de dados, a seguir, serão explicados algumas das principais formas que estão relacionadas com o objeto de estudo em questão, a rede 5G, para então entendermos parte de como é feita a segurança da rede.

A Cifra é um algoritmo matemático que protege e codifica uma mensagem para proteger sua confidencialidade. A cifra transforma o texto original em uma sequência de caracteres aparentemente aleatórios, chamada de texto cifrado, que são ilegíveis para terceiros.

A Criptografia Simétrica, também conhecida como criptografia de chave, é um método que utiliza uma única chave para cifrar e decifrar uma mensagem, o que significa que o destinatário precisa ter a mesma chave que o remetente para acessar o conteúdo da mensagem. É uma abordagem eficiente e rápida, mas se torna limitada pela necessidade de compartilhar a chave de forma segura entre o remetente e o destinatário.

Criptografia Assimétrica ou criptografia de chave pública, utiliza um par de chaves diferentes para proteger a informação, uma chave pública e uma chave privada. A chave pública é disponibilizada para qualquer pessoa que deseje enviar uma mensagem criptografada para o proprietário, que possui a chave privada que é mantida em segredo. A mensagem é criptografada com a chave pública, tornando-se ilegível para qualquer pessoa que não possua a chave privada correspondente. É mais segura comparada a criptografia simétrica, porém é mais lenta e computacionalmente mais intensa.

A Criptografia Híbrida Combina a segurança da criptografia de chave pública com a eficiência da criptografia de chave simétrica. Na criptografia híbrida, uma chave de criptografia simétrica aleatória é gerada para cada mensagem a ser criptografada. A chave de criptografia simétrica é então criptografada usando uma chave pública, que é fornecida pelo destinatário da mensagem. A mensagem criptografada e a chave de criptografia simétrica criptografada são então enviadas ao destinatário. Ao receber a mensagem, o destinatário usa sua chave privada correspondente para descriptografar a chave de criptografia simétrica. Em seguida, ele usa essa chave para descriptografar a mensagem.

O Hash se refere a uma função matemática que transforma dados de entrada em uma sequência de caracteres alfanuméricos de tamanho fixo. Sua principal característica é que os números de hash são unidirecionais, ou seja, é fácil calcular o valor de hash a partir dos dados de entrada, mas é praticamente impossível reverter o processo e descobrir os dados de entrada a partir do valor de hash. São usadas em criptografia para proteger a integridade dos dados, pois qualquer alteração nos dados de entrada resultará em um valor de hash diferente. Assim, é possível verificar se os dados foram alterados, comparando o valor de hash original com o valor de hash calculado após a alteração.

Assinatura digital é uma técnica utilizada para verificar a autenticidade de um documento eletrônico, sendo possível garantir que o documento não foi alterado e que foi realmente criado pela pessoa ou entidade que alega ter criado. É criada usando uma chave privada que pertence ao signatário, que pode ser uma pessoa ou uma organização. Essa chave privada é usada para gerar uma assinatura digital única para cada documento. A assinatura digital é criptografada com a chave pública correspondente, que é fornecida ao destinatário juntamente com o documento original. Ao receber o documento juntamente

com a assinatura digital, o destinatário pode usar a chave pública para descriptografar a assinatura, e verificar se ela corresponde ao documento original.

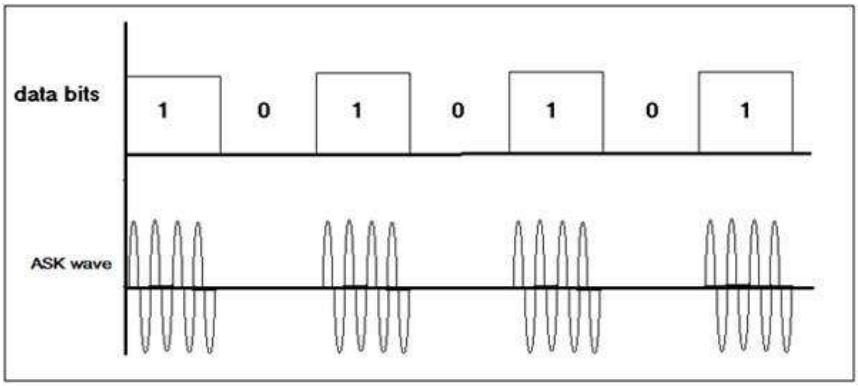
2.1.6 Modulação de onda

A modulação de onda é um processo utilizado em telecomunicações e transmissões de rádio com o propósito de transferir informações de um ponto a outro por meio da variação dos parâmetros de onda portadora. Isso permite que as informações sejam transmitidas de maneira eficiente através de diferentes meios de comunicação, como o ar, cabos ou fibras ópticas. Existem várias formas de modulação de onda, cada uma com suas características específicas.

2.1.6.1 Formas de modulação de onda

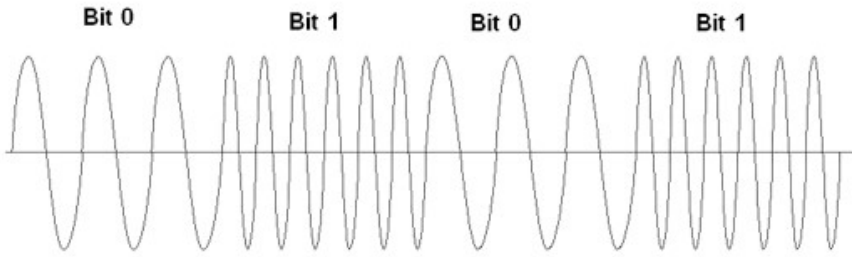
Modulação por Chaveamento de Amplitude (Amplitude Shift Keying, ASK) modifica a amplitude do sinal na portadora, enquanto a fase e frequência permanecem iguais. Pode ser implementado para representar vários níveis de sinal, cada um com uma amplitude diferente, embora, sua utilização mais comum, seja para representação de sinais binários. O sistema que utiliza apenas dois níveis de sinal é conhecido como BASK (Binary Amplitude Shift-Keying).

