

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE ENGENHARIA ELÉTRICA E INFORMÁTICA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Daniel Ferreira Pires

DESENVOLVIMENTO DE BLOQUEADOR PARA USO EM PRÉDIOS URBANOS:

BLOQUEADOR POR AUTENTICAÇÃO

CAMPINA GRANDE

2025

DANIEL FERREIRA PIRES

DESENVOLVIMENTO DE BLOQUEADOR PARA USO EM PRÉDIOS URBANOS:
BLOQUEADOR POR AUTENTICAÇÃO

Trabalho de Conclusão de Curso apresentado à Coordenação de Engenharia Elétrica da Universidade Federal de Campina Grande, como parte dos requisitos necessários para a obtenção do título de Bacharel em Engenharia Elétrica.

Orientador: Prof. Dr. Bruno Barbosa Albert

CAMPINA GRANDE

2025

DANIEL FERREIRA PIRES

DESENVOLVIMENTO DE BLOQUEADOR PARA USO EM PRÉDIOS URBANOS:
BLOQUEADOR POR AUTENTICAÇÃO

Trabalho de Conclusão de Curso apresentado à Coordenação de Engenharia Elétrica da Universidade Federal de Campina Grande, como parte dos requisitos necessários para a obtenção do título de Bacharel em Engenharia Elétrica.

Aprovado em __ de ___ de ___.

Banca Examinadora:

_____

Prof Dr. Bruno Barbosa Albert (Orientador)
Universidade Federal de Campina Grande (UFCG)

_____

Professor Avaliador (Examinador)
Universidade Federal de Campina Grande (UFCG)

AGRADECIMENTOS

Agradeço a Deus por ter me dado forças para chegar até aqui. Agradeço aos meus pais, Rejane Pires e Eridan Pires, por terem sido exemplos de amor, força e determinação. Agradeço a minha namorada, Beatriz Farias, que ao longo desta jornada me deu todo apoio e incentivo, estando comigo nos melhores e piores dias.

Aos amigos que o curso me deu: Natã Macedo, Aylla Echily , Jhonatan Souza e Virginia Sousa. Obrigado pelas ajudas nas disciplinas, conversas e risadas. e os ensinamentos que vão além dos muros da universidade.

“Dedico este trabalho aos meus pais, por todo amor, apoio e ensinamentos que me proporcionaram ao longo da vida.”

"A tecnologia é apenas uma ferramenta. No fim, as pessoas são quem fazem a diferença."

— Bill Gates

RESUMO

Este trabalho, desenvolvido no curso de Engenharia Elétrica com ênfase em Telecomunicações, apresenta a implementação de um mecanismo de controle de acesso em redes móveis 5G baseado na verificação da identidade de equipamentos por meio do IMEI (International Mobile Equipment Identity). A proposta consiste na integração de um Equipment Identity Register (EIR) ao núcleo de rede 5G utilizando a plataforma Open5GS, permitindo a validação de dispositivos durante o processo de registro na rede.

Como alternativa ao uso de bloqueadores de sinal (jammers), que atuam de forma indiscriminada e são proibidos por regulamentação, a solução proposta realiza o bloqueio de forma seletiva diretamente no núcleo da rede, impedindo apenas dispositivos não autorizados sem afetar usuários legítimos.

Para isso, foi desenvolvido um servidor EIR em linguagem C, com interface HTTP e integração com banco de dados MongoDB, responsável por armazenar os dispositivos autorizados e bloqueados. Além disso, o componente AMF *(Access and Mobility Management Function)* do Open5GS foi modificado para realizar a verificação do IMEI durante o procedimento de registro.

Os resultados demonstram que a solução é capaz de permitir o acesso de dispositivos autorizados e bloquear aqueles não cadastrados, contribuindo para o aumento da segurança e do controle de acesso em redes móveis.

Palavras-chave: 5G, Open5GS, EIR, IMEI, Segurança em Telecomunicações.

ABSTRACT

This work, developed in the Electrical Engineering program with emphasis on Telecommunications, presents the implementation of an access control mechanism for 5G mobile networks based on equipment identity verification using the IMEI (International Mobile Equipment Identity). The proposed solution integrates an Equipment Identity Register (EIR) into a 5G core network using the Open5GS platform, enabling device validation during the network registration process.

As an alternative to signal jammers, which operate indiscriminately and are restricted by regulations, the proposed approach performs selective blocking directly within the core network, preventing only unauthorized devices from accessing the network without affecting legitimate users.

To achieve this, an EIR server was developed in the C programming language, with an HTTP interface and integration with a MongoDB database to store authorized and blocked devices. In addition, the AMF *(Access and Mobility Management Function)* component of Open5GS was modified to perform IMEI verification during the registration procedure.

The results show that the solution is able to allow access for authorized devices and block unauthorized ones, contributing to improved security and access control in mobile networks.

Keywords: 5G, Open5GS, EIR, IMEI, Telecommunications Security.

LISTA DE TABELAS

Tabela 1: Tipos de small cells e suas aplicações.....10
Tabela 2: Tipos de small cells e suas aplicações.....11
Tabela 3: Simuladores de redes 5g.....15

LISTA DE FIGURAS

Figura 1: Demonstração ICCID chip..... 4
Figura 2:Demonstração ICCID Configurações.....5
Figura 3: Demonstração IMEI..... 6
Figura 4: Core Virtualizado.....16
Figura 5: Diagrama de Comunicação 5G.....19
Figura 6: Diagrama de Comunicação 5G novo.....20
Figura 7: Interface Open5GS..... 24
Figura 8: Whitelist..... 26
Figura 9: Resposta Dispositivo autorizado.....26
Figura 10: Resposta Dispositivo negado..... 27

LISTA DE ABREVIATURAS E SIGLA

1G – Primeira geração de telefonia móvel
2G – Segunda geração de telefonia móvel
3G – Terceira geração de telefonia móvel
4G – Quarta geração de telefonia móvel
5G – Quinta geração de telefonia móvel
AMF – *Access and Mobility Management Function* (Função de Gerenciamento de Acesso e Mobilidade)
CN – *Core Network* (Rede Central)
EIR – *Equipment Identity Register* (Registro de Identidade de Equipamentos)
ERB – Estação Rádio Base
ICCID – *Integrated Circuit Card Identifier* (Identificador do Cartão SIM)
IMSI – *International Mobile Subscriber Identity* (Identidade Internacional do Assinante Móvel)
JSON – *JavaScript Object Notation* (Notação de Objetos JavaScript)
PEI – *Permanent Equipment Identifier* (Identificador Permanente do Equipamento)
RAN – *Radio Access Network* (Rede de Acesso por Rádio)
SIM – *Subscriber Identity Module* (Módulo de Identidade do Assinante)
SNR – *Serial Number* (Número de Série do Equipamento)
SUCI – *Subscription Concealed Identifier* (Identificador Oculto do Assinante)
TMSI – *Temporary Mobile Subscriber Identity* (Identidade Temporária do Assinante Móvel)
UE – *User Equipment* (Equipamento do Usuário)
USIM – *Universal Subscriber Identity Module* (Módulo Universal de Identidade do Assinante)

SUMÁRIO

1 INTRODUÇÃO.....1
1.1 Objetivos.....2
1.1.1 Objetivo geral.....2
1.1.2 Objetivos específicos.....2
2 FUNDAMENTAÇÃO TEÓRICA.....3
2.1 Sistema de identificação.....3
2.2 Jammers.....6
2.3 Rede 5G.....8
2.3.1 Small cells.....9
3 METODOLOGIA.....10
3.1 Criação do núcleo.....10
3.2 Modificação do sistema de autenticação.....14
3.3 Comparação entre bloqueadores.....16
4 RESULTADOS E DISCUSSÕES.....16
5 CONCLUSÃO.....16
REFERÊNCIAS.....17
7 Anexo.....18

1 INTRODUÇÃO

O uso não autorizado de celulares por detentos é um dos principais desafios para a segurança pública, visto que desencadeia uma série de problemas relacionados à segurança dos civis e dificulta o cumprimento dos objetivos do sistema prisional brasileiro, quais sejam o cumprimento das decisões judiciais e a reintegração desses indivíduos à sociedade brasileira.

Houve iniciativas governamentais que buscaram suprimir o uso de aparelhos telefônicos dentro das penitenciárias com a implementação de bloqueadores em diferentes períodos (Campos, 2025). A mais recente delas teve a aprovação da câmara dos deputados, com o Projeto de Lei (PL) 4389/2024, que torna obrigatório o uso de bloqueadores de sinais de celular em todos os presídios e estabelecimentos prisionais do País (Miranda, 2025).

O acesso a aparelhos celulares, assim, torna possível o cometimento de crimes dentro dos presídios, que vão desde golpes, como o falso sequestro, o *vishing* ou o roubo de dados financeiros, até operações de facções controladas por chefes já encarcerados.Considerando que as medidas atuais de fiscalização se mostram ineficazes quanto ao combate desse problema, faz-se necessária a proposição de uma nova abordagem para sua resolução. Uma dessas formas, que já foi levantada e está sendo implementada em alguns presídios brasileiros, é o uso de bloqueadores de sinais convencionais, mesmo que pesquisas demonstrem que seu uso isolado é ineficaz (Pagnan, 2018).

Os bloqueadores usados atualmente se baseiam na negação de uma faixa de frequência ao colocar um sinal de interferência na faixa de frequência do sinal a ser bloqueado. Assim, nenhum usuário consegue utilizar o serviço no raio de interferência, e se o sinal do bloqueador não tiver potência suficiente apenas diminuirá a velocidade da conexão em vez de interromper.

A rede 5G tem como diferencial sua abordagem baseada em serviços, na qual as funções de rede são desacopladas e organizadas como serviços modulares, o que permite a rápida adesão à novos serviços. A Arquitetura Baseada em

Serviços(SBA) facilita o fatiamento de rede, por meio do qual múltiplas redes virtuais são criadas para atender a requisitos de serviço específicos.

A arquitetura da atual geração de comunicações móveis (5G) tem como composição um Equipamento de Usuário (UE), que se comunica com a Rede de Acesso via Rádio (RAN) e passa a informação para Rede Central (CN), responsável por gerenciar diversas funções de rede. Entre essas funções está a Função de Gestão de Acesso e Mobilidade (AMF), que trabalha no acesso e na autenticação do UE e de sua mobilidade para as antenas próximas (ERB's).

