Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Bacharelado em Ciência da Computação

Aplicação da Arquitetura *Zero-Trust* para a Segurança de Recursos em Redes 5G

Victor Duque Alves Pinto

JUIZ DE FORA
MARÇO, 2025

Aplicação da Arquitetura *Zero-Trust* para a Segurança de Recursos em Redes 5G

Victor Duque Alves Pinto

Universidade Federal de Juiz de Fora

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Bacharelado em Ciência da Computação

Orientador: Edelberto Franco Silva

JUIZ DE FORA

MARÇO, 2025

Aplicação da Arquitetura *Zero-Trust* para a Segurança de Recursos em Redes 5G

Victor Duque Alves Pinto

MONOGRAFIA SUBMETIDA AO CORPO DOCENTE DO INSTITUTO DE CIÊNCIAS EXATAS DA UNIVERSIDADE FEDERAL DE JUIZ DE FORA, COMO PARTE INTEGRANTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE BACHAREL EM CIÊNCIA DA COMPUTAÇÃO.

Aprovada por:

Edelberto Franco Silva
Doutor em Ciência da Computação

Alex Borges Vieira
Doutor em Ciência da Computação

Luciano Jerez Chaves
Doutor em Ciência da Computação

JUIZ DE FORA
13 DE MARÇO, 2025

Resumo

A tecnologia 5G trouxe avanços em velocidade e conectividade, mas também novos desafios de segurança, especialmente devido ao aumento da utilização de dispositivos IoT. Este trabalho investiga a aplicação da arquitetura *Zero-Trust* (ZTA) para reforçar a segurança no controle de acesso a recursos em redes 5G. A metodologia inclui o desenvolvimento e teste de uma aplicação baseada no modelo ZTA, considerando a confiabilidade do usuário, do dispositivo e do histórico de acessos. Os experimentos demonstraram que a solução proposta foi eficaz na identificação de acessos suspeitos, mitigando riscos como roubo de chip e ataques DoS. Como contribuição, o estudo apresenta um modelo teórico de segurança *Zero-Trust* aplicado ao 5G, detalha sua implementação e avalia seu desempenho em cenários de ataque. Os resultados indicam que a abordagem pode fortalecer a proteção de recursos críticos, garantindo maior segurança para redes 5G.

Palavras-chave: *Zero-Trust*, 5G, segurança, fatias de rede

Abstract

The 5G technology has brought advancements in speed and connectivity but also new security challenges, especially due to the increased use of IoT devices. This study investigates the application of the Zero-Trust Architecture (ZTA) to enhance security in access control for 5G network resources. The methodology includes the development and testing of an application based on the ZTA model, considering user, device, and access history reliability. The experiments demonstrated that the proposed solution was effective in identifying suspicious access attempts, mitigating risks such as SIM card theft and DoS attacks. As a contribution, the study presents a theoretical security model of Zero-Trust applied to 5G, details its implementation, and evaluates its performance in attack scenarios. The results indicate that this approach can strengthen the protection of critical resources, ensuring greater security for 5G networks.

Keywords: Zero-Trust, 5G, security, network slices

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Abreviações

3GPP	*3rd Generation Partnership Project*
5GC	*5G Core*
5GS	*5G System*
ABAC	*Attribute-Based Access Control*
AMF	*Access and Mobility management Function*
API	*Application Programming Interface*
AUSF	*Authentication Server Function*
DoS	*Denial of Service*
EAP	*Extensible Authentication Protocol*
EAP-AKA'	*EAP – Authentication and Key Agreement Prime*
eMBB	*Enhanced mobile broadband*
IoT	*Internet of Things*
ITU	*International Telecommunications Union*
MAC	*Media Access Control*
MSK	*Master Session Key*
mMTC	*Massive machine type communication*
NF	*Network Function*
NG-RAN	*Next Generation Radio Access Network*
NIST	*National Institute of Standards and Technology*
NWDAF	*Network Data Analysis Function*
PA	*Policy administrator*
PE	*Policy engine*
PDP	*Policy decision point*
PIP	*Policy information point*
PEP	*Policy enforcement point*
RBAC	*Role Based Access Control*
SBA	*Service-Based Architecture*
SDN	*Software defined networking*
SMF	*Session Management Function*
UDM	*Unified Data Management*
UE	*User Equipment*
USIM	*Universal Subscriber's Identity Module*
UPF	*User Plane Function*
URLLC	*Ultra-reliable low latency communication*
ZT	*Zero-Trust*
ZTA	*Zero-Trust Architecture*

1 Introdução

As redes móveis de quinta geração, mais conhecidas por 5G, foram implantadas no Brasil em 2022 e, em 2024, já havia mais de 810 municípios brasileiros, incluindo todas as capitais, com suporte a essa tecnologia (ANATEL, 2024). Essa tecnologia de redes móveis promete maior velocidade, segurança e robustez em comparação com as gerações anteriores, como 3G e 4G, além de menor latência e maior largura de banda. Além disso, é possível, por meio de, por exemplo, fatiamento das redes, fornecer requisitos específicos para aplicações que utilizem essa tecnologia. No entanto, sua complexidade e características intrínsecas introduzem novos desafios de cibersegurança (MECHAILEH, 2023).