Representação da modulação de amplitude para representação de um sinal binário



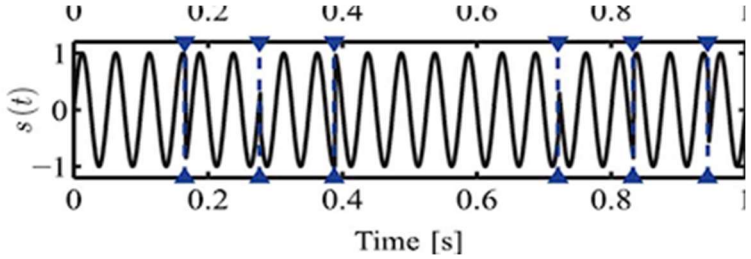
A Modulação por Chaveamento de Frequência (Frequency Shift Keying, FSK) modifica a frequência do sinal na portadora, enquanto a amplitude e fase permanecem inalterados. A frequência permanece constante para um elemento de sinal, mas varia para o elemento seguinte, caso seja diferente. Para que os filtros reconhecedores de frequência usados na recepção destes sinais possam reconhecer o bit é preciso transmitir pelo menos 3 ciclos do sinal. Utilizando apenas duas frequências na modulação de sinal, podemos chamá-la de BFSK (Binary Frequency Shift-Keying).

Representação da modulação de frequência para representação de um sinal binário

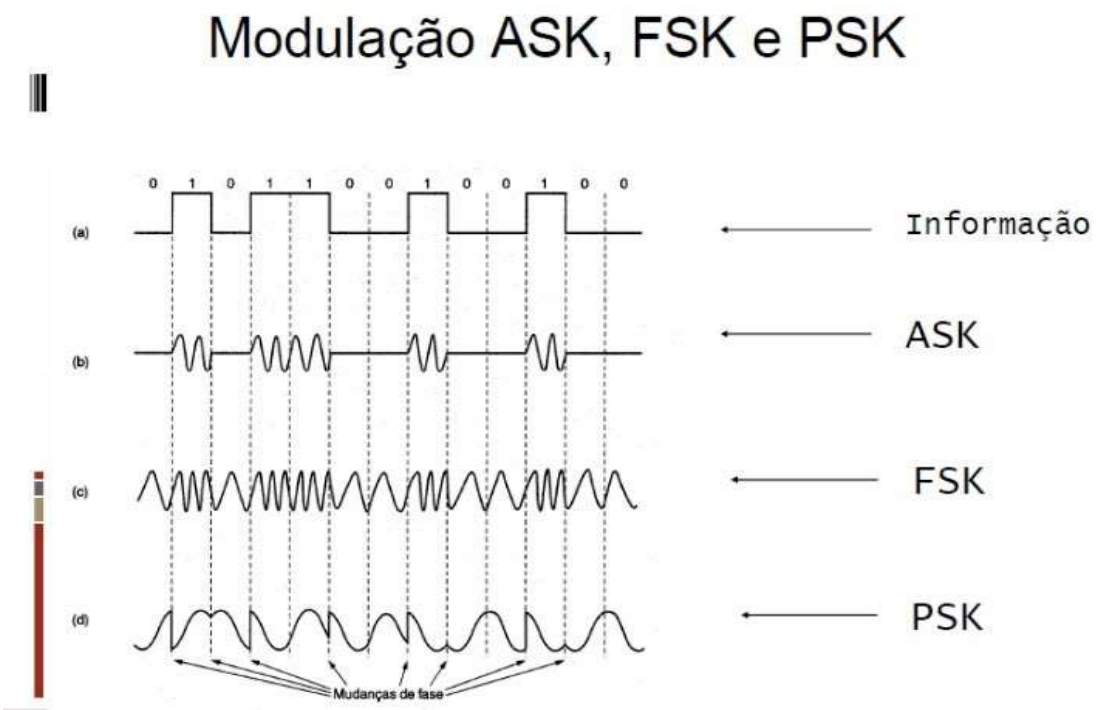


Na Modulação por Chaveamento de Fase (Phase Shift Keying) a fase da onda do sinal na portadora é modificada, enquanto a amplitude e frequência permanecem constantes. O PSK é mais comum e utilizado que o ASK e FSK. A modulação de sinal que utiliza apenas duas fases é chamada de BPSK (Binary Phase Shift-Keying).

Representação da modulação de fase para representação de um sinal binário



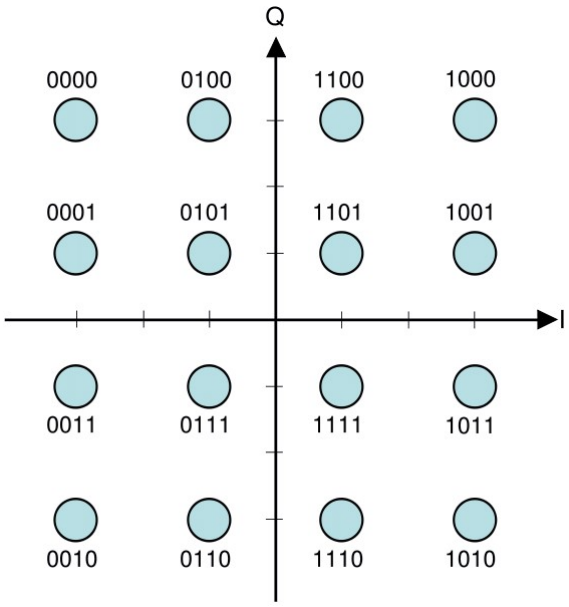
Comparação entre os tipos de modulação



O Diagrama de Constelação define a amplitude e a fase de um elemento de sinal, usando duas portadoras, uma em fase e outra em quadratura. Possui dois eixos, sendo um eixo x