Tendo em vista a dificuldade e o custo operacional dos bloqueadores, almejamos utilizar as funcionalidades da própria rede 5G para impossibilitar o acesso de usuários não autorizados, desabilitando-as com o auxílio da AMF.

1.1 Objetivos

1.1.1 Objetivo geral

Desenvolver um sistema de bloqueio de sinal por identificadores e de zonas delimitadas, usando a aplicação da versatilidade das redes 5G.

1.1.2 Objetivos específicos

Avaliar a viabilidade técnica da solução proposta frente aos métodos convencionais.

Estudar a arquitetura 5G e suas funcionalidades de autenticação (AMF) aplicáveis ao controle de acesso.

1.2 Estrutura do trabalho

O presente trabalho está organizado em capítulos que abordam de forma progressiva os conceitos teóricos, a metodologia adotada, a implementação da solução proposta e a análise dos resultados obtidos.

O Capítulo 2 trata da fundamentação teórica, abordando os conceitos essenciais relacionados às redes móveis, incluindo a evolução das gerações de comunicação (1G a 5G), a arquitetura das redes 5G, os elementos do núcleo de rede, além dos conceitos de identificação de dispositivos e assinantes, com destaque para o IMEI, IMSI e o funcionamento do *Equipment Identity Register* (EIR). Também são discutidos aspectos relacionados à simulação e emulação de redes móveis.

O Capítulo 3 apresenta a metodologia adotada no desenvolvimento do trabalho, descrevendo o ambiente experimental utilizado, incluindo a virtualização do sistema, a implementação do núcleo 5G com Open5GS, a utilização do UERANSIM para emulação de dispositivos e a implementação do servidor EIR. Neste capítulo também são detalhadas as modificações realizadas no fluxo de autenticação, bem como o funcionamento do sistema antes e após a integração do EIR.

O Capítulo 4 apresenta os resultados obtidos a partir dos experimentos realizados, incluindo a validação do ambiente, a análise do comportamento da rede com e sem a implementação do EIR, e a comparação com métodos tradicionais de bloqueio, como o uso de bloqueadores de sinal (*jammers*). Além disso, são discutidos os impactos da solução proposta e suas implicações práticas.

O Capítulo 5 apresenta as conclusões do trabalho, destacando as principais contribuições, limitações e possibilidades de trabalhos futuros, incluindo análises mais aprofundadas em cenários reais e estudos de viabilidade econômica.

Por fim, são apresentados os anexos, contendo trechos relevantes dos códigos desenvolvidos e utilizados na implementação da solução proposta.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Sistema de identificação

No decorrer das gerações da rede móvel, a forma de identificação do usuário foi sendo alterada. Na 1G, de natureza totalmente analógica, essa identificação ocorria por meio do número de telefone associado ao terminal. Não havia autenticação criptográfica, o que tornava possível a clonagem de aparelhos e fraudes frequentes.

Com a 2G (GSM/IS-54) surgiu o conceito de *SIM Card* (*Subscriber Identity Module*), no qual passou a ser armazenado o IMSI (*International Mobile Subscriber Identity*) e o ICCID (Integrated Circuit Card Identifier), um identificador numérico único que permite à rede autenticar o assinante. A fim de reduzir riscos de exposição, foram criados identificadores temporários, como o TMSI (*Temporary Mobile Subscriber Identity*).

Já na 3G (UMTS/WCDMA), a autenticação foi reforçada com a introdução do USIM (*Universal Subscriber Identity Module*) e protocolos mais sofisticados, como o AKA (*Authentication and Key Agreement*), que usam o IMSI apenas no início da comunicação, substituindo-o por identificadores temporários durante a sessão.

Na 4G (LTE), manteve-se o princípio do IMSI armazenado no cartão USIM, mas com autenticação baseada em EPS-AKA, além de reforço na privacidade para reduzir a vulnerabilidade a ataques de interceptação de identidade.

Por fim, na 5G, a identificação do usuário continua a se basear no IMSI (rebatizado como SUPI – *Subscription Permanent Identifier*), mas a rede introduziu um novo identificador, o SUCI (*Subscription Concealed Identifier*), que utiliza criptografia assimétrica para proteger o IMSI durante a transmissão aérea, impedindo sua exposição a ataques de rastreamento e fortalecendo a privacidade do assinante.

Os Aparelhos telefônicos atuais carregam esse 4 identificadores principais:

- **IMSI:** É um número de identificação único do assinante móvel. A maioria dos SIM cards armazena apenas um IMSI, que está associado a uma lista de redes às quais o assinante está autorizado a acessar. Existem chips no mercado que apresentam a função de múltiplos IMSI, os chamados de MULTI-IMSI, que permitem que o SIM altere suas identidades para acessar mais redes e selecionar aquela com a melhor cobertura.
- **MSISDN:** Significa Número Internacional do Diretório de Assinantes Móveis. É um número único que identifica exclusivamente uma assinatura ou plano em uma operadora de celular em todo o mundo. Comumente nos referimos como “o número da linha telefônica”.
- **IMEI:** O Identificador Internacional de Equipamento Móvel, ou IMEI, é um único número de série de 15 dígitos que pode ser usado para identificar cada equipamento ou dispositivo de forma exclusiva.
- **ICCID:** É o Número de Identificação do Cartão de Circuito Integrado. Trata-se de um código exclusivo de cada chip, que inclui o país, a rede doméstica e o número de identificação.

Para se identificar o ICCID, do chip temos 2 métodos: o primeiro consiste em localizar o código no próprio chip, contendo de 18 a 22 dígitos sempre iniciando com 89, que o identifica como um produto para redes de telecomunicação. de acordo com a imagem 1:

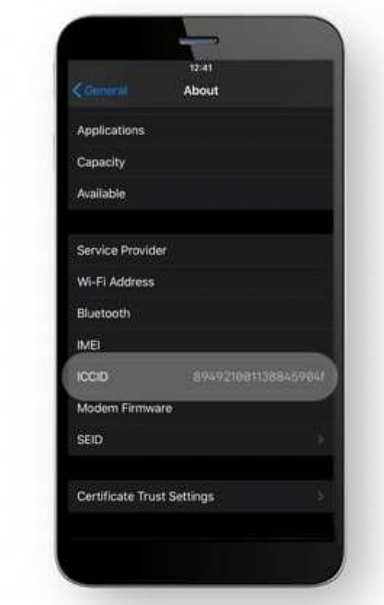
Figura 1: Demonstração ICCID chip



fonte:https://penosapo.wordpress.com/wp-content/uploads/2012/03/iccid-number-printed-on-sim-card.jpg

O segundo método para identificar o ICCID necessita que a leitura seja feita através da interface de um smartphone, de modo a ser encontrado no menu de configurações, como mostrado na seguinte imagem:

Figura 2:Demonstração ICCID Configurações



fonte:https://www.emnify.com/pt-br/blog/iccid

Já descobrir o SUPI/IMSI é uma tarefa um pouco mais complexa, visto que ele é o identificador permanente do assinante. Redes reais utilizam-no apenas dentro de procedimentos seguros de autenticação; redes e dispositivos protegem esses valores. Sendo o meio mais confiável, a solicitação é realizada direto com a operadora do Cartão SIM.

Por fim, para identificar o IMEI, temos 3 formas de consulta confiáveis. A Primeira e mais fácil consiste em digitar o código “*#06#” no aplicativo telefone (discar). Na tela, aparecerá o IMEI junto do código de barras. Caso seu aparelho tenha a capacidade de comportar mais de um chip, então constará a mesma quantidade de IMEI’s que o aparelho suporta. como mostrado na figura 3:

Figura 3: Demonstração IMEI



fonte:Autoria própria(2025)

A segunda forma de encontrar o IMEI é semelhante à do ICCID, porque consiste em acessar as configurações do aparelho. Como mostrado na figura 3, o IMEI fica logo acima do ICCID.

A terceira forma é encontrar o IMEI escrito. Essa consulta pode ser efetuada tanto no aparelho quanto na caixa original do produto, mas a localização varia de acordo com o aparelho.

2.2 Jammers

Os jammers, também conhecidos como bloqueadores de sinal, são dispositivos destinados a interferir intencionalmente em comunicações radioelétricas, degradando ou impedindo a recepção de sinais legítimos em uma determinada faixa de frequência.

Tecnicamente, a ação de um jammer pode ser entendida como a elevação do ruído efetivo ou a injeção de sinais espúrios na banda alvo, reduzindo a relação sinal-a-ruído (SNR) ou a relação sinal-a-interferência (SIR) no receptor. Quando a SNR/SIR cai abaixo do limiar necessário para demodulação e decodificação, o receptor torna-se incapaz de recuperar a informação transmitida, resultando em perda de conectividade, falha em protocolos de controle e degradação de qualidade de serviço. Essa interferência pode ser relacionada pela equação de sinal ruído (SNR) que afeta a capacidade do canal, sendo vista pelo teorema Shannon–Hartley:

$$C = B^* \log_2(1 + SNR)$$

ou

$$C = B * \log_2(S + N)$$

em que:

- C representa a capacidade do canal (em bits por segundo),
- B é a largura de banda do canal (em hertz),
- S é a potência média do sinal (em watts),
- N é a potência média do ruído (em watts).
- SNR é a relação entre a potência do sinal e o ruído.

Os jammers são tipicamente classificados segundo o modo de operação e o comportamento espectral:

- ***Barrage jammer*****:** Ocupa uma larga faixa de frequência com ruído, afetando múltiplos canais simultaneamente;
- ***Spot jammer*****:** Concentra potência em uma frequência estreita, visando um canal ou sinal específico;
- ***Sweep jammer*****:** Varre periodicamente um conjunto de frequências, causando interferência temporalmente distribuída;
- ***Deceptive jammer*****:** Injeta sinais que mimetizam mensagens legítimas ou comandos de controle, provocando respostas errôneas nos receptores;
- ***Smart/Adaptive jammer*****:** Monitora o espectro e ajusta dinamicamente potência, frequência e padrão de emissão para maximizar a eficácia com menor consumo de energia.