A necessidade da avaliação do impacto da segurança é constatada desde as gerações anteriores de redes móveis, se intensificando com o advento do 5G. Usuários, sejam indivíduos ou empresas, demandam proteção robusta contra ataques cibernéticos. Um relatório do *Threat Intelligence Center* da Nokia destacou que o aumento no uso de dispositivos Internet das Coisas, do inglês *Internet of Things* (IoT) contribuiu para um crescimento significativo em ataques DDoS (Negação de Serviço Distribuída - *Distributed Denial-of-Service*) por *botnets*, saltando de 400 mil para quase 1 milhão de incidentes, representando mais de 40% dos ataques DDoS (CISO ADVISOR, 2023). Esse cenário é particularmente preocupante no contexto do 5G, que permite a conexão de um número ainda maior de dispositivos IoT, potencializando os riscos de ataques cibernéticos.

Além disso, violações de segurança em redes móveis podem causar grande impacto na rede, em função do potencial negativo que podem impor aos seus usuários e aos dados acessados e trafegados por eles. Tal impacto se torna ainda mais avassalador quando aplicado a um ambiente que suporta um número muito grande de dispositivos conectados. E um dos aspectos mais relevantes do 5G é a capacidade de suportar um número significativamente maior de dispositivos conectados; como exemplo, é possível citar aqueles relacionados à IoT. Tal suporte amplia a superfície de ataque para potenciais invasores, especialmente considerando que muitos dispositivos IoT possuem padrões

ou configurações de segurança inadequados (MECHAILEH, 2023). Como desafio central deste trabalho tem-se o fato de que, embora o 5G incorpore políticas e métodos de segurança mais robustos que suas predecessoras, essas medidas ainda são insuficientes para mitigar todos os riscos. A IoT, que se beneficia da maior capacidade de conexão do 5G, também introduz vulnerabilidades, pois muitos dispositivos carecem de padrões de segurança adequados. Essa lacuna pode ser explorada por invasores, aumentando o risco de ataques cibernéticos (KASPERSKY, 2023).

Diante desse cenário, a arquitetura *Zero-Trust* (ZTA - *Zero-Trust Architecture*) emerge como uma abordagem promissora para fortalecer a segurança do ambiente 5G. O modelo ZTA parte do princípio de que nenhum usuário ou dispositivo é intrinsecamente confiável, exigindo verificação e autorização contínuas para acessar recursos e sistemas computacionais. Essa constante avaliação dificulta a invasão de recursos críticos, especialmente em redes com uma superfície de ataque ampliada, como é o caso do 5G.

Desta forma, este trabalho propõe investigar a aplicação do modelo *Zero-Trust* no controle de acesso a aplicações sob fatias de redes 5G. Seguindo os padrões definidos pelo 3GPP-5G, tais como identidade digital segura, transporte seguro, políticas de *framework* e monitoramento de segurança (OLSSON et al., 2021), a integração do modelo *Zero-Trust* se faz possível como uma camada adicional para a segurança do ambiente como um todo. Para validar a viabilidade e eficácia da proposta, foram conduzidos experimentos em um ambiente computacional simulado dos componentes de redes 5G.

Como contribuições deste trabalho, temos:

1. a apresentação de uma base teórica relacionada aos tópicos que permeiam a tecnologia 5G, e o *Zero-Trust*;

2. a modelagem da aplicação proposta, definindo os passos necessários à sua implementação e integração ao 5G;

3. a realização de simulações em diferentes cenários de ataques e a discussão sobre a eficácia do *Zero-Trust* na proteção de aplicações e recursos ofertados por serviços da rede 5G.

O trabalho está organizado em seis capítulos, onde: o Capítulo 2 apresenta a

fundamentação teórica, abordando conceitos como arquitetura e serviços do 5G, *device fingerprint*, ataques *Denial of Service* (DoS), os tipos de controle de acesso e *Zero-Trust*; o Capítulo 3 revisa artigos relacionados ao tema, com foco em 5G e *Zero-Trust*; o Capítulo 4 detalha o desenvolvimento da aplicação proposta; o Capítulo 5 descreve os cenários e experimentos realizados; e, por fim, o Capítulo 6 apresenta as conclusões e contribuições do trabalho.

2 Fundamentação Teórica

Este capítulo tem o propósito de apresentar toda a fundamentação teórica do trabalho no que se refere aos tópicos do 5G (Seção 2.1), de SDN (Seção 2.2), de *device fingerprint* (Seção 2.3), de ataques de negação de serviço (Seção 2.4), de métodos de controle de acesso (Seção 2.5) e da ZTA (Seção 2.6).

2.1 Redes 5G

As redes 5G são a quinta geração das redes móveis, e são uma evolução das gerações anteriores, trazendo uma maior velocidade e largura de banda para os usuários. Para atingir esses objetivos, Dangi et al. (2022) cita que essas redes proporcionam suporte a três grupos de serviços aos usuários:

- a *enhanced mobile broadband* (eMBB), que disponibiliza uma maior conectividade da Internet e largura de banda, além de uma latência moderada;
- a *massive machine type communication* (mMTC), que fornece, com alto custo-benefício, uma conexão banda larga a longa distância, com baixo consumo de energia e alta cobertura de dispositivos, essencial para as aplicações IoT;
- a *ultra-reliable low latency communication* (URLLC), que traz uma baixa latência e excelente qualidade de serviço, o que não era possível na arquitetura tradicional de redes.