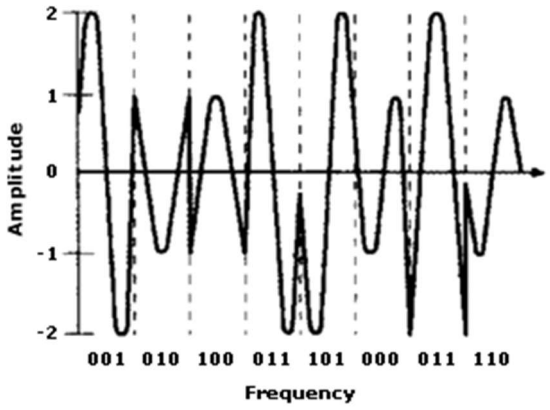
relacionado a portadora em fase, e um eixo Y relacionado a portadora em quadratura que são representados como um ponto no plano. A informação carregada por esse ponto(bit), é descrita próximo a ele, onde cada ponto no diagrama pode carregar quatro informações relacionadas a amplitude e fase. O eixo x define a amplitude do componente em fase e o eixo y define a amplitude do componente em quadratura. O vetor que conecta o ponto a origem representa a amplitude do elemento de sinal (resultante de x e y) e o ângulo que o vetor faz com o eixo x representa a fase do elemento de sinal.

Representação do diagrama de constelação



Há também a Modulação por Amplitude em Quadratura (Quadrature Ampliture Modulation, QAM), que é um tipo de modulação por amplitude em quadratura. As formas de modulação ASK, FSK e PSK alteram apenas uma das três características da onda senoidal por vez, já a QAM utiliza duas portadoras, uma em fase e outra em quadratura com diferentes níveis de amplitude para cada portadora. Portanto QAM é a combinação das modulações ASK e PSK, e possui inúmeras variações.

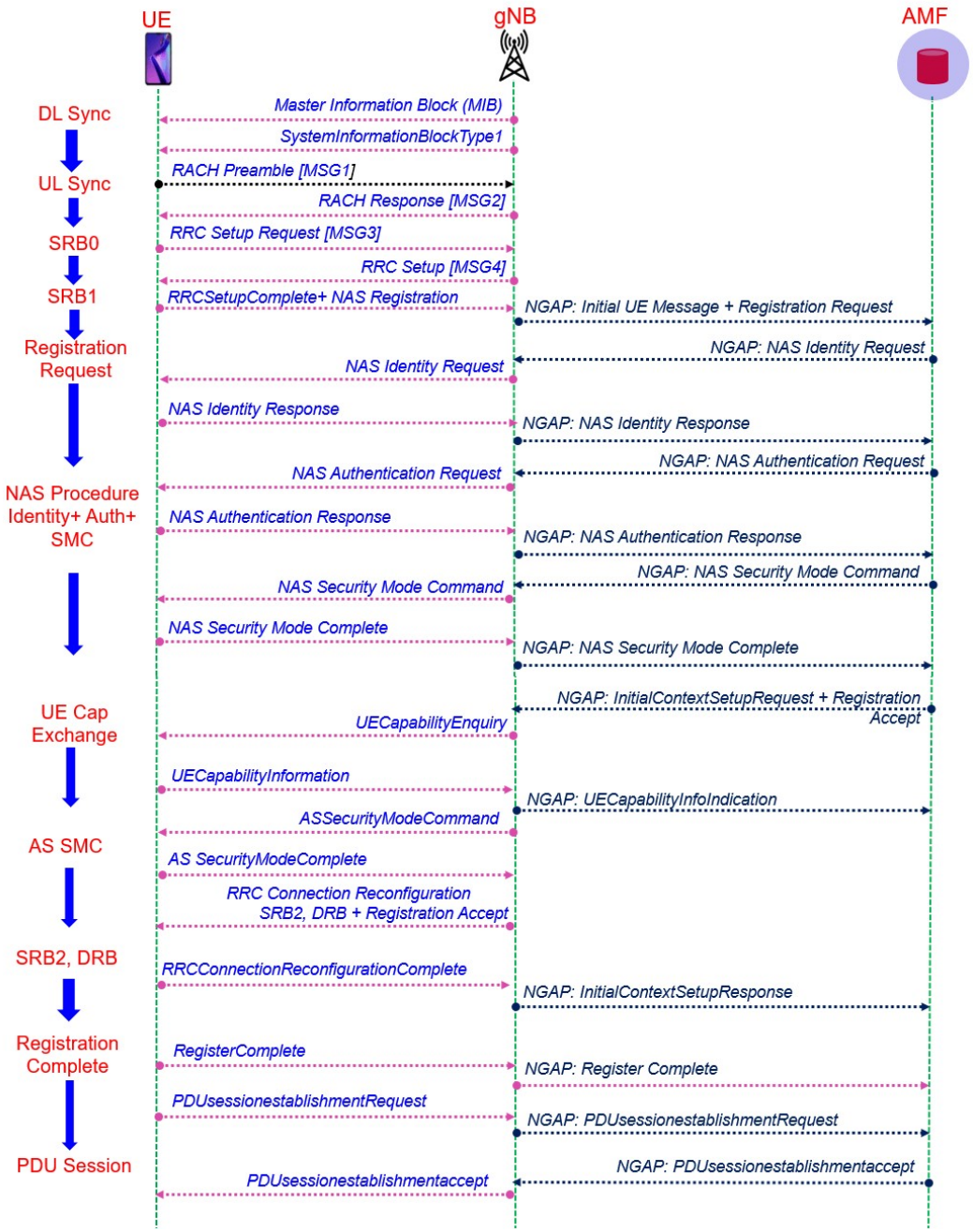
Representação da modulação QAM



2.1.7 Sequência de anexação inicial

A anexação inicial é o processo que ocorre quando queremos estabelecer a primeira conexão do dispositivo com a rede. No entanto, se ocorrerem eventos específicos, como troca de operadora ou expiração de uma sessão, um novo "initial attach sequence" pode ser necessário para estabelecer novamente o registro e autenticação do UE com a rede. Existem diversos procedimentos que ocorrem durante a anexação inicial.

Diagrama representando o fluxo de sinalização no processo de anexação inicial



A pesquisa de célula e sincronização de downlink é o procedimento pelo qual um UE adquire sincronização de tempo e frequência com uma célula, decodifica a ID da célula e as informações de PBCH (Physical Broadcast Channel) que é um canal físico usado para transmitir o MIB (Master Information Block), e este por sua vez contém informações essenciais para que os dispositivos possam ser sincronizados a rede.