Uma vez que o ponto principal desse trabalho é o uso de bloqueadores para

presídios próximos a centros urbanos, o uso de *jammers* em presídios próximos a centros povoados apresenta uma série de problemas que tornam essa prática extremamente delicada. Do ponto de vista da segurança pública, o bloqueio de sinais de telefonia celular não se limita apenas ao interior do presídio, já que a propagação das ondas eletromagnéticas é difícil de controlar. Assim, moradores, trabalhadores e transeuntes nas imediações podem ser afetados, perdendo acesso a serviços essenciais de comunicação, o que inclui chamadas de emergência para polícia, bombeiros e atendimento médico.

Esse tipo de interferência também pode comprometer sistemas de infraestrutura crítica, como sensores urbanos, terminais de pagamento, alarmes e até sistemas de navegação e temporização que dependem de sinais de rádio. Além disso, juridicamente, a utilização de jammers é proibida em muitos países, uma vez que interferir intencionalmente em espectro licenciado é ilegal. Isso significa que, além do risco operacional, a administração penitenciária pode estar sujeita a penalidades legais, multas e responsabilização civil por danos causados à população vizinha.

2.3 Rede 5G

A quinta geração (5G) representa uma mudança de paradigma na comunicação móvel, oferecendo altas velocidades, baixa latência e grande densidade de dispositivos conectados. As principais características do 5G incluem:

- **Altas taxas de transmissão:** até 10 Gbps para usuários estacionários e 1 Gbps para usuários móveis.
- **Baixa latência:** menor que 1 ms, permitindo aplicações críticas em tempo real, como veículos autônomos e cirurgias remotas.
- **Conectividade massiva:** suporte a até 1 milhão de dispositivos por km², essencial para Internet das Coisas (IoT).
- **Eficiência energética:** otimização de consumo em dispositivos e infraestrutura, reduzindo custos operacionais.

A arquitetura do 5G é baseada em uma rede segmentada em plano de controle e plano de usuário, composta por elementos funcionais, como:

- **AMF (Access and Mobility Management Function):** gerencia a mobilidade e registro de usuários.
- **SMF (Session Management Function):** controla sessões de dados e roteamento.
- **UPF (User Plane Function):** encaminha os dados do usuário.
- **UDM/HSS (Unified Data Management / Home Subscriber Server):** gerencia os perfis e a autenticação de assinantes.
- **AUSF (Authentication Server Function):** realiza a autenticação e a segurança dos usuários.

Essa arquitetura modular permite maior flexibilidade, integração com diferentes tecnologias de acesso (RAN, small cells, mmWave) e implementação de políticas de segurança avançadas. O 5G habilita novos serviços e modelos de negócios, incluindo:

- **IoT e Smart Cities:** sensores conectados para monitoramento ambiental, trânsito e segurança.
- **Indústria 4.0:** automação e controle em tempo real de máquinas e robôs.
- **Saúde:** telemedicina e procedimentos remotos com baixa latência.
- **Entretenimento e mídia:** streaming em alta resolução, realidade aumentada e virtual.

Embora amplamente utilizado em redes legadas, o uso do IMEI como mecanismo ativo de controle de acesso ainda não é amplamente integrado ao núcleo 5G em plataformas abertas.

2.3.1 Small cells

Com a maturidade das redes móveis e o crescimento exponencial da demanda por tráfego de dados, tornou-se necessário adotar soluções que permitissem ampliar a cobertura e, ao mesmo tempo, garantir a qualidade dos serviços oferecidos. Nesse contexto, a utilização de small cells surge como uma alternativa eficiente, uma vez que possibilita a oferta de recursos localizados, o preenchimento de zonas de sombra na cobertura e o uso mais eficaz do espectro, aumentando a capacidade global da rede.

As *small cells* podem ser definidas como estações rádio base de baixa potência, que operam em espectro licenciado, são gerenciadas por operadoras e oferecem melhorias significativas em termos de cobertura e capacidade. Elas podem ser implantadas em diferentes cenários, desde ambientes residenciais e corporativos até áreas públicas metropolitanas e rurais, representando uma solução versátil e de baixo custo.

Essas células variam em alcance e potência, indo das femtocélulas (menores, voltadas para residências e pequenos escritórios) até as metrocélulas (maiores, projetadas para prover capacidade em centros urbanos). Além disso, tecnologias como WiFi e WLANs baseadas no padrão IEEE 802.11 podem ser consideradas em um conceito mais amplo de *small cells*, especialmente quando integradas a redes móveis para complementação de cobertura.

A tabela abaixo mostra a diferença entre cada uma e suas aplicações:

Tabela 1: Tipos de small cells e suas aplicações

Tipo	**Implantação típica**	**Nº de usuários suportados**	**Faixa de potência típica**	**Alcance aproximado**
Femtocell	Residências e ambientes empresariais	Residencial: 4–8 Empresarial: 16–32	10–100 mW 0,2–1 W	Dezenas de metros
Picocell	Áreas públicas internas/externas (aeroportos, shoppings, estações)	64–128 usuários	100–250 mW 1–5 W	Dezenas de metros
Microcell	Áreas urbanas para preencher lacunas de cobertura macro	128–256 usuários	5–10 W	Algumas centenas de metros
Metrocells	Áreas urbanas para prover capacidade adicional	>250 usuários	10–20 W	Centenas de metros
WiFi (IEEE 802.11)	Residências, escritórios e ambientes empresariais	<50 usuários	20–100 mW 0,2–1 W	Algumas dezenas de metros

Fonte: Adaptado de *Fundamentals of 5G Mobile Networks* (2015).

2.3.1 EIR — Registro de identidade de equipamentos

O *Equipment Identity Register* (EIR), ou Registro de Identidade de Equipamentos, é um elemento funcional das redes móveis responsável por armazenar e gerenciar informações relacionadas à identificação dos dispositivos utilizados pelos usuários. Sua principal função é verificar a legitimidade de equipamentos a partir do identificador único denominado *International Mobile Equipment Identity* (IMEI), contribuindo diretamente para a segurança da rede e prevenção de fraudes.

O EIR opera por meio da classificação dos dispositivos em diferentes listas, tradicionalmente denominadas lista branca (*white list*), lista cinza (*grey list*) e lista negra (*black list*). Equipamentos presentes na lista branca são considerados autorizados para acesso pleno à rede, enquanto dispositivos na lista cinza são monitorados por apresentarem comportamento suspeito. Já os equipamentos incluídos na lista negra são bloqueados, sendo impedidos de utilizar os serviços da rede móvel. Essa abordagem permite um controle granular e dinâmico sobre os dispositivos conectados.

Tabela 2: Tipos de small cells e suas aplicações

Estado\Lista	Significado Operacional	Ação típica do AMF
WHITELISTED	Equipamento Permitido	Prosseguir com a sessão
BLACKLISTED	Equipamento Proibido	Rejeitar acesso

Fonte: Adaptado de 3GPP a global iniciative (2026)

Nas arquiteturas de redes móveis de quinta geração (5G), embora o EIR não seja definido como uma função central obrigatória no núcleo 5G (*5G Core*), suas funcionalidades podem ser implementadas de forma integrada ou externa ao núcleo, interagindo com elementos como o *Access and Mobility Management Function* (AMF). Durante o processo de registro do equipamento na rede, o AMF pode solicitar a identidade do dispositivo e realizar verificações junto a um sistema equivalente ao EIR, permitindo a tomada de decisão quanto à aceitação ou rejeição do acesso.

No contexto deste trabalho, o EIR é implementado como um serviço externo integrado ao núcleo 5G baseado na plataforma Open5GS, sendo responsável por validar o IMEI dos dispositivos durante o processo de autenticação. Essa integração permite simular cenários de bloqueio seletivo de equipamentos, evidenciando a viabilidade da abordagem e sua aplicabilidade em ambientes controlados de pesquisa e desenvolvimento.

2.3.1 EIR — Registro de identidade de equipamentos

A simulação e a emulação de redes móveis são abordagens fundamentais para o desenvolvimento, teste e validação de novas tecnologias em telecomunicações, especialmente em cenários relacionados às redes de quinta geração (5G). Essas técnicas permitem a análise do comportamento da rede em condições controladas, reduzindo custos e complexidade associados à implementação em ambientes reais.

A simulação consiste na modelagem abstrata de sistemas de comunicação por meio de ferramentas computacionais que reproduzem o comportamento da rede com base em modelos matemáticos e estatísticos. Nesse contexto, elementos como latência, perda de pacotes e mobilidade podem ser avaliados sem a necessidade de infraestrutura física. No entanto, a simulação apresenta limitações quanto ao nível de realismo, uma vez que não envolve a execução de protocolos reais em pilhas completas de comunicação.

Por outro lado, a emulação proporciona um ambiente mais próximo da realidade, permitindo a execução de softwares e protocolos reais em uma infraestrutura controlada. Na emulação de redes móveis, componentes do núcleo da rede, estações rádio base e dispositivos de usuário são implementados por meio de softwares especializados, possibilitando a interação real entre os elementos da rede. Essa abordagem é amplamente utilizada em pesquisas relacionadas ao 5G, pois permite validar funcionalidades e testar integrações de forma prática.

Dentre as ferramentas utilizadas para emulação de redes móveis, destacam-se o Open5GS, que implementa o núcleo da rede 4G/5G, e o UERANSIM, responsável por emular dispositivos de usuário (*User Equipment* – UE)

e estações rádio base (*gNodeB* – gNB). A combinação dessas ferramentas possibilita a criação de um ambiente completo de rede móvel, no qual é possível realizar testes de autenticação, mobilidade, controle de acesso e políticas de segurança.

No presente trabalho, a emulação é empregada como principal metodologia experimental, permitindo a integração do EIR ao núcleo 5G e a avaliação do comportamento da rede diante de diferentes cenários de bloqueio de dispositivos. Essa abordagem possibilita a análise prática dos impactos da utilização do EIR, bem como a comparação com métodos alternativos, como os bloqueadores de sinal. Assim, a emulação se mostra uma ferramenta essencial para a validação das propostas apresentadas, garantindo maior confiabilidade aos resultados obtidos.