Conforme definido pela *International Telecommunication Union* (ITU), a agência destinada a tecnologia da informação e comunicação da ONU, cada um dos serviços mencionados tem os seus usos da Figura 2.1. O eMBB é, por exemplo, utilizado em *streaming de vídeos*, *cloud* e realidade aumentada, o URLLC, usado em automação industrial e veículos autônomos, e o mMTC, utilizado em sistemas IoT e monitoramento remoto via sensores (ITU, 2018). A ITU também determinou, em termos de latência, os requisitos

mínimos para esses serviços, que são 4 ms e 1 ms para eMBB e URLLC, respectivamente (ITU, 2017); o mMTC, por ser focado em uma cobertura maior das aplicações, possui uma latência mais elevada.

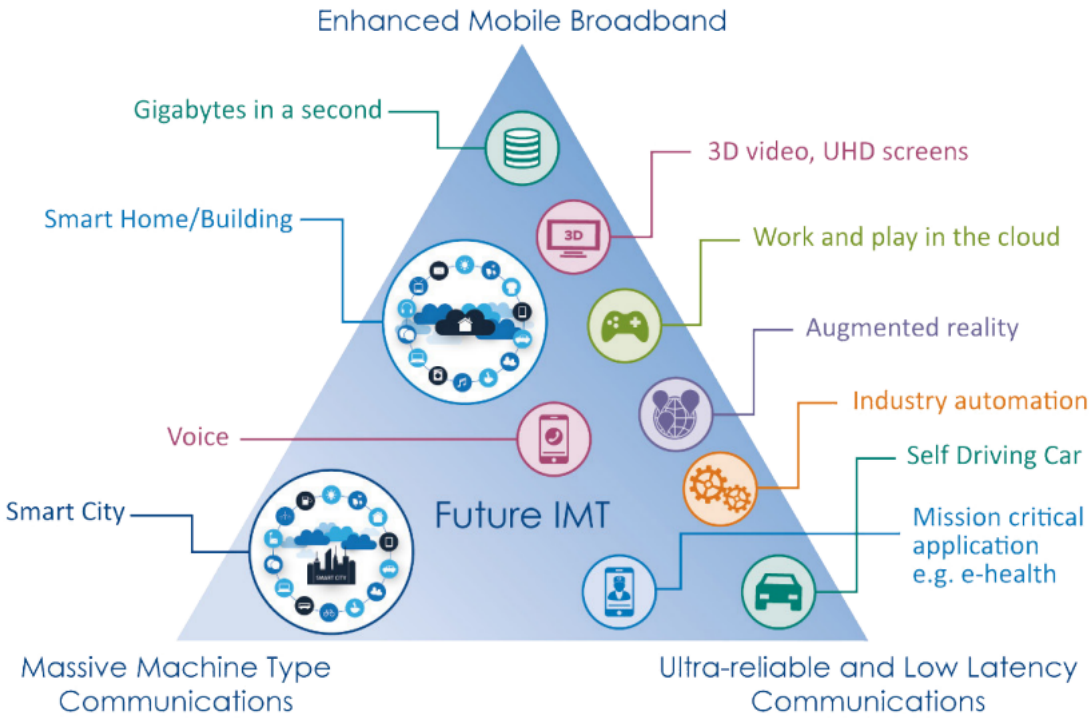

Figura 2.1: Cenários de uso do 5G (ITU, 2018)

Com relação à arquitetura, o *3rd Generation Partnership Project* (3GPP) estabeleceu os principais componentes de sistemas 5G, conforme indicado na Figura 2.2. De acordo com 3GPP (2022), o 5G *System* (5GS) utiliza elementos como o equipamento do usuário (UE), a rede de acesso de rádio (NG-RAN) e o 5G *Core* (5GC).

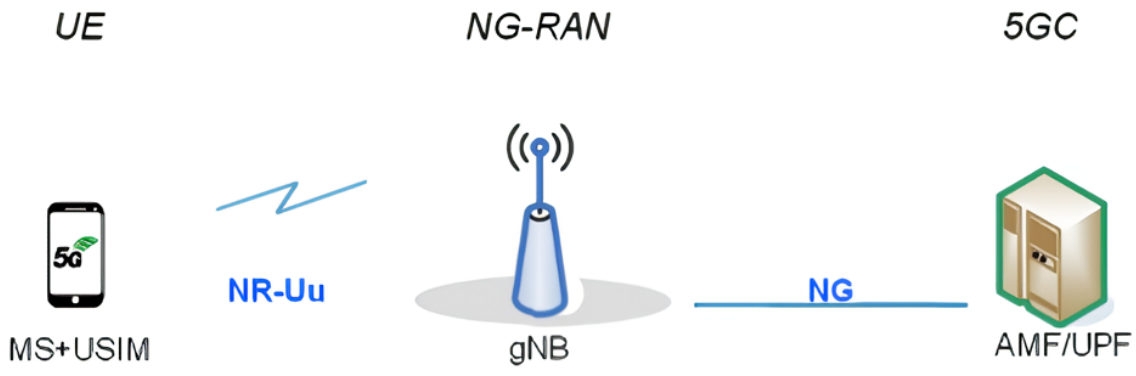

Figura 2.2: Visão geral do 5GS (3GPP, 2022)

O 5GS possui uma arquitetura orientada a serviços (SBA), o que significa que os elementos da arquitetura são definidos em termos de funções de rede (NFs) em vez de entidades de rede. Assim, qualquer NF disponibiliza serviços para outros NFs ou usuários que estejam autorizados a usarem tais serviços, o que garante modularidade e reusabilidade do sistema (3GPP, 2022).