O UE realiza a sincronização UL (Uplink) pelo Procedimento RACH, onde o UE seleciona um preâmbulo (sinal curto e aleatório enviado antes dos dados reais em uma transmissão, msg#1), e também inicia uma temporização T300 para aguardar a mensagem de configuração RRC (Radio Resource Control) do gNB.

O gNB detecta a primeira mensagem de RACH (Msg#1) enviada por um dispositivo e responde enviando uma informação de controle de enlace descendente (Downlink Control Information, DCI) codificada com um Verificador de Redundância Cíclica (Cyclic Redundancy Check, CRC) que por sua vez, está codificado pelo Identificador Temporário de Rede de Acesso Aleatório (Random Access Radio Network Temporary Identifier, RA-RNTI). O DCI enviado ao EU contém atribuição de recursos de frequência e tempo, bem como um Esquema de Modulação e Codificação (Modulation and Coding Scheme, MCS, Msg#2) que será enviada no Canal Físico Compartilhado de Enlace Descendente (Physical Downlink Shared Channel, PDSCH).

A solicitação de Controle de Recursos de Rádio (Radio Resource Control, RRC) é realizada na (Msg#3) e inclui a identificação do usuário, que pode ser um número aleatório e será usado pelo UE para resolver disputas enquanto decodifica a configuração de conexão RRC (Msg#4).

Na fase RRC setup Complete + NAS Registration, o UE envia a mensagem “RRC Setup Complete” junto com “Registration Request” na mensagem NAS (Network Access Stratum) dedicada. A solicitação de registro também carrega informações de capacidade de rede do UE. O gNB seleciona o AMF para esta sessão e aloca NGAP (NG Application Protocol) para o UE.

Ao chegar a fase “Initial UE Message”, o gNB a envia para o AMF. A mensagem carrega o pedido de registro recebida do UE dentro da mensagem “RRC Setup Complete”. O NGAP também é incluído na mensagem.

A transferência de identidade do UE é condicional. Se houver uma alteração no último AMF selecionado pelo gNB e o SUCI não for fornecido pelo UE nem recuperado do AMF antigo, o procedimento de Solicitação de Identidade é iniciado pelo AMF enviando uma mensagem de Solicitação de Identidade para o UE solicitando o Identificador Oculto de Assinatura (Subscriber Concealed Identifier, SUCI). O UE responde com “Identity Response” incluindo o SUCI.

Na fase de Autenticação e Segurança NAS, o Core executa o procedimento de Autenticação para que o UE seja legítimo e legalmente autorizado a obter serviço da rede. O AMF sinaliza o algoritmo de segurança NAS selecionado para o UE e solicita o IMEISV (International Mobile Equipment Identity Software Version) do UE como parte

do comando do modo de segurança NAS. O UE responde com a conclusão do procedimento de segurança do NAS e contém o IMEISV no modo de segurança completo.

Na fase “Initial Context Setup Request” O AMF aloca um NGAP, que será usado pelo gNB para endereçar o contexto do UE no AMF. O AMF envia uma mensagem “INITIAL CONTEXT SETUP REQUEST” ao gNB para iniciar o processo inicial de estabelecimento da sessão. A mensagem geralmente contém a mensagem NAS de aceitação de registro e carrega uma ou mais solicitações de configuração de sessão de PDU. A mensagem também carrega o “AMF UE NGAP ID”, “UE Aggregate Maximum Bit Rate”, recursos de segurança do UE e chave de segurança.

O gNB consulta informações de capacidade do EU e, depois de receber a resposta, atualiza o AMF. O gNB envia também uma mensagem de Comando de Modo de Segurança para que o UE inicie o processo de criptografia e proteção de integridade. O UE deriva a chave de acordo com a proteção de integridade e o algoritmo de criptografia indicado pela mensagem Security Mode Command e, em seguida, responde à mensagem Security Mode Complete ao gNB.

O gNB emite uma mensagem de reconfiguração RRC até o UE para estabelecer SRB2 (Second Signaling Radio Baerer) e DRB (Data Radio Baerer). Depois que o SRB2 e o DRB são estabelecidos com sucesso, o UE responde ao gNB com uma mensagem “RRC Reconfiguration Complete. O gNB sinaliza o DRB de configuração bem-sucedida com a mensagem “INITIAL CONTEXT SETUP RESPONSE” para o AMF.

Por fim, na fase “Register Complete e PDU Session Stablishment Request” o UE envia a solicitação de Registro Completo e de estabelecimento de sessão de PDU para o AMF. O AMF envia uma mensagem “PDU SESSION RESOURCE SETUP REQUEST” para gNB contendo a lista de sessões PDU (Protocol Data Unit) que precisam ser estabelecidas, a lista de QoS (Quality Of Service) para cada sessão PDU. O gNB mapeia o fluxo de QoS e envia ao UE a mensagem “PDU Session Stablishment Accept”.