3 METODOLOGIA

Este trabalho adota uma abordagem experimental baseada na emulação de redes móveis de quinta geração (5G), com o objetivo de avaliar a viabilidade da integração de um sistema de verificação de identidade de equipamentos (Equipment Identity Register – EIR) ao núcleo da rede. A metodologia consiste na implementação de um ambiente controlado que permite a reprodução de cenários reais de autenticação e controle de acesso de dispositivos.

A escolha pela emulação se justifica pela possibilidade de utilizar implementações reais dos protocolos de rede, garantindo maior fidelidade em relação ao comportamento observado em ambientes operacionais. Dessa forma, é possível validar a proposta de bloqueio seletivo de dispositivos com base no identificador IMEI, bem como comparar essa abordagem com métodos tradicionais, como o uso de bloqueadores de sinal.

3.1 Ambiente Experimental

O ambiente experimental desenvolvido neste trabalho foi concebido com o objetivo de permitir a emulação de uma rede móvel de quinta geração (5G) de forma

controlada, possibilitando a implementação e validação de mecanismos de controle de acesso baseados na identidade dos dispositivos. Para isso, optou-se pela utilização de um ambiente virtualizado, permitindo maior flexibilidade, reprodutibilidade dos experimentos e isolamento dos componentes envolvidos.

A virtualização do ambiente foi adotada como estratégia para reduzir a dependência de infraestrutura física dedicada, além de facilitar a configuração, modificação e restauração do sistema durante os testes. Essa abordagem permite a execução simultânea de múltiplos serviços em um único host físico, mantendo a separação lógica entre os elementos da rede.

Como sistema operacional, foi utilizada a distribuição Linux Ubuntu 22.04 LTS. A escolha dessa versão se deve à sua estabilidade, amplo suporte da comunidade e compatibilidade com as ferramentas empregadas neste trabalho, como o Open5GS e o UERANSIM. Além disso, o Ubuntu 22.04 apresenta suporte a longo prazo (*Long Term Support* – LTS), garantindo atualizações de segurança e manutenção contínua, o que o torna adequado para aplicações acadêmicas e de pesquisa.

O ambiente experimental foi estruturado de forma a integrar três componentes principais: o núcleo da rede 5G, responsável pelo controle e gerenciamento das conexões; o sistema de emulação de dispositivos de usuário; e o servidor EIR, responsável pela verificação da identidade dos equipamentos. A comunicação entre esses elementos ocorre por meio de interfaces padronizadas, reproduzindo o funcionamento de uma rede móvel real em escala reduzida.

3.1.1 Criação do núcleo

Neste trabalho, o núcleo da rede 5G foi implementado utilizando o Open5GS, uma solução *open-source* que oferece suporte completo aos principais elementos funcionais definidos pela 3GPP, tais como AMF (Access and Mobility Management Function), SMF (Session Management Function), UPF (User Plane Function) e UDM/HSS para gerenciamento de assinantes.

Em comparação com outros núcleos *open-source*, como o free5GC e o OAI Core, o Open5GS apresenta vantagens em termos de facilidade de instalação, configuração e manutenção, sendo considerado mais acessível para ambientes de laboratório e prototipagem rápida.

O free5GC é totalmente compatível com 3GPP, mas exige configuração complexa e experiência em conteinerização, enquanto o OAI Core é altamente flexível para pesquisa acadêmica, porém possui documentação menos acessível e menor compatibilidade com dispositivos comerciais.

Tabela 3: Simuladores de redes 5g.

Núcleo	**Principais Características**	**Vantagens**	**Desvantagens / Limitações**
Open5GS	Core completo 5G; suporte AMF, SMF, UPF, UDM/HSS; fácil integração com RAN	- Instalação/configuração simples - Boa documentação e comunidade ativa - Ideal para laboratórios	- Menos flexível que OAI para pesquisa avançada
free5GC	Core 5G compatível 3GPP; arquitetura modular; conteinerização	- Compatível 3GPP - Escalável, cloud-native	- Configuração complexa - Curva de aprendizado maior
OAI Core	Plataforma acadêmica 5G/LTE; integração com OAI RAN	- Flexível para pesquisa - Permite modificações detalhadas	- Documentação limitada - Compatibilidade reduzida com dispositivos comerciais

Fonte: Autoria Própria (2025).

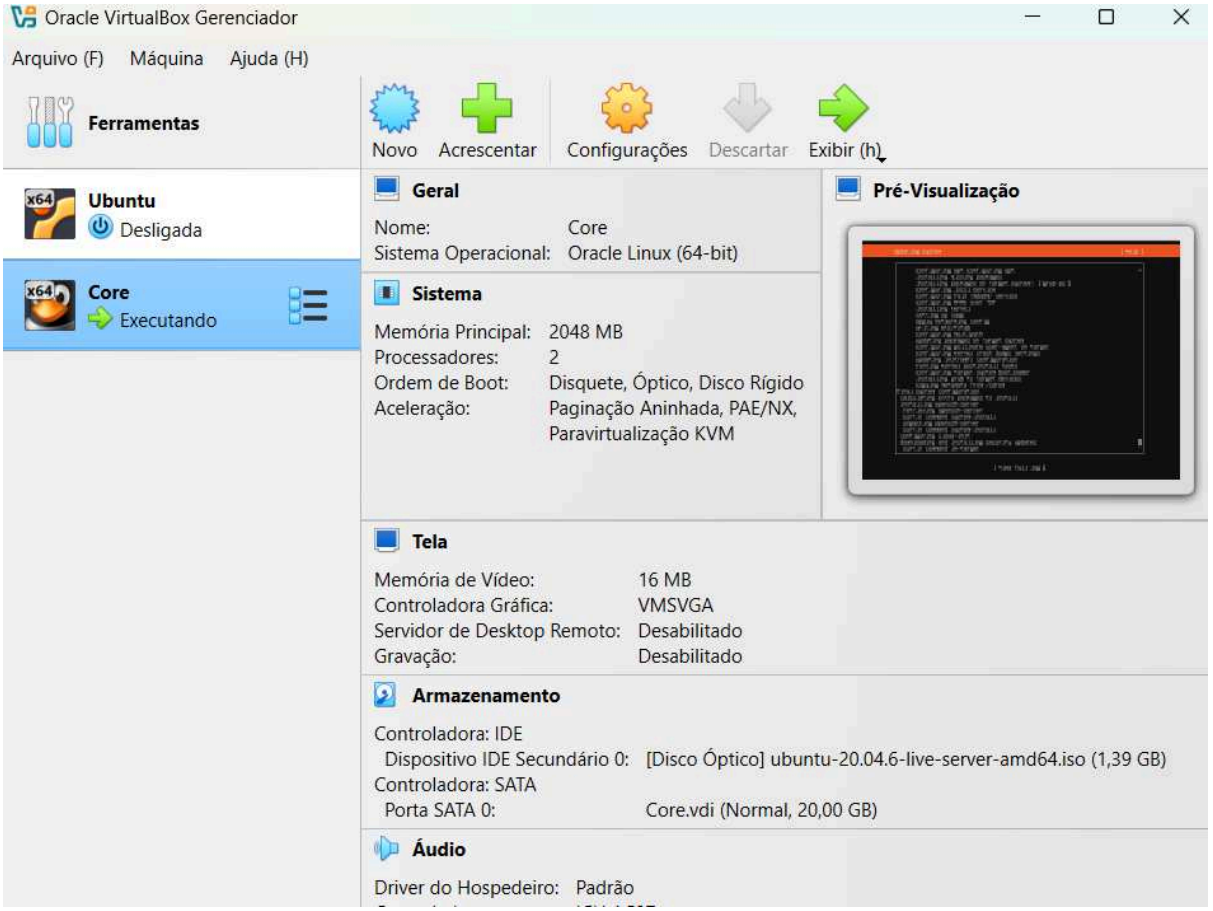
Escolhido o simulador de núcleo, o próximo passo é a criação da máquina virtual. A virtualização de recursos computacionais tornou-se uma prática essencial na pesquisa e desenvolvimento de redes móveis de quinta geração (5G). Por meio da criação de máquinas virtuais (VMs), é possível emular ambientes de rede complexos com baixo custo, flexibilidade de configuração e facilidade de reprodutibilidade dos experimentos. Nesse contexto, a implementação do núcleo 5G utilizando o Open5GS, um projeto de código aberto voltado para simulação e testes de redes móveis, representa uma solução prática e eficiente.

Para a criação do ambiente virtualizado foram definidos requisitos mínimos, de modo a garantir a execução estável do Open5GS e a simulação dos principais componentes da rede 5G. Os requisitos considerados são:

- **Hardware**: processador de múltiplos núcleos (≥ 2 vCPUs), memória RAM ≥ 8 GB e espaço em disco ≥ 50 GB;
- **Software**: sistema operacional host baseado em Linux ou Windows, hipervisor Oracle VM VirtualBox e imagem ISO do Ubuntu Server 20.04 LTS para o ambiente convidado.

A escolha pelo VirtualBox se justifica por ser uma ferramenta gratuita, de fácil configuração e amplamente utilizada em ambientes acadêmicos, garantindo compatibilidade com diferentes sistemas operacionais hospedeiros.

Figura 4: Core Virtualizado



fonte: Autoria propria(2025)

3.1.2 Emulação do Equipamento do Usuário

Para a emulação do equipamento do usuário (*User Equipment* – UE) e da

estação rádio base (*gNodeB* – gNB), foi utilizada a ferramenta UERANSIM. Essa solução permite simular o comportamento de dispositivos reais em uma rede 5G, implementando os protocolos necessários para o processo de registro, autenticação e estabelecimento de sessões de dados.

A escolha do UERANSIM se deve à sua compatibilidade com o Open5GS, bem como à sua facilidade de configuração e utilização em ambientes de teste. A ferramenta permite a definição de parâmetros essenciais do dispositivo, como o identificador do assinante (IMSI), a chave de autenticação e o identificador do equipamento (IMEI), sendo este último fundamental para os objetivos deste trabalho.