Já o 5G *Core* é representado por diversas entidades, executadas através das NFs e bem definidas quanto ao seu escopo. Como o escopo deste trabalho são as funções relacionadas à autenticação e ao controle de acesso, destacam-se as entidades AMF, responsável por controlar o acesso do UE e do NG-RAN, e o UPF, que manipula os dados do usuário. Como mostrado na Figura 2.3, há outras entidades e também pontos de referência entre o acesso e o *core*, os quais são denominados "NG" e são constituídos de várias interfaces (como N2 e N3) (3GPP, 2022).

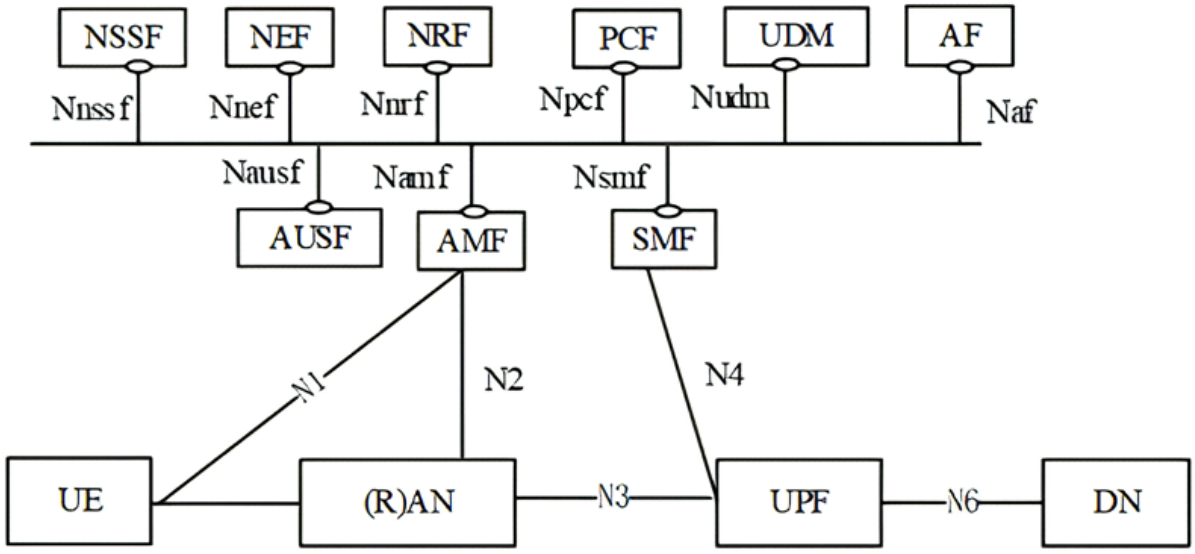

Figura 2.3: Arquitetura do 5GS (3GPP, 2022)

Em termos de autenticação, esta etapa no 5G foi projetada para ser mais segura e eficiente do que nas gerações anteriores, utilizando novos protocolos que garantem a identidade do usuário e protegem as comunicações. De acordo com Edris, Aiash e Loo (2022), um dos principais métodos de autenticação nesse contexto é uma adição ao EAP[1], o EAP-AKA' (*Extensible Authentication Protocol – Authentication and Key Agreement Prime*),

[1] *Extensible Authentication Protocol* (EAP): *Framework* para prover diferentes métodos de autenticação

que está diretamente relacionado ao *Universal Subscriber's Identity Module* (USIM), o chip do dispositivo.

Como apresentado por Edris, Aiash e Loo (2022), quando um usuário tenta acessar a rede 5G, seu dispositivo se comunica com a estação base (gNB), que encaminha a solicitação para a função de autenticação da rede (SEAF). Esse pedido é então direcionado ao AUSF (*Authentication Server Function*), que trabalha em conjunto com o UDM (*Unified Data Management*), onde as credenciais do usuário estão armazenadas. O AUSF gera um desafio de autenticação, enviando um número aleatório (RAND) e um valor de autenticação (AUTN) para o dispositivo.

Neste momento, surge a necessidade de atributos do SIM ou USIM, que contém uma chave secreta única, denominada "chave k", compartilhada apenas entre o *chip* do usuário e a operadora. Usando tal chave, o SIM processa o desafio recebido e gera uma resposta criptográfica. Essa resposta é então enviada de volta à rede, onde o servidor compara com o valor esperado. Se tudo estiver correto, a autenticação é bem-sucedida e uma chave de sessão, também chamada de *master session key* (MSK), é gerada, permitindo que o dispositivo acesse a rede de forma segura (EDRIS; AIASH; LOO, 2022).