2.1.8 5G AKA

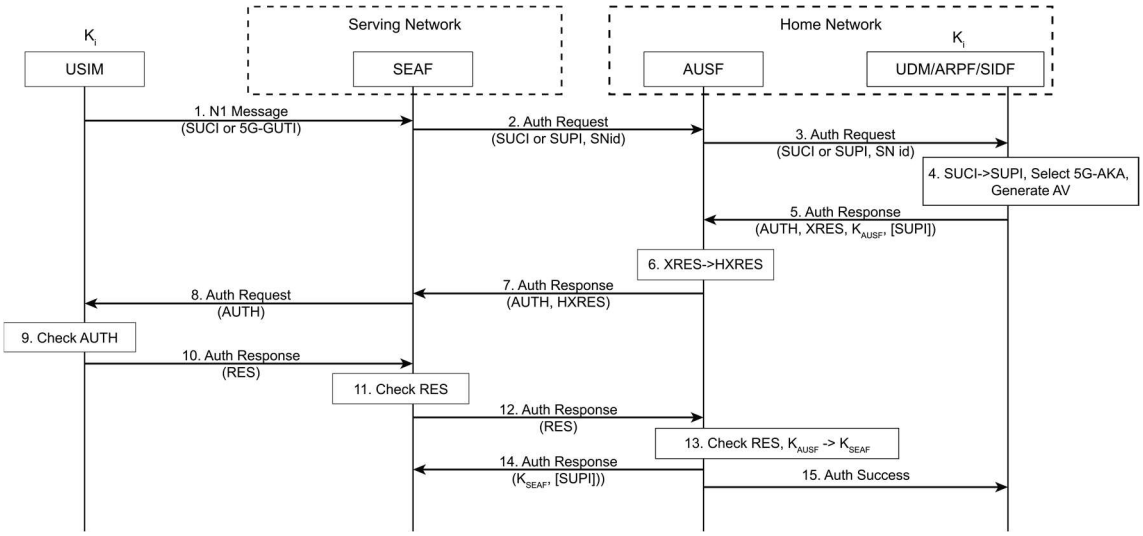
A arquitetura baseada em serviços (SBA) foi proposta para a rede 5G, assim, novas entidades e novas solicitações de serviço também foram definidas no 5G, como a Função de Âncora de Segurança (SEAF), Função de Servidor de Autenticação (AUSF), o Gerenciamento Unificado de Dados (UDM) e a Função de Ocultação do Identificador de Subscrição (SIDF).

O SEAF atua como "intermediário" durante o processo de autenticação entre uma UE e sua rede doméstica. Ele pode rejeitar uma autenticação da UE, mas depende da rede doméstica da UE para aceitar a autenticação. O AUSF toma a decisão sobre a autenticação do UE, mas depende de outros serviços para calcular os dados de autenticação quando 5G-AKA é usado.

O UDM é a entidade que hospeda funções relacionadas ao gerenciamento de dados, como o ARPF (Repositório de Credenciais de Autenticação e Função de Processamento), que seleciona um método de autenticação com base na identidade do assinante e na política configurada, após isso, calcula os dados de autenticação e os materiais de chaveamento para o AUSF, se necessário.

O SIDF desencripta o SUCI (Identificador Oculto de Subscrição) para obter a sua identidade a longo prazo, chamada de SUPI (Identificador Permanente de Subscrição), por exemplo, o IMSI (Identidade Internacional de Assinante Móvel). No 5G, uma identidade de longo prazo do assinante é sempre transmitida através das interfaces de rádio de forma criptografada. Mais especificamente, uma criptografia baseada em chave pública é usada para proteger o SUPI. Portanto, somente o SIDF tem acesso à chave privada associada a uma chave pública distribuída aos UEs para criptografar seus SUPIs.

Nas redes 5G a autenticação por meio do 5G AKA ocorre de acordo com o diagrama



No 5G-AKA, o SEAF (Função de âncora de segurança) pode iniciar o procedimento de autenticação após receber qualquer mensagem de sinalização do UE deve enviar ao SEAF um identificador temporário, um 5G-GUTI (Identidade temporária globalmente exclusiva) ou um SUCI (Identificador oculto de inscrição) se um 5G-GUTI não tiver sido alocado pela rede servidora para o UE. O SUCI é a forma criptografada do SUPI (Identificador Permanente de Assinatura) usando a chave pública da rede doméstica. Assim, o identificador permanente de um UE, por exemplo, o IMSI (identidade de assinante móvel internacional), nunca é enviado em texto não criptografado pelas redes de 5G.

O SEAF inicia a autenticação enviando uma solicitação de autenticação para o AUSF, que primeiro verifica se a rede servidora solicitando o serviço de autenticação está autorizada.

Após o sucesso, o AUSF envia uma solicitação de autenticação para UDM/ARPF (gerenciamento unificado de dados/ Repositório de credenciais de autenticação e Função de processamento).

Se um SUCI (Identificador oculto de inscrição) for fornecido pelo AUSF, o SIDF (Função de ocultação do identificador de assinatura) será invocado para descriptografar o SUCI e assim obter o SUPI (Identificador Permanente de Assinatura), que é usado posteriormente para selecionar o método de autenticação configurado para o assinante. Neste caso, o 5G-AKA será utilizado.

O UDM/ARPF inicia o 5G-AKA enviando a resposta de autenticação ao AUSF com um vetor de autenticação que consiste em um token AUTH (token de autenticação), um token XRES (token de resposta esperado), a chave K AUSF (chave utilizada para derivar outras chaves para autenticação e encriptação) e o SUPI, se o SUCI for incluído no pedido de autenticação.

O AUSF recebe o XRES e calcula o HXRES (hash do token de resposta esperado). Após isso, o AUSF armazena o K AUSF e envia a resposta de autenticação ao SEAF, juntamente com o token AUTH e o HXRES. O SUPI não é enviado ao SEAF nesta resposta de autenticação. Ele só é enviado para o SEAF após a autenticação do UE ser bem-sucedida.

O SEAF armazena o HXRES e envia o token AUTH para o EU, que valida o token AUTH usando a chave secreta que compartilha com a rede doméstica. Se a validação for bem-sucedida, o UE considera a rede como autenticada.

O UE continua a autenticação computando e enviando ao SEAF um token RES (token de resposta, que é validado pelo SEAF. Após a validação, o token RES é enviado pelo SEAF ao AUSF para validação. OBS: AUSF, que está em uma rede doméstica, toma a decisão final sobre a autenticação.

Se o token RES do UE for válido, o AUSF usa o K AUSF (chave utilizada para derivar outras chaves para autenticação e encriptação) para calcular uma a K SEAF (chave âncora). O AUSF envia a K SEAF para o SEAF, juntamente com o SUPI (Identificador Permanente de Assinatura), se aplicável. O AUSF também informa o UDM/ARPF dos resultados da autenticação para que eles possam registrar os eventos.