Durante os experimentos, o UERANSIM foi configurado para iniciar o processo de registro na rede, enviando mensagens ao núcleo 5G conforme especificado pelo padrão 3GPP. A troca de mensagens entre o UE e o AMF possibilita a obtenção do IMEI do dispositivo, que é posteriormente utilizado no processo de verificação junto ao sistema EIR.

Essa abordagem permite simular diferentes dispositivos e cenários de acesso à rede, possibilitando a análise do comportamento do sistema diante de equipamentos autorizados e bloqueados.

3.1.3 Implementação do Servidor EIR

O sistema EIR foi desenvolvido como um serviço externo ao núcleo da rede, com a função de verificar a legitimidade dos dispositivos a partir do seu identificador IMEI. A implementação foi realizada de forma a permitir a comunicação com o AMF por meio de requisições HTTP, proporcionando uma arquitetura modular e de fácil integração.

O servidor EIR foi configurado para operar na porta 5000, disponibilizando um endpoint responsável pela validação dos dispositivos. Ao receber uma requisição contendo o IMEI, o servidor realiza a verificação com base em uma lista de dispositivos previamente definida, classificando-os como autorizados ou

bloqueados.

A integração entre o Open5GS e o EIR foi implementada por meio da utilização da biblioteca libcurl, permitindo que o AMF envie requisições HTTP durante o processamento do registro do dispositivo. Essa verificação ocorre após o recebimento da identidade do equipamento, possibilitando a tomada de decisão quanto à continuidade ou rejeição do processo de autenticação.

Essa abordagem permite simular o comportamento de um EIR real, introduzindo um mecanismo de controle seletivo de acesso à rede. Além disso, a utilização de um serviço externo facilita a adaptação e expansão do sistema, possibilitando a implementação de políticas mais complexas de gerenciamento de dispositivos em trabalhos futuros.

3.2 Fluxo do Sistema

Nesta seção são apresentados os fluxos de funcionamento do sistema antes e após a implementação do mecanismo de verificação de identidade de equipamentos (EIR). Essa abordagem permite evidenciar as modificações introduzidas no processo de autenticação da rede, bem como destacar as contribuições da solução proposta.

3.2.1 Fluxo do Sistema Funcionamento convencional

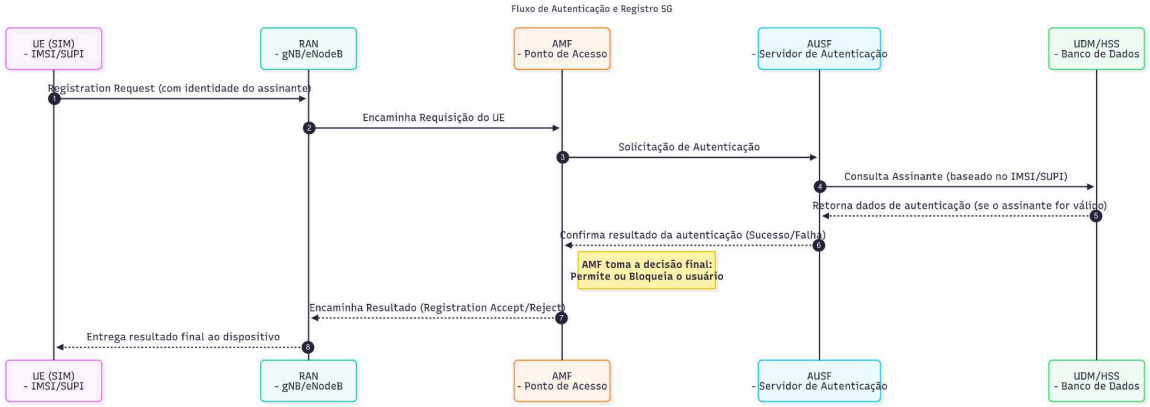
No funcionamento padrão do núcleo 5G, sem a integração de um sistema EIR, o processo de autenticação do dispositivo ocorre exclusivamente com base nas credenciais do assinante, como o *International Mobile Subscriber Identity* (IMSI) e as chaves de autenticação armazenadas no núcleo da rede.

Nesse cenário, não há verificação da identidade do equipamento (IMEI), o que implica que dispositivos não autorizados podem acessar a rede desde que possuam credenciais válidas de assinante.

Nesse modelo, observa-se que o controle de acesso está centrado

exclusivamente no assinante, não considerando a legitimidade do equipamento utilizado.

Figura 5: Diagrama de Comunicação 5G.



fonte:Autoria própria(2025).

Sendo:

1. **UE → RAN (*Registration Request*):** O seu celular ou dispositivo (UE), contendo o SIM card com sua identidade de assinante (IMSI/SUPI), liga ou entra em uma área de cobertura e envia um pedido de registro para a rede através da torre de rádio mais próxima (**RAN**).
2. **RAN → AMF (Encaminha Requisição):** A RAN, sendo apenas uma ponte, não toma decisões. Ela simplesmente pega o pedido do UE e o encaminha para o "cérebro" da rede, a AMF. Como você disse, a AMF recebe o UE.
3. **AMF → AUSF (Solicitação de Autenticação):** A AMF vê que um novo dispositivo quer se registrar e precisa verificar sua identidade. Ela delega essa tarefa de segurança para o especialista, o servidor de autenticação (AUSF).
4. **AUSF → UDM (Consulta Assinante):** A AUSF precisa das "credenciais" do assinante para realizar o desafio criptográfico. Ela consulta o banco de dados mestre (UDM) para verificar se o IMSI/SUPI do assinante existe e para obter os vetores de autenticação associados a ele. Esta é a "Consulta IMSI/Assinan**te"** que você mencionou.
5. **UDM → AUSF (Retorno de Dados):** A UDM verifica em sua base de dados. Se o assinante existe e é válido (está na sua "whitelist"), ela retorna os dados de segurança para a AUSF. Se não encontrar o assinante, ela informa que

ele é desconhecido e o processo para aqui.

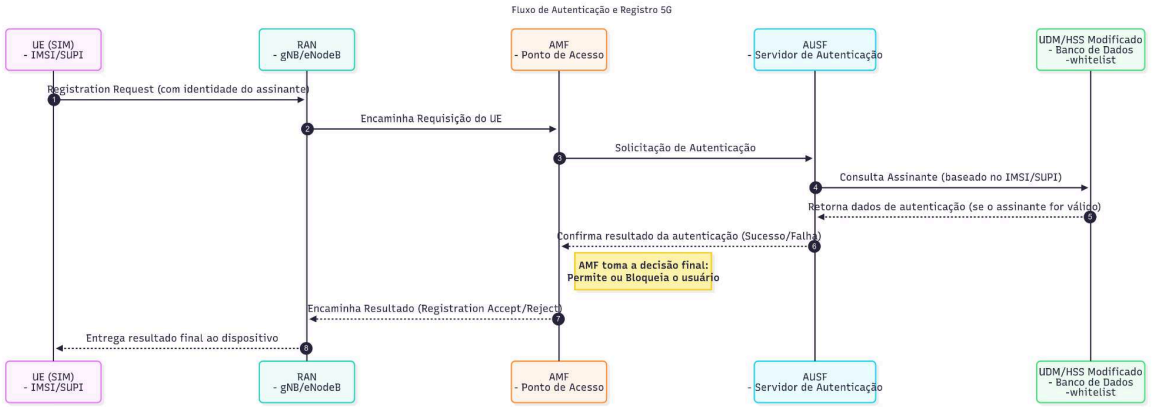
6. **AUSF → AMF (Confirma Resultado):** A AUSF realiza o procedimento de autenticação com o UE (um desafio criptográfico que omitimos no diagrama para simplificar) e informa o resultado final (sucesso ou falha) para a AMF.
7. **Decisão Final na AMF:** Com a confirmação da AUSF, a AMF toma a decisão final: permitir ou não o usuário na rede. Ela verifica outras políticas e se prepara para aceitar ou rejeitar a conexão.
8. **AMF → RAN (Encaminha Resultado):** A AMF envia sua decisão final de volta para a **RAN**.
9. **RAN → UE (Entrega Resultado Final):** A RAN, novamente atuando como uma ponte, encaminha o resultado para o dispositivo do usuário (UE), que agora sabe se seu registro na rede foi aceito ou negado.

3.2.2 Fluxo do Sistema com Implementação do EIR

Com a implementação do sistema EIR, foi introduzida uma etapa adicional no processo de autenticação, permitindo a verificação da identidade do equipamento por meio do IMEI. Essa modificação adiciona uma camada extra de segurança ao sistema, possibilitando o bloqueio seletivo de dispositivos.

O fluxo modificado ocorre conforme as etapas a seguir:

Figura 6: Diagrama de Comunicação 5G novo.



fonte:Autoria própria(2025).

No modelo tradicional de funcionamento do núcleo de redes móveis 5G, o processo de autenticação é realizado exclusivamente com base nas credenciais do assinante, como o identificador IMSI e as chaves de autenticação armazenadas nas funções centrais da rede. Nesse contexto, o dispositivo é autorizado a acessar a rede desde que apresente credenciais válidas, não sendo realizada qualquer verificação da identidade física do equipamento utilizado. Como consequência, um dispositivo potencialmente não autorizado pode obter acesso à rede caso utilize um assinante legítimo, evidenciando uma limitação no controle de acesso baseado apenas na identidade do usuário.

Com a implementação do sistema EIR proposta neste trabalho, o fluxo de autenticação passa a incorporar uma etapa adicional de verificação da identidade do equipamento por meio do IMEI. Após a obtenção dessa informação pelo AMF, o identificador é encaminhado a um servidor externo responsável por validar a legitimidade do dispositivo, permitindo a tomada de decisão quanto à continuidade do acesso. Dessa forma, além da autenticação do assinante, passa a ser considerada também a autenticidade do equipamento, possibilitando o bloqueio seletivo de dispositivos específicos. Essa modificação introduz uma camada adicional de segurança ao sistema, tornando o controle de acesso mais robusto e alinhado às necessidades de gestão eficiente da rede.