O uso do EAP-AKA' no 5G traz benefícios importantes. Diferente das versões anteriores, ele melhora a privacidade do usuário, ao evitar que sua identidade permanente ou *Subscriber's Permanent Identifier* (SUPI) seja transmitida em texto claro, pois há um processo de criptografia, reduzindo, assim, os riscos de rastreamento. Além disso, ele gera chaves mais fortes, tornando a comunicação mais segura contra ataques de interceptação e falsificação de identidade.

2.2 SDN

Software defined networking (SDN), ou rede definida por *software*, é caracterizada por possuir um sistema central de controle que coordena todos os elementos de comutação da rede a partir de uma interface programável (GUEDES et al., 2014). Partindo dessa definição, as SDNs, por fazerem uma divisão entre o plano de controle e o plano de dados, trazem um maior controle das redes de computadores por meio da programação, o que gera vários benefícios (XIA et al., 2015). Tais benefícios variam desde o aprimoramento

no desempenho até a inovação na arquitetura e operações das redes (XIA et al., 2015).

Em relação à sua estrutura, uma SDN segue o modelo de 3 camadas da Figura 2.4. De acordo com Xia et al. (2015), cada camada possui uma funcionalidade específica:

- A camada de infraestrutura (*Infrastructure Layer*) corresponde aos dispositivos comutadores (exemplo, *switches* e roteadores), os quais coletam informações do estado da rede e as enviam para os controladores. Além disso, esses dispositivos também encaminham os pacotes da rede conforme as regras estabelecidadas pelos controladores.

- A camada de aplicação (*Application Layer*) contém as aplicações SDN que serão utilizadas para acessar e controlar os dispositivos de *switching*. Isso é possível pois a camada de controle oferece uma plataforma programável para um usuário da rede realizar essas ações.

- A camada de controle (*Control Layer*) realiza a conexão entre a camada de aplicação e a camada de infraestrutura. Essa camada provê funções de acesso dos controladores aos dispositivos de switching, e para a camada de aplicação, ela oferece pontos de acesso ao serviço por meio de uma *Application Programming Interface* (API). Por meio dessa API, são recebidas as informações do estado de redes que foram geradas pelos dispositivos de switching, e as aplicações SDN tomam e encaminham as decisões de acordo com essas informações, também utilizando a API.

Para tratar de cenários com necessidades distintas, conforme explica Gonçalves, Bittencourt e Madeira (2022), uma solução é a utilização de redes virtuais, também chamadas de fatias de rede ou *slices*, que estão em um mesmo meio físico. Há vantagens em fazer essa abordagem, pois cada *slice* pode oferecer características próprias, como banda dedicada e latência, exigidos pelo usuário ou, no caso do 5G, os requisitos mínimos para o funcionamento adequado dos seus serviços (eMBB, URLLC e mMtC).

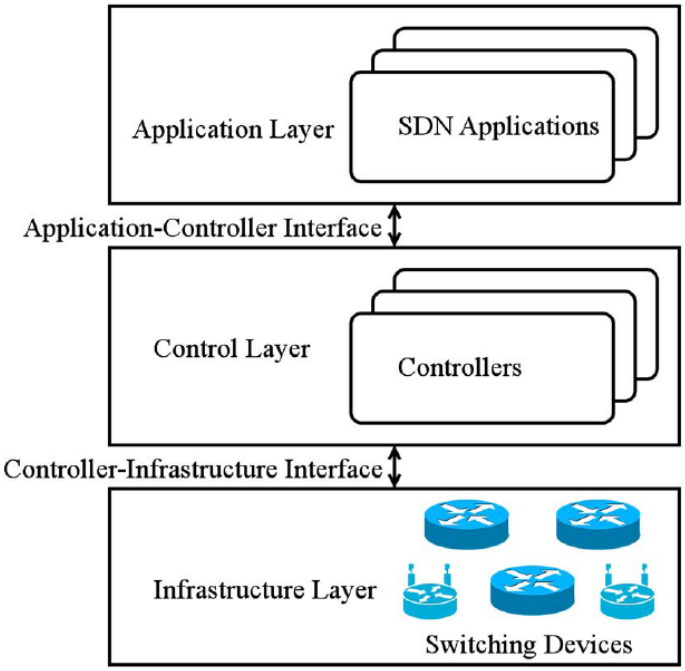

Figura 2.4: Modelo de referência da arquitetura de uma SDN (XIA et al., 2015)

2.3 *Device FingerPrint*

Device Fingerprint é uma forma de reduzir a chance de ataques e tentativas de falsificação, pois atribui a um dispositivo uma assinatura de acordo com suas características (XU et al., 2016). O termo impressão digital (*fingerprint*) se aplica, já que cada dispositivo tem um conjunto de atributos únicos para sua correta identificação.

Como exemplo para esta técnica, é possível listar uma série de atributos relacionados a um *smartphone* 5G. Conforme a Tabela 2.1, vê-se uma lista de tuplas atributo-valor que tornam único o dispositivo em questão. Caso um ou mais atributos sejam modificados, é possível, utilizando-se de técnicas de *device fingerprint*, identificar o impacto na assinatura daquele dispositivo e alterar sua confiança associada.