3 METODOLOGIA

Nesta seção, abordaremos a metodologia que foi utilizada para a instalação do simulador de rede 5G, destacando passos essenciais como a escolha do software de virtualização, a configuração da máquina virtual, o simulador de redes e a ferramenta de gerenciamento e criação de múltiplas máquinas virtuais.

3.1.1 Criação do ambiente de testes

A VirtualBox oferece flexibilidade na criação de ambientes virtuais, suporte a diversos sistemas operacionais e uma interface intuitiva. Para esse projeto foi utilizado a VirtualBox, que é um ambiente para criação de máquinas virtuais desenvolvida pela Oracle. Vale destacar, que a aplicação do simulador de redes funciona também em outras aplicações de máquinas virtuais.

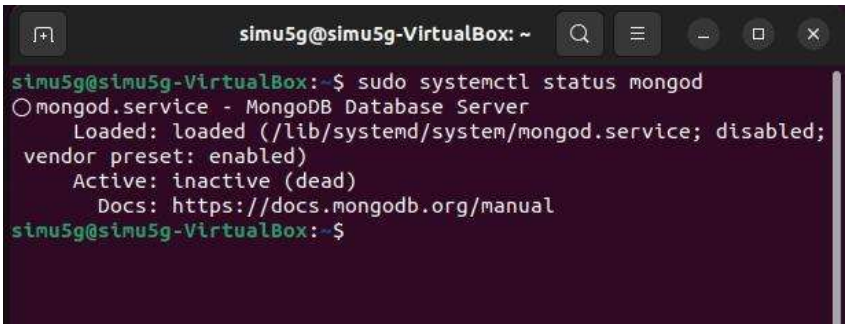
3.1.2 Instalação e configuração do simulador

O simulador de redes escolhido foi o Open5GS devido a clareza na documentação e suporte. A sua instalação é feita via terminal do Linux, seguindo a sequência de procedimentos descritos no apêndice 1.

3.1.3 Testes iniciais usando o simulador.

Durante o processo de instalação do Open5GS, é possível executar testes para a verificação de suas funcionalidades à medida que são implantadas.

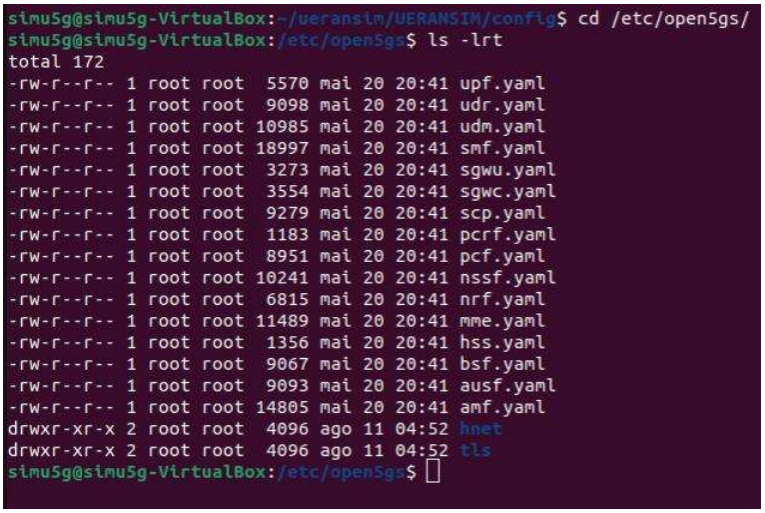
Verificação de status do MongoDB (banco de dados)



Habilitando o serviço MongoDB

Além do serviço MongoDB, é possível consultar os arquivos de instalação que contém as NFs do 5G, bem como verificar seu funcionamento.