3.2 Modificação do sistema de autenticação

A modificação do sistema de autenticação proposta neste trabalho introduz uma alteração significativa no fluxo de registro da rede 5G, ao incorporar a verificação da identidade do equipamento como critério adicional para concessão de acesso. No modelo padrão definido pelo 3GPP (TS 23.501 e TS 24.501), o processo de autenticação é centrado exclusivamente na identidade do assinante, utilizando identificadores como o SUCI/IMSI e mecanismos de autenticação suportados pelas funções UDM (*Unified Data Management*) e AUSF (*Authentication Server Function*). Nesse contexto, a rede estabelece confiança com base nas credenciais do usuário, não considerando, de forma obrigatória, a legitimidade do dispositivo físico utilizado para acesso.

Com o objetivo de superar essa limitação, foi realizada uma modificação no comportamento do *Access and Mobility Management Function* (AMF), responsável pelo gerenciamento do registro e mobilidade do usuário. Essa modificação consistiu na inserção explícita de uma etapa de solicitação da identidade do equipamento por meio da mensagem *Identity Request*, forçando o dispositivo a fornecer seu identificador físico durante o procedimento de autenticação. A resposta do dispositivo, por meio da mensagem *Identity Response*, contém o identificador do equipamento, que pode ser o IMEI ou o IMEISV, conforme definido pelas especificações do 3GPP (TS 23.003).

O IMEI (*International Mobile Equipment Identity*) é um identificador numérico de 15 dígitos estruturado em três componentes: o *Type Allocation Code* (TAC), responsável por identificar o modelo do equipamento; o *Serial Number* (SNR), que individualiza o dispositivo; e o dígito verificador (*Check Digit*), calculado pelo algoritmo de Luhn, utilizado para validação da integridade do número. Em aplicações práticas, especialmente em sistemas de controle como o EIR, é comum a utilização apenas dos 14 primeiros dígitos (TAC + SNR), uma vez que o último dígito não agrega informação de identificação, sendo destinado exclusivamente à verificação matemática do código.

De forma complementar, o IMEISV (*International Mobile Equipment Identity and Software Version*) expande o conceito do IMEI ao incluir dois dígitos adicionais que representam a versão de software do equipamento (*Software Version Number* – SVN), totalizando 16 dígitos. Nesse caso, os 14 primeiros dígitos continuam representando a identidade física do dispositivo, enquanto os dois últimos permitem distinguir variações de firmware. A ausência do dígito verificador no IMEISV implica que sua validação não depende do algoritmo de Luhn, sendo mais voltada à diferenciação de versões do equipamento do que à verificação estrutural do identificador.

Adicionalmente, destaca-se o ICCID (*Integrated Circuit Card Identifier*), identificador associado ao cartão SIM, composto por uma sequência numérica que identifica de forma única o chip do assinante. Embora relevante para operações de provisionamento e gerenciamento, o ICCID não representa o equipamento físico e, portanto, não é adequado para controle de acesso baseado em dispositivo. Ainda assim, sua distinção em relação ao IMEI e IMEISV é fundamental para compreender a separação entre identidade do assinante e identidade do equipamento no contexto

das redes móveis.

A partir da obtenção do identificador do equipamento, o sistema modificado realiza o encaminhamento dessa informação a um servidor externo EIR por meio de uma requisição HTTP, implementada com o uso da biblioteca libcurl integrada ao Open5GS. Essa integração ocorre diretamente no fluxo de processamento do AMF, especificamente após a recepção da identidade do dispositivo, caracterizando uma interceptação ativa no procedimento de autenticação. O servidor EIR, por sua vez, realiza a análise do identificador com base em políticas previamente definidas, retornando uma resposta que classifica o dispositivo como autorizado ou bloqueado.

A decisão final de acesso passa, então, a ser condicionada não apenas à autenticação do assinante, mas também à validação do equipamento. Caso o dispositivo seja considerado legítimo, o fluxo de autenticação segue conforme o padrão estabelecido pelo 3GPP. Em contrapartida, caso o equipamento esteja associado a uma condição de bloqueio, o AMF interrompe o processo de registro, impedindo o estabelecimento da conexão com a rede. Essa intervenção ocorre antes da conclusão da autenticação, caracterizando um mecanismo preventivo de controle de acesso.

Dessa forma, a modificação introduzida redefine o modelo tradicional de autenticação ao transformar um processo unidimensional, baseado apenas no assinante, em um modelo bidimensional, que considera simultaneamente a identidade do usuário e do equipamento. Essa abordagem amplia significativamente a capacidade de controle da rede, permitindo a implementação de políticas de segurança mais rigorosas e alinhadas às demandas atuais de gestão de dispositivos, além de se apresentar como uma alternativa tecnicamente superior a métodos indiscriminados, como o uso de bloqueadores de sinal (*jammers*), por possibilitar ações seletivas, rastreáveis e compatíveis com a operação regular da rede.

3.3 Comparação entre bloqueadores

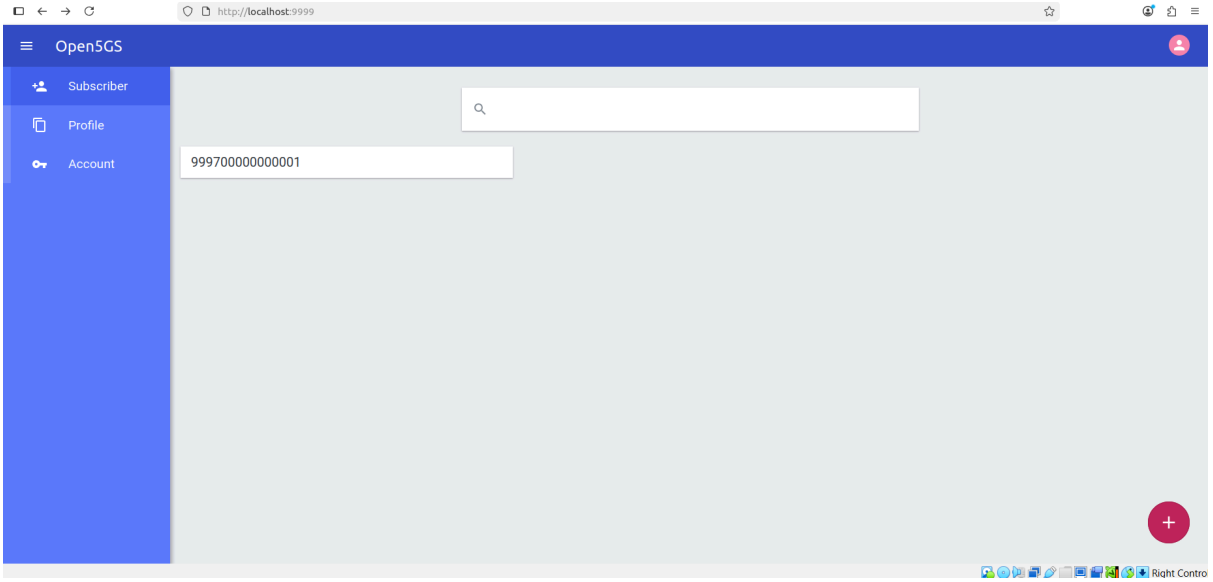
4 RESULTADOS E DISCUSSÕES

4.1 Validação do Ambiente Experimental

Após a implementação do ambiente descrito no Capítulo 3, foram realizados testes para validar o correto funcionamento da rede 5G emulada. Inicialmente, verificou-se a comunicação entre os componentes do núcleo da rede (Open5GS) e o sistema de emulação (UERANSIM), confirmando o estabelecimento do processo de registro do dispositivo e a autenticação do assinante.

Como parte essencial da validação do ambiente, foi realizado o cadastro de usuários por meio da interface web MongoDB, utilizada pelo Open5GS para gerenciamento das informações dos assinantes. O acesso à interface é realizado via navegador, geralmente por meio do endereço local do servidor (por exemplo, **http://127.0.0.1:9999**), onde é possível inserir manualmente os dados necessários para autenticação na rede.

Figura 7: Interface Open5GS.



Fonte: Autoria Própria (2026).

O processo de cadastro consiste na inclusão de informações como **IMSI (International Mobile Subscriber Identity)**, chave de autenticação (*Key*), código de autenticação (*OP/OPc*), além de parâmetros relacionados ao perfil de serviço do usuário.

Esses dados são fundamentais para que o núcleo da rede consiga autenticar corretamente o dispositivo durante o processo de registro.

Após o cadastro, o sistema de emulação de usuário (UERANSIM) é configurado com os mesmos parâmetros, permitindo que o dispositivo virtual realize a tentativa de conexão. A correspondência entre os dados cadastrados no banco e os utilizados pelo emulador é essencial para o sucesso da autenticação.

Os testes demonstraram que, uma vez corretamente configurado, o usuário é capaz de se registrar na rede e estabelecer comunicação com o núcleo 5G, confirmando a integridade do ambiente experimental. Essa etapa foi fundamental para garantir que as modificações introduzidas posteriormente, como a integração do sistema EIR, pudessem ser avaliadas de forma isolada e confiável.

4.2 Resultados sem a Implementação do EIR

No cenário sem a utilização do sistema EIR, foi observado que o processo de autenticação ocorria normalmente, sem qualquer verificação da identidade do equipamento. O dispositivo, ao enviar sua solicitação de registro, era autenticado com base nas credenciais do assinante, sendo posteriormente autorizado a acessar a rede.

Mesmo em situações onde o IMEI do dispositivo era considerado inválido ou não autorizado no contexto do experimento, a rede não realizava qualquer tipo de bloqueio, uma vez que essa informação não era utilizada no processo decisório. Esse comportamento evidencia uma limitação do modelo tradicional, no qual não há distinção entre dispositivos legítimos e potencialmente comprometidos.

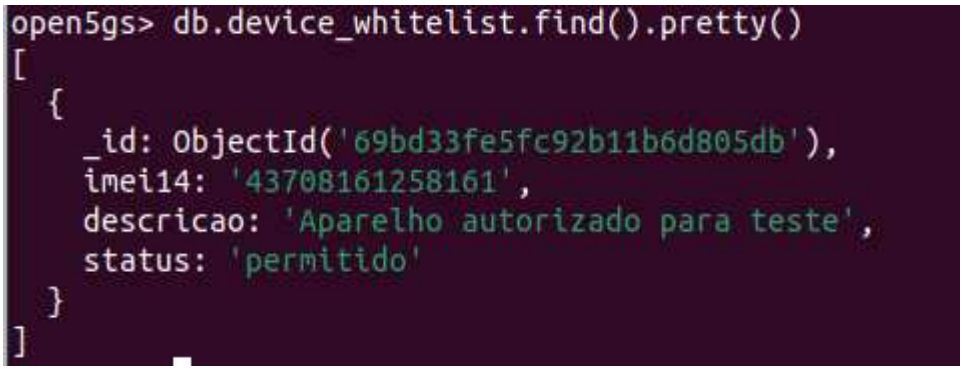
Essa ausência de controle sobre o equipamento reforça a necessidade de mecanismos adicionais de segurança, especialmente em cenários onde há risco de utilização indevida da rede por dispositivos não autorizados.