Para ser eficiente, essa ferramenta de identificação necessita ser menos suscetível à falsificação e deve permanecer estável quando ocorrerem mudanças no sistema (XU et al., 2016). Assim, com o *device fingerprint*, quando um invasor acessar um recurso, ainda que consiga copiar o endereço *Media Access Control* (MAC) ou mesmo roubar o chip de autenticação do dispositivo (para o caso de redes 5G), ele poderá ser facilmente identificado como um usuário ilegítimo, visto que as características do dispositivo se alteraram.

Tabela 2.1: Exemplo de atributos para *Device Fingerprint* de um celular 5G fictício.

Atributo	**Valor**
IMEI/SUPI	356938035643809
MAC (Wi-Fi)	00:1A:2B:3C:4D:5E
MAC (Bluetooth)	00:1B:44:11:3A:B7
Modelo do Dispositivo	Samsung Galaxy S23 Ultra
SO	Android 14
Kernel	5.15.104-perf-g9c5b23d
Chipset	Qualcomm Snapdragon 8 Gen 2
Modem 5G	Qualcomm X70
Tipo de Rede	5G NR (New Radio) SA
Operadora	Claro Brasil
Frequências Suportadas	n78 (3.5 GHz), n41 (2.5 GHz), n28 (700 MHz)
Sensores Ativos	Acelerômetro, Giroscópio, Proximidade, Barômetro
Timezone/Localização	UTC-3 (Brasília), Lat: -23.5505, Long: -46.6333
Último IP Público	203.0.113.84

2.4 Ataques DoS

Para manter a estabilidade na distribuição dos seus serviços, redes 5G devem se manter operantes na maior parte do tempo, porém, há casos de interferências propositais para tentar diminuir ou mesmo encerrar o seu funcionamento apropriado. Um exemplo disso é o ataque *Denial of Service* (DoS) ou negação de serviço, em que um usuário invasor realiza, de forma direta ou indireta, o esgotamento dos recursos de um sistema por aumento do tráfego da rede, fazendo com que haja a diminuição na disponibilidade dos serviços oferecidos pelo sistema (ZLOMISLIć; FERTALJ; SRUK, 2014).

De acordo com Zlomislić, Fertalj e Sruk (2014), os ataques DoS podem ser divididos nas seguintes categorias:

- ataques *flood*: há uma grande quantidade de requisições de comunicação para o alvo do ataque, e tais requisições podem até mesmo serem legítimas, mas ainda deixam o alvo indisponível;

- ataques de amplificação: ocorre redirecionamento de respostas amplificadas, maiores que o normal, para a vítima do ataque, a fim de realizar uma sobrecarga no alvo e, por consequência, exaustão dos recursos;

- exploração de vulnerabilidades em protocolos: por mais seguros e bem desenvolvidos protocolos possam ser, ainda podem apresentar falhas ou se comportar fora do esperado, e nesses casos, um atacante pode aproveitar para realizar uma tentativa de negação de serviço;

- pacotes malformados: implementações de *software* podem apresentar problemas de segurança e confiabilidade, e um invasor pode se aproveitar disso, enviando pacotes maliciosos para eles.

Esses ataques afetam diretamente a qualidade e a continuidade dos serviços oferecidos, gerando consequências tanto para os usuários quanto para as entidades e empresas envolvidas.

Um ataque DoS pode comprometer a Qualidade de Serviço (QoS) de um *slice* de rede. No ambiente 5G, cada *slice* é desenvolvido para atender a necessidades específicas de diferentes serviços, como eMBB, URLLC e mMTC. Um atacante com o uso de DoS pode, por exemplo, saturar a largura de banda, tornando os serviços mais lentos ou até mesmo inacessíveis (ZHANG et al., 2016). Além disso, pode aumentar a latência, prejudicando aplicações sensíveis ao tempo, como sistemas de veículos autônomos e cirurgias remotas, e reduzir a confiabilidade, afetando serviços essenciais que requerem alta disponibilidade, como as comunicações de emergência.

Outro impacto significativo de um ataque DoS nesse cenário é o efeito cascata que ele pode gerar em outros recursos da rede. Embora a segmentação dos *slices* de rede seja projetada para garantir isolamento, esse tipo de ataque pode consumir recursos compartilhados da infraestrutura, como a capacidade de processamento e armazenamento em nuvem, e até derrubar funções críticas de controle da rede, como autenticação e roteamento, afetando múltiplos *slices* simultaneamente (WANG et al., 2018).

2.5 Métodos de Controle de Acesso

Em conjunto com a correta autenticação de um usuário (mais especificamente no caso de redes 5G, autenticação do dispositivo), é necessário também um meio de realizar a sua autorização ao acesso de algum recurso. Isso pode ser feito com estratégias distintas,

variando de método para método conforme a característica avaliada.

2.5.1 *Role Based Access Control* (RBAC)

Role Based Access Control (RBAC) é um modelo desenvolvido na década de 70, em que o usuário recebe um papel, o qual pode ser redistribuído a qualquer momento, e assim, caso necessário, a permissão de acesso é alterada de forma simples (GOULART; DANTAS, 2018). As permissões para acessar um determinado recurso, portanto, em vez de estarem relacionadas com o identificador de um sujeito, estão intrinsecamente ligadas ao papel atribuído (YUAN; TONG, 2005).