Consulta de arquivos locais contendo as NFs

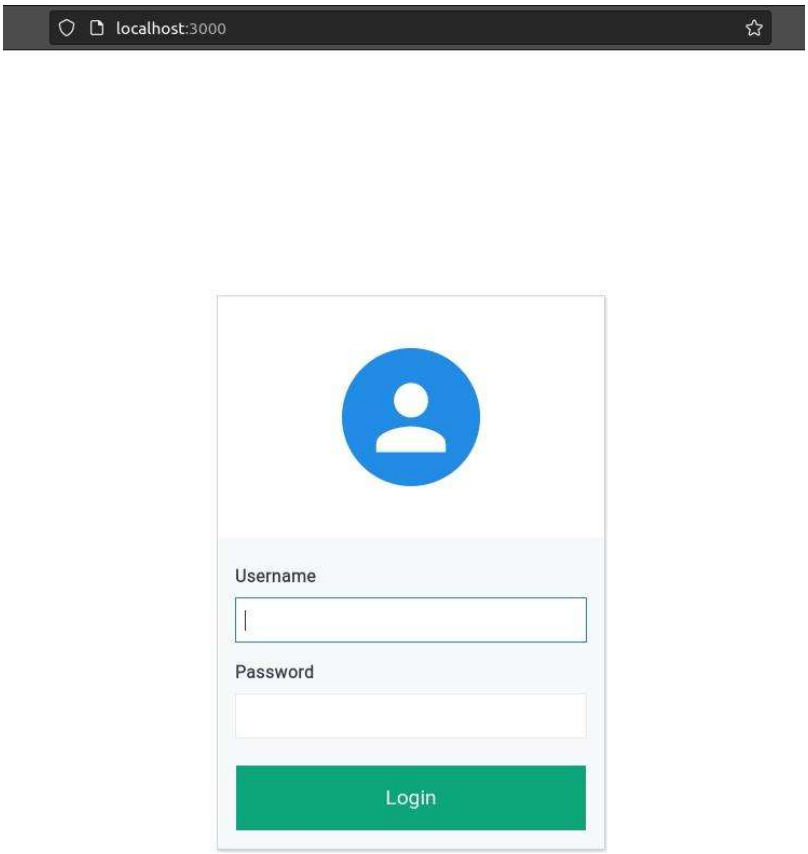


Verificação de status das NFs

```
ago 11 04:52:36 simu5g-VirtualBox open5gs-upfd[10171]: 08/11 04

● open5gs-amfd.service - Open5GS AMF Daemon
     Loaded: loaded (/lib/systemd/system/open5gs-amfd.service;
     Active: active (running) since Fri 2023-08-11 04:52:30 -03
   Main PID: 9962 (open5gs-amfd)
      Tasks: 2 (limit: 7003)
     Memory: 6.1M
        CPU: 13ms
     CGroup: /system.slice/open5gs-amfd.service
             └─9962 /usr/bin/open5gs-amfd -c /etc/open5gs/amf.y

ago 11 04:52:41 simu5g-VirtualBox open5gs-amfd[9962]: 08/11 04:
ago 11 04:52:41 simu5g-VirtualBox open5gs-amfd[9962]: 08/11 04:
ago 11 04:52:41 simu5g-VirtualBox open5gs-amfd[9962]: 08/11 04:
ago 11 04:52:41 simu5g-VirtualBox open5gs-amfd[9962]: 08/11 04:
ago 11 04:52:41 simu5g-VirtualBox open5gs-amfd[9962]: 08/11 04:
ago 11 04:52:41 simu5g-VirtualBox open5gs-amfd[9962]: 08/11 04:
ago 11 04:52:41 simu5g-VirtualBox open5gs-amfd[9962]: 08/11 04:
ago 11 04:52:41 simu5g-VirtualBox open5gs-amfd[9962]: 08/11 04:
ago 11 04:52:42 simu5g-VirtualBox open5gs-amfd[9962]: 08/11 04:
ago 11 04:52:42 simu5g-VirtualBox open5gs-amfd[9962]: 08/11 04:

● open5gs-ausfd.service - Open5GS AUSF Daemon
     Loaded: loaded (/lib/systemd/system/open5gs-ausfd.service;
     Active: active (running) since Fri 2023-08-11 04:52:38 -03
   Main PID: 10695 (open5gs-ausfd)
      Tasks: 2 (limit: 7003)
     Memory: 4.6M
        CPU: 7ms
     CGroup: /system.slice/open5gs-ausfd.service
             └─10695 /usr/bin/open5gs-ausfd -c /etc/open5gs/aus

ago 11 04:52:38 simu5g-VirtualBox open5gs-ausfd[10695]: Open5GS
ago 11 04:52:38 simu5g-VirtualBox open5gs-ausfd[10695]: 08/11 0
ago 11 04:52:38 simu5g-VirtualBox open5gs-ausfd[10695]: 08/11 0
ago 11 04:52:38 simu5g-VirtualBox open5gs-ausfd[10695]: 08/11 0
ago 11 04:52:38 simu5g-VirtualBox open5gs-ausfd[10695]: 08/11 0
ago 11 04:52:38 simu5g-VirtualBox open5gs-ausfd[10695]: 08/11 0
ago 11 04:52:38 simu5g-VirtualBox open5gs-ausfd[10695]: 08/11 0
ago 11 04:52:38 simu5g-VirtualBox open5gs-ausfd[10695]: 08/11 0
ago 11 04:52:41 simu5g-VirtualBox open5gs-ausfd[10695]: 08/11 0
ago 11 04:52:41 simu5g-VirtualBox open5gs-ausfd[10695]: 08/11 0

● open5gs-nrfd.service - Open5GS NRF Daemon
     Loaded: loaded (/lib/systemd/system/open5gs-nrfd.service;
     Active: active (running) since Fri 2023-08-11 04:52:32 -03
   Main PID: 10079 (open5gs-nrfd)
      Tasks: 2 (limit: 7003)
     Memory: 4.8M
        CPU: 20ms
     CGroup: /system.slice/open5gs-nrfd.service
             └─10079 /usr/bin/open5gs-nrfd -c /etc/open5gs/nrf.

ago 11 04:52:41 simu5g-VirtualBox open5gs-nrfd[10079]: 08/11 04
ago 11 04:52:41 simu5g-VirtualBox open5gs-nrfd[10079]: 08/11 04
```

O ambiente do Open5GS proporciona a simulação de conexão na rede, pois gera um localhost e um usuário com IMSI, este endereço pode ser usado para conectar o usuário ao localhost e realizar a conexão entre ambos.

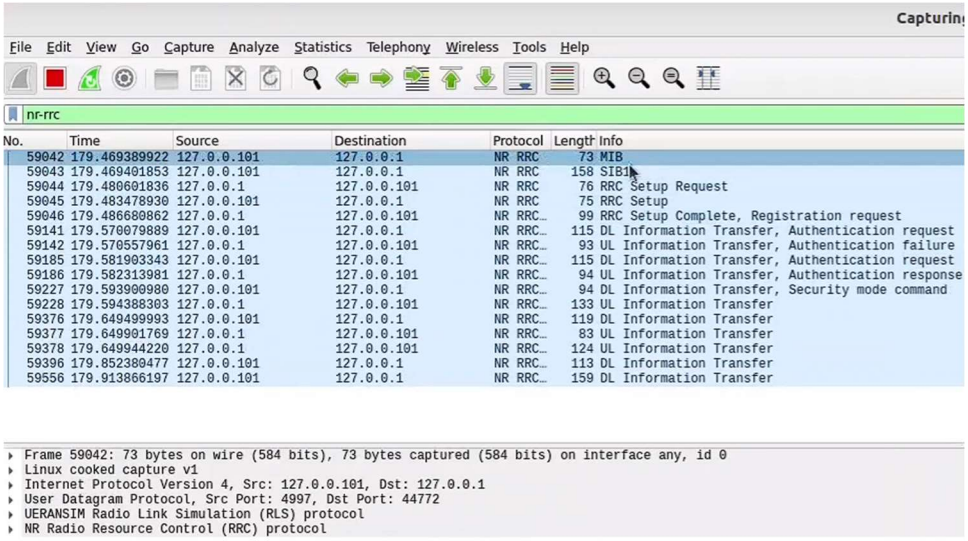
Interface gerada pelo localhost para realizar a conexão



3.1.4 Verificação do tráfego na rede

Por fim, utilizando uma ferramenta de análise de tráfego e aplicando um filtro de rede do tipo nr-rrc (New Radio-Radio Resource Control) podemos ver o usuário realizando a sequência de anexação inicial que foi descrita anteriormente. Para a realização deste teste, a ferramenta de análise de tráfego utilizada foi o Wireshark.