4.3 Resultados com a Implementação do EIR

Com a integração do sistema EIR ao núcleo da rede, foi possível observar mudanças significativas no comportamento do processo de autenticação. A inclusão

da verificação do IMEI introduziu um novo critério de decisão, permitindo o controle seletivo de dispositivos.

Figura 8: Whitelist.



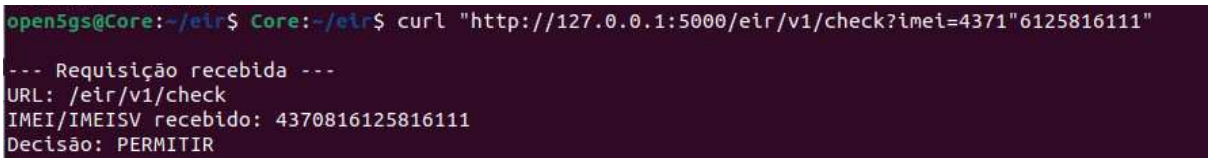
Fonte: Autoria Própria (2026).

Durante os testes, foram analisados dois cenários principais:

4.3.1 Dispositivo autorizado

Quando o IMEI do dispositivo estava presente na base de dados do EIR como autorizado, o servidor retornava uma resposta positiva ao AMF. Nesse caso, o fluxo de autenticação seguia normalmente, permitindo o registro do dispositivo na rede e o estabelecimento de sessões de comunicação.

Figura 9: Resposta Dispositivo autorizado.



Fonte: Autoria Própria (2026).

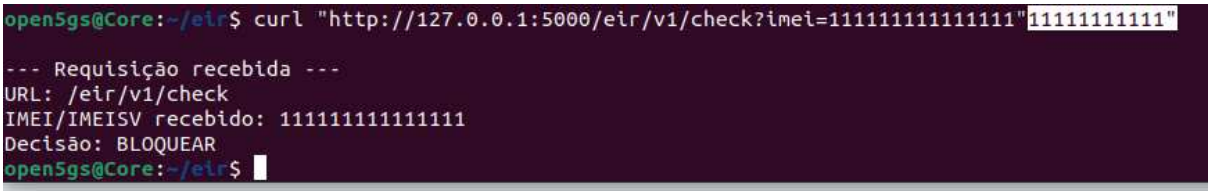
Os logs do sistema indicaram que a consulta ao EIR não interferiu de forma significativa no funcionamento do processo, mantendo a transparência para dispositivos legítimos.

4.3.2 Dispositivo bloqueado

No cenário em que o IMEI do dispositivo estava classificado como bloqueado, o servidor EIR retornava uma resposta negativa ao AMF. Como resultado, o processo de autenticação era interrompido antes de sua conclusão, impedindo o registro do dispositivo na rede.

Observou-se que o bloqueio ocorreu de forma imediata e seletiva, afetando apenas o dispositivo identificado, sem impacto sobre outros usuários ou sobre a estabilidade da rede.

Figura 10: Resposta Dispositivo negado.



Fonte: Autoria Própria (2026).

Esse comportamento demonstra a eficácia do mecanismo proposto na restrição de acesso com base na identidade do equipamento.

4.4 Resultados com a Implementação do EIR

Os resultados obtidos permitem estabelecer uma comparação direta entre a abordagem proposta, baseada no EIR, e métodos tradicionais de bloqueio de dispositivos, como o uso de bloqueadores de sinal (*jammers*).

Os *jammers* atuam por meio da emissão de interferência eletromagnética, impedindo a comunicação entre dispositivos e a rede de forma indiscriminada. Essa abordagem, além de afetar todos os usuários na área de cobertura, pode comprometer serviços críticos e é, em muitos casos, restrita por regulamentações.

Em contraste, o sistema EIR implementado neste trabalho permite um controle seletivo, baseado na identidade do dispositivo. Apenas equipamentos previamente identificados como não autorizados são bloqueados, enquanto os demais continuam operando normalmente.

Além disso, a abordagem baseada em EIR apresenta vantagens adicionais, como:

- maior controle e rastreabilidade dos dispositivos;
- ausência de interferência no espectro de radiofrequência;
- conformidade com boas práticas de engenharia e regulamentação.

Dessa forma, os resultados demonstram que a utilização do EIR constitui uma alternativa tecnicamente superior aos bloqueadores de sinal, especialmente em cenários que exigem controle preciso e seletivo do acesso à rede.

5 CONCLUSÃO

O presente trabalho teve como objetivo a implementação e análise de um mecanismo de controle de acesso baseado na identidade de equipamentos em redes móveis 5G, por meio da integração de um servidor EIR ao núcleo de rede Open5GS. A proposta buscou superar limitações do modelo tradicional de autenticação, que considera exclusivamente a identidade do assinante, sem levar em conta a legitimidade do dispositivo utilizado.

A partir da construção de um ambiente experimental virtualizado, utilizando ferramentas como Open5GS e UERANSIM, foi possível validar o funcionamento do núcleo 5G e reproduzir o processo de autenticação de dispositivos. Com base nesse ambiente, foi realizada a modificação do fluxo de autenticação, incorporando uma etapa adicional de verificação do IMEI por meio de um servidor EIR externo.

Os resultados obtidos demonstraram que, na ausência do EIR, a rede não realiza distinção entre dispositivos, permitindo o acesso mesmo quando o equipamento não é confiável. Por outro lado, com a implementação do mecanismo proposto, foi possível realizar o bloqueio seletivo de dispositivos com base em sua identidade, sem impactar o funcionamento da rede para usuários legítimos.

A comparação com métodos tradicionais de bloqueio, como o uso de *jammers*, evidenciou que a abordagem baseada em EIR apresenta vantagens significativas, incluindo maior precisão no controle de acesso, ausência de interferência no espectro de radiofrequência e maior conformidade com regulamentações. Dessa forma, a solução proposta se mostra mais adequada para aplicações que exigem segurança e controle refinado sobre os dispositivos conectados.

Além disso, o trabalho demonstrou que a integração do EIR pode ser realizada de forma modular e com baixo impacto na arquitetura existente, permitindo sua adaptação a diferentes cenários e aplicações. A utilização de um servidor externo para a verificação do IMEI contribui para a flexibilidade da solução,

possibilitando futuras expansões, como a integração com bases de dados reais ou sistemas de gerenciamento centralizado.

Como limitações do estudo, destaca-se o fato de o ambiente experimental ser baseado em emulação, o que, embora adequado para validação conceitual, pode não refletir completamente as condições de redes reais. Além disso, o servidor EIR implementado possui caráter simplificado, não contemplando todas as funcionalidades presentes em sistemas comerciais.

Como trabalhos futuros, propõe-se a realização de uma análise financeira comparativa entre a solução baseada em EIR e métodos tradicionais, como o uso de bloqueadores de sinal e a implantação de infraestrutura dedicada de rede móvel. Essa análise deve considerar diferentes cenários de aplicação, uma vez que os custos associados a *jammers*, à instalação de antenas e à implementação do núcleo de rede podem variar de forma não linear em função da área de cobertura, densidade de usuários e características do ambiente. Dessa forma, estudos econômicos complementares podem contribuir para a avaliação da viabilidade prática da solução proposta em contextos reais.

Também se sugere a implementação de uma base de dados mais robusta para o EIR, a integração com sistemas reais de gerenciamento de equipamentos, bem como a análise de desempenho do impacto da verificação do IMEI no tempo de autenticação. Adicionalmente, recomenda-se a validação da solução em ambientes reais ou semi-reais, visando avaliar sua escalabilidade, confiabilidade e aplicabilidade em cenários operacionais.

Por fim, conclui-se que a utilização de mecanismos de controle baseados na identidade do equipamento representa uma abordagem promissora para o aumento da segurança em redes móveis, especialmente no contexto das redes 5G, onde a diversidade de dispositivos conectados exige soluções cada vez mais eficientes, seletivas e adaptáveis.

REFERÊNCIAS

AGYAPONG, P. et al. *Design considerations for a 5G network architecture*. IEEE Communications Magazine, v. 52, n. 11, p. 65–75, nov. 2014.

CAMPOS, J. *Bloqueadores não funcionam e celulares são usados pelo crime organizado em prisões do RS*. G1, 2025. Disponível em: https://g1.globo.com/google/amp/rs/rio-grande-do-sul/noticia/2025/05/16/bloqueadores-nao-funcionam-e-celulares-sao-usados-pelo-crime-organizado-em-prisoes-do-rs.ghtml. Acesso em: 8 jul. 2025.

GSMA. *IMEI Allocation and Approval Guidelines*. Disponível em: https://www.gsma.com. Acesso em: 20 mar. 2026.

GOLDSMITH, A. *Wireless Communications*. Cambridge: Cambridge University Press, 2005.

MIRANDA, T. *Comissão aprova projeto que obriga presídio a instalar bloqueador de celular*. Agência Câmara de Notícias, 2024. Disponível em: https://www.camara.leg.br/noticias/1164657-comissao-aprova-projeto-que-obriga-presidio-a-instalar-bloqueador-de-celular. Acesso em: 8 jul. 2025.

MONGODB. *MongoDB Database Platform*. Disponível em: https://www.mongodb.com. Acesso em: 20 mar. 2026.

OPEN5GS. *Open source 5G Core and EPC implementation*. Disponível em: https://open5gs.org. Acesso em: 20 mar. 2026.