De acordo com Oyeyinka et al. (2018), existem três regras a serem seguidas por esse método:

- Atribuição do papel: a menos que o usuário tenha recebido um papel, ele não pode acessar o recurso solicitado.
- Autorização do papel: um usuário só pode receber um papel se ele for autorizado a recebê-lo.
- Autorização da permissão: o acesso só é permitido no caso de a permissão ser concedida ao papel do usuário.

É considerado um método que provê uma boa escabilidade, visto que, como não é necessário atribuir permissões a usuários individuais, mas sim a papéis, os quais podem envolver vários usuários ao mesmo tempo, gerando menos *overhead* na administração do sistema (YUAN; TONG, 2005).

2.5.2 *Attribute-Based Access Control* (ABAC)

No *Attribute-Based Access Control* (ABAC), o acesso é avaliado a partir de uma análise dos atributos das entidades envolvidas nessa operação, permitindo ou negando uma solicitação dependendo do que foi considerado (HU et al., 2015). De acordo com Yuan e Tong (2005), os atributos podem ser classificados de diferentes formas, conforme a entidade utilizada:

- Atributos do sujeito: são toda a identidade do usuário, como seu identificador, nome ou até mesmo a organização a que pertence.

- Atributos do recurso: são as características do recurso que vai ser acessado pelo sujeito, por exemplo, informações da qualidade do serviço ou a quem pertence o recurso

- Atributos do ambiente: englobam informações do contexto em que o sistema está inserido, tais como intervalo de tempo, nível de segurança da rede e a atividade de possíveis invasores.

Assim, um ABAC pega uma regra na política do sistema e verifica se os atributos do sujeito, do recurso e do ambiente são compatíveis, em caso positivo, permite o acesso, caso contrário, o acesso é negado (YUAN; TONG, 2005). É, portanto, um modelo bem flexível, já que, para configurar se uma requisição deve ser permitida ou não, basta mudar os atributos das entidades envolvidas, sem necessidade de mudanças nas relações entre sujeito e recurso (HU et al., 2015).

2.6 *Zero-Trust*

O *Zero-Trust* baseia-se em que, por padrão, nenhum usuário é confiável, independente da sua localização, desconsiderando os princípios da segurança de perímetro. A confiança do sistema é concedida para determinada requisição/transação a partir de uma autenticação e autorização do usuário e, em função de ser algo que deve ser sempre executado, faz com que o sistema possua o poder de ajustar o nível de segurança de acordo com cada recurso (TEERAKANOK; UEHARA; INOMATA, 2021).

2.6.1 Princípios do *Zero-Trust*

O Instituto Nacional de Padrões e Tecnologia (NIST), do departamento de comércio dos Estados Unidos, estabeleceu princípios fundamentais para o *Zero-Trust* (ROSE et al., 2020):

- todos os dados e serviços computacionais são considerados recursos;

- toda comunicação é feita independentemente da localização da rede;
- o acesso aos recursos é feita de acordo com a sessão e também de acordo com o recurso escolhido, ou seja, a confiança do usuário é avaliada e, caso seja autorizado, garante acesso a um único recurso com o mínimo de privilégios possíveis;
- o acesso aos recursos depende da política dinâmica, isto é, a organização define o que são os recursos, quem são os usuários e o nível de privilégio desses usuários;
- a organização monitora e mede a integridade e segurança de todos os seus ativos, partindo da ideia de que nenhum ativo é confiável;
- a autenticação e autorização dos recursos são dinâmicas e devem ser executadas antes que o acesso ao recurso seja permitido;
- a organização deve coletar todas as informações possíveis a respeito dos seus ativos, da infraestrutura e comunicações da rede, com o intuito de aprimorar a criação e execução das políticas de acesso aos recursos.

2.6.2 Arquitetura *Zero-Trust*

A arquitetura *Zero-Trust* pode ser implementada seguindo os componentes lógicos da Figura 2.5. Segundo Teerakanok, Uehara e Inomata (2021), Rose et al. (2020), os cinco principais componentes da *Zero-Trust Architecture* (ZTA) são: sujeito, recurso, o ponto de decisão de políticas (PDP), que é dividido em mecanismo de política (PE) e administração de política (PA); o ponto de execução de políticas (PEP) e, por fim, os complementos. Fica claro que a implementação da ZTA muito se correlaciona com os modelos de controle de acesso expostos anteriormente. Desta forma, veremos os detalhes de cada componente dessa arquitetura.

O sujeito é qualquer usuário ou dispositivo que solicita acesso a um recurso, enquanto que o recurso em si é qualquer recurso da organização cujo acesso está sendo solicitado pelo sujeito (TEERAKANOK; UEHARA; INOMATA, 2021).