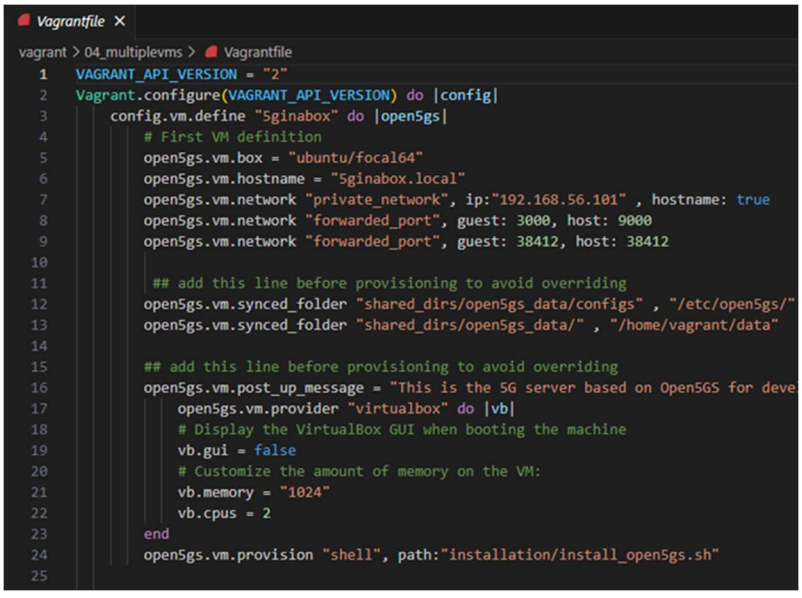
Captura dos dados de tráfego na anexação inicial do usuário



3.1.5 Instalação de ferramentas de gerenciamento de máquinas virtuais.

A instalação e configuração da máquina virtual e do simulador de redes necessita de aproximadamente uma hora para chegar ao estágio final, porém, esse tempo pode ser diminuído e este serviço pode ser otimizado, utilizando uma ferramenta de gerenciamento de máquinas virtuais. O programa usado foi o VagrantFile, e através deste, é possível criar e configurar diversas máquinas para serem instaladas simultaneamente com alocação de memória e processamento reduzidos, uma vez que a interface gráfica é removida, e o usuário pode interagir apenas via terminal. E uma opção de grande eficiência, pois possibilita que as NFs que compõe o core do 5G sejam criadas separadamente e ainda interajam entre si.

Arquivo VagrantFile para a criação de múltiplas máquinas virtuais



3.2 Estudo da arquitetura de segurança da rede 5G

Esta é a etapa em que a pesquisa se encontra atualmente, portanto, segue em desenvolvimento. Entretanto, nesta fase será possível verificar a segurança dos elementos que compõe o 5G, bem como verificar as características de segurança da rede nos serviços oferecidos, de forma a aprimorar a segurança da mesma.

Conclusão

Diante do que foi exposto, através deste projeto foi possível aprender sobre todos os elementos que compõem a arquitetura e o funcionamento da rede 5G e implementar um simulador de redes para efetuar testes. O estudo da arquitetura de segurança é o objeto de estudo principal a partir desse ponto e deve ser desenvolvido.

Referências Bibliográficas

SBRISSIA, Helena. **1G, 2G, 3G, 4G e 5G: entenda a evolução da internet móvel.** Tecmundo. Disponível em: <1G, 2G, 3G, 4G e 5G: entenda a evolução da internet móvel - TecMundo>. Acesso em 25 jan. 2023.

Apêndice I

Comandos para instalação do simulador de redes

Open5GS

```
sudo apt-get update
sudo apt-get install -y gnupg wget curl
```

Install MongoDB

wget -qO - https://www.mongodb.org/static/pgp/server-6.0.asc | sudo apt-key add –

echo "deb [arch=amd64,arm64] https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/6.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-6.0.list

sudo apt update

O MongoDb não possui uma compilação oficial para o Ubuntu 22.04 no momento.
Ubuntu 22.04 atualizou libssl para 3 e não propõe libssl1.1
Você pode forçar a instalação do libssl1.1 adicionando a fonte ubuntu 20.04:

echo "deb http://security.ubuntu.com/ubuntu focal-security main" | sudo tee /etc/apt/sources.list.d/focal-security.list

sudo apt-get update && sudo apt-get install libssl1.1

Em seguida, exclua o arquivo de lista de segurança focal que você acabou de criar:

```
sudo rm /etc/apt/sources.list.d/focal-security.list

sudo apt install -y mongodb-org mongodb-org-database

systemctl sudo start mongod

systemctl sudo enable mongod

systemctl sudo status mongod
```

Install NodeJs

```
curl -fsSL https://deb.nodesource.com/setup_18.x | sudo -E bash –
sudo apt install nodejs
```

Install Open5GS

```
sudo add-apt-repository ppa:open5gs/latest
sudo apt-get install -y software-properties-common
sudo apt-get -y update && sudo apt install -y open5gs
```

Verificar a instalação do Open5GS

```
sudo service open5gs-* status
```

Reiniciar a conexão de internet

sudo apt-get install net-tools

Instalar a interface web

```
curl -fsSL https://open5gs.org/open5gs/assets/webui/install | sudo -E bash –
```

UERANSIM

```
sudo apt install make gcc g++ libsctp-dev lksctp-tools iproute2 git

sudo snap install cmake --classic
```

mkdir ueransim && cd ueransim

```
git clone https://github.com/aligungr/UERANSIM

cd UERANSIM

make
```

Verificar informações do conteúdo instalado

```
cd config/

../build/nr-gnb -c open5gs-gnb.yaml    # Verificação de status inicial

sudo service open5gs-amfd status       # Verificar o funcionamento da AMFD

cd /etc/open5gs/

ls -lrt

more *yaml

grep -i “addr” *.yaml                  # listagem de ping das NFs
```