PAGNAN, R. *PCC comandava crime até em presídio com bloqueador de celular*. Folha de S. Paulo, 2018. Disponível em: https://www1.folha.uol.com.br/cotidiano/2018/07/pcc-comandava-crime-ate-em-presidio-com-bloqueador-de-celular.shtml. Acesso em: 8 jul. 2025.

SHANNON, C. E.; WEAVER, W. *The mathematical theory of communication*. Urbana: University of Illinois Press, 1949.

STALLINGS, W. *Wireless Communications and Networks*. 2. ed. Upper Saddle River: Pearson, 2005.

3GPP. *Procedures for the 5G System (5GS)*. TS 23.502. Disponível em: https://www.3gpp.org. Acesso em: 20 mar. 2026.

3GPP. *Security architecture and procedures for 5G system*. TS 33.501. Disponível em: https://www.3gpp.org. Acesso em: 20 mar. 2026.

3GPP. *System Architecture for the 5G System (5GS)*. TS 23.501. Disponível em: https://www.3gpp.org. Acesso em: 20 mar. 2026.

UBUNTU. *Ubuntu 22.04 LTS*. Disponível em: https://ubuntu.com. Acesso em: 20 mar. 2026.

UERANSIM. *5G UE and RAN simulator*. Disponível em: https://github.com/aligungr/UERANSIM. Acesso em: 20 mar. 2026.

7 Anexos

ANEXO A – Código do servidor EIR

Este anexo apresenta o código final do servidor EIR, composto pelos arquivos *eir_server.h* e *eir_server.c*.

A.1 Arquivo eir_server.h

```
#ifndef EIR_SERVER_H
#define EIR_SERVER_H

#define EIR_PORT 5000

int iniciar_servidor_eir(void);

#endif
```

A.2 Arquivo eir_server.c

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <microhttpd.h>

#include "eir_server.h"
#include "eir_validation.h"

#define RESPONSE_BUFFER_SIZE 256

static int send_json_response(struct MHD_Connection *connection,
                              const char *json,
                              int status_code)
{
    struct MHD_Response *response;
    int ret;

    response = MHD_create_response_from_buffer(
        strlen(json),
        (void *)json,
        MHD_RESPMEM_MUST_COPY
    );
```

```
    if (!response)
        return MHD_NO;

    MHD_add_response_header(response, "Content-Type", "application/json");
    ret = MHD_queue_response(connection, status_code, response);
    MHD_destroy_response(response);

    return ret;
}

static void extrair_imei14(const char *imei_in, char *imei14_out)
{
    int i;

    if (!imei_in || !imei14_out) {
        return;
    }

    for (i = 0; i < 14 && imei_in[i] != '\0'; i++) {
        imei14_out[i] = imei_in[i];
    }

    imei14_out[i] = '\0';
}

static int request_handler(void *cls,
                           struct MHD_Connection *connection,
                           const char *url,
                           const char *method,
                           const char *version,
                           const char *upload_data,
                           size_t *upload_data_size,
                           void **con_cls)
{
    const char *imei_param;
    char imei14[15];
    char json[RESPONSE_BUFFER_SIZE];
    int autorizado;

    (void)cls;
    (void)version;
    (void)upload_data;
    (void)upload_data_size;
    (void)con_cls;

    if (strcmp(method, "GET") != 0) {
        return send_json_response(
            connection,
            "{\"error\":\"method_not_allowed\"}",
```

```
            MHD_HTTP_METHOD_NOT_ALLOWED
        );
    }

    if (strcmp(url, "/eir/v1/check") != 0) {
        return send_json_response(
            connection,
            "{\"error\":\"not_found\"}",
            MHD_HTTP_NOT_FOUND
        );
    }

    imei_param = MHD_lookup_connection_value(
        connection,
        MHD_GET_ARGUMENT_KIND,
        "imei"
    );

    if (!imei_param) {
        return send_json_response(
            connection,
            "{\"error\":\"imei_not_informed\"}",
            MHD_HTTP_BAD_REQUEST
        );
    }

    extrair_imei14(imei_param, imei14);

    if (strlen(imei14) != 14) {
        return send_json_response(
            connection,
            "{\"error\":\"invalid_imei\"}",
            MHD_HTTP_BAD_REQUEST
        );
    }

    autorizado = validar_imei14_no_mongo(imei14);

    if (autorizado) {
        snprintf(json, sizeof(json),
                 "{\"status\":0,\"imei14\":\"%s\",\"message\":\"allowed\"}",
                 imei14);
        return send_json_response(connection, json, MHD_HTTP_OK);
    } else {
        snprintf(json, sizeof(json),
                 "{\"status\":1,\"imei14\":\"%s\",\"message\":\"blocked\"}",
                 imei14);
        return send_json_response(connection, json, MHD_HTTP_FORBIDDEN);
    }
}
```

```
int iniciar_servidor_eir(void)
{
   struct MHD_Daemon *daemon;

   daemon = MHD_start_daemon(
      MHD_USE_INTERNAL_POLLING_THREAD,
      EIR_PORT,
      NULL,
      NULL,
      &request_handler,
      NULL,
      MHD_OPTION_END
   );

   if (!daemon) {
      fprintf(stderr, "Erro ao iniciar o servidor EIR na porta %d.\n", EIR_PORT);
      return 1;
   }

   printf("Servidor EIR iniciado na porta %d.\n", EIR_PORT);
   printf("Endpoint: http://127.0.0.1:%d/eir/v1/check?imei=<imei>\n", EIR_PORT);

   getchar();

   MHD_stop_daemon(daemon);
   printf("Servidor finalizado.\n");

   return 0;
}

int main(void)
{
   return iniciar_servidor_eir();
}
```

ANEXO B – Código do Cliente EIR

Este anexo apresenta o código final do cliente EIR integrado ao AMF, composto pelos arquivos *eir-client.h* e *eir-client.c*.

B.1 Arquivo eir-client.h

```
#ifndef AMF_EIR_CLIENT_H
#define AMF_EIR_CLIENT_H

int amf_eir_check_imei14(const char *imeisv_bcd);

#endif
```

B.2 Arquivo eir-client.c

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

#include "eir-client.h"

static void extrair_imei14(const char *imeisv_bcd, char *imei14)
{
    if (!imeisv_bcd || strlen(imeisv_bcd) < 14) {
        imei14[0] = '\0';
        return;
    }

    strncpy(imei14, imeisv_bcd, 14);
    imei14[14] = '\0';
}

int amf_eir_check_imei14(const char *imeisv_bcd)
{
    char imei14[15];
    char cmd[512];
    char buffer[256];
    FILE *fp;
```

```
    extrair_imei14(imeisv_bcd, imei14);
    if (imei14[0] == '\0')
        return 0;

    snprintf(cmd, sizeof(cmd),
        "curl -s --max-time 2 \"http://127.0.0.1:5000/eir/v1/check?imei=%s\"",
        imei14);

    fp = popen(cmd, "r");
    if (!fp)
        return 0;

    buffer[0] = '\0';
    if (fgets(buffer, sizeof(buffer), fp) == NULL) {
        pclose(fp);
        return 0;
    }

    pclose(fp);

    if (strstr(buffer, "\"status\":0"))
        return 1;

    return 0;
}
```

ANEXO C – MODIFICAÇÃO DO ARQUIVO *gmm-handler.c*

C.1 Inclusão do cabeçalho do cliente EIR.

```
#include "nas-security.h"

#include "ngap-path.h"
```

```
#include "nas-path.h"
#include "sbi-path.h"

#include "gmm-handler.h"
#include "eir-client.h"

#undef OGS_LOG_DOMAIN
#define OGS_LOG_DOMAIN __gmm_log_domain
```

C.2 Trecho inserido em *gmm_handle_security_mode_complete.*

```
if (security_mode_complete->presencemask &
    OGS_NAS_5GS_SECURITY_MODE_COMPLETE_IMEISV_PRESENT) {

    imeisv = &security_mode_complete->imeisv;
    ogs_assert(imeisv);
    mobile_identity_imeisv =
        (ogs_nas_mobile_identity_imeisv_t *)imeisv->buffer;
    ogs_assert(mobile_identity_imeisv);

    switch (mobile_identity_imeisv->type) {
    case OGS_NAS_5GS_MOBILE_IDENTITY_IMEISV:
        /* TS23.003 6.2.2 Composition of IMEISV
         *
         * The International Mobile station Equipment Identity and
         * Software Version Number (IMEISV) is composed.
         *
         * TAC(8 digits) - SNR(6 digits) - SVN(2 digits)
         * IMEISV(16 digits) ==> 8bytes
         */
        if (imeisv->length == sizeof(ogs_nas_mobile_identity_imeisv_t)) {
            memcpy(&amf_ue->nas_mobile_identity_imeisv,
                mobile_identity_imeisv, imeisv->length);
            ogs_nas_imeisv_to_bcd(mobile_identity_imeisv, imeisv->length,
                    amf_ue->imeisv_bcd);
```

```
            ogs_nas_imeisv_bcd_to_buffer(amf_ue->imeisv_bcd,
                    amf_ue->masked_imeisv, &amf_ue->masked_imeisv_len);
            amf_ue->masked_imeisv[5] = 0xff;
            amf_ue->masked_imeisv[6] = 0xff;
            if (amf_ue->pei)
                ogs_free(amf_ue->pei);
            amf_ue->pei = ogs_msprintf("imeisv-%s", amf_ue->imeisv_bcd);
            ogs_assert(amf_ue->pei);

            if (!amf_eir_check_imei14(amf_ue->imeisv_bcd)) {
                ogs_error("[%s] IMEI not allowed by EIR [%s]",
                        amf_ue->supi ? amf_ue->supi : "unknown",
                        amf_ue->imeisv_bcd);
                                                                    return
OGS_5GMM_CAUSE_UE_IDENTITY_CANNOT_BE_DERIVED_BY_THE_NETWO
RK;
            }
        } else {
            ogs_error("[%s] Unknown IMEISV Length [%d]",
                    amf_ue->supi, imeisv->length);
            ogs_log_hexdump(OGS_LOG_ERROR, imeisv->buffer, imeisv->length);
        }
        break;
    default:
        ogs_warn("[%s] Invalid IMEISV Type [%d]",
                amf_ue->supi, mobile_identity_imeisv->type);
        break;

    }
}
```