O PDP define quem pode ou não acessar um determinado recurso, além de decidir se a comunicação do sujeito com o recurso deve ser estabelecida ou cortada. Em relação

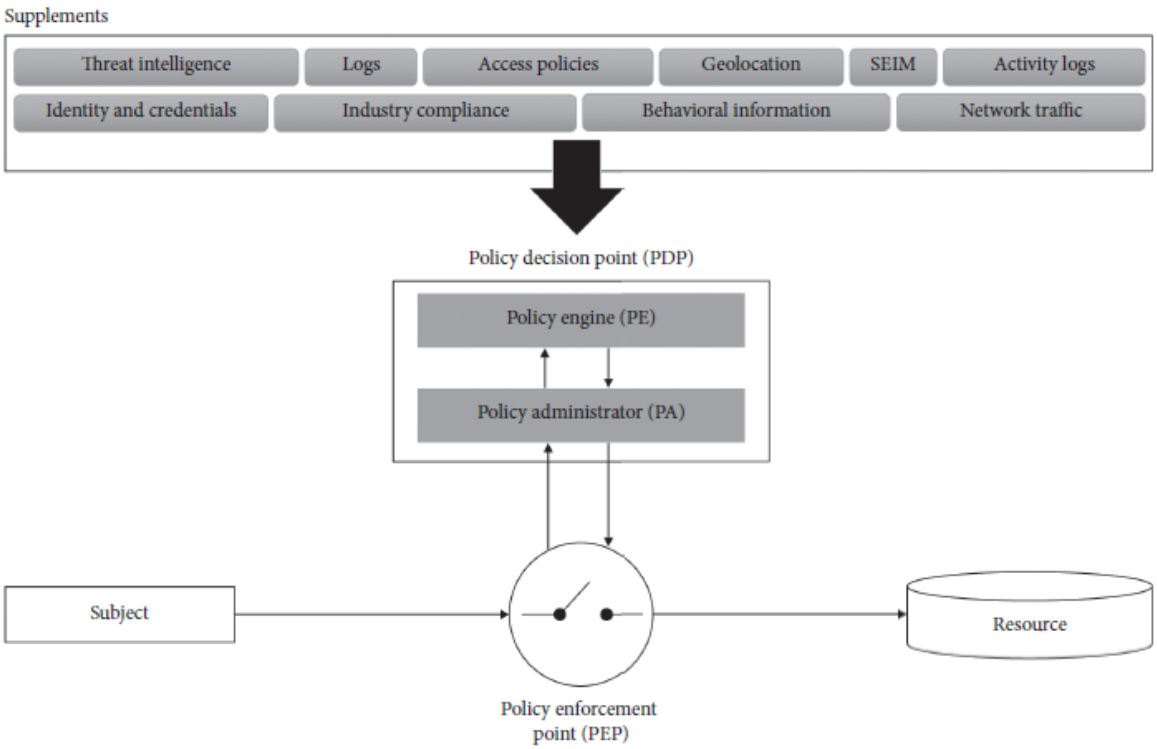

Figura 2.5: Componentes lógicos da ZTA (TEERAKANOK; UEHARA; INOMATA, 2021)

aos componentes específicos do PDP, o PE realiza o procedimento de tomada de decisão e o PA é o que faz o controle da comunicação (TEERAKANOK; UEHARA; INOMATA, 2021).

O PEP recebe o pedido de acesso ao recurso do sujeito e o envia ao PDP. Após o PDP tomar a decisão do que fazer com esse pedido de acesso, ele solicita que o PEP estabeleça ou corte a comunicação do sujeito com o recurso. Portanto, o PEP é a porta de acesso que faz o papel de ligar o sujeito aos recursos (TEERAKANOK; UEHARA; INOMATA, 2021).

Por fim, os complementos são os componentes que trazem informações para o PE, a fim de que ele tome mais decisões corretas, algo que pode aumentar a segurança do sistema (TEERAKANOK; UEHARA; INOMATA, 2021).

A partir dos conceitos fundamentais apresentados, é possível seguir adiante com a correlação de todas as tecnologias no incremento à segurança do acesso a recursos no ambiente 5G. Fica claro que o ambiente 5G é composto de aplicações, também denominadas recursos, sobre fatias de rede, as quais trazem benefícios, como determinado valor de latência, ao dispositivo que as acessam. Por isso, e como foco deste trabalho, é interes-

sante investigar a aplicação de modelos de controle de acesso e identificação de dispositivo junto à ZTA para a gestão do acesso aos recursos ofertados pelo 5G.

3 Artigos Relacionados

Como forma de complementar a compreensão do leitor sobre o estado da arte dos temas abordados, este capítulo apresenta uma visão geral de artigos que estão relacionados ao tema deste trabalho. A intenção é estabelecer exemplos de abordagens do *Zero-Trust* no ambiente do 5G.

O artigo de Aiello (2022) traz uma fundamentação teórica da arquitetura *Zero-Trust* e cita sua integração nas redes 5G. É comentado que, diferente da segurança baseada em perímetro, o *Zero Trust* traz novos usuários, a rápida adoção de sistemas baseados em nuvem e novos dispositivos IoT. Por fim, conclui que a implementação do *Zero-Trust* é gradual e deve ser feita de acordo com as capacidade de segurança atuais; cita que o paradigma de confiança possui falhas e como o tráfego de rede dentro do *Zero-Trust* não possui confiança por padrão, as organizações devem definir o nível de segurança de cada recurso e fazer a análise do tráfego.

O trabalho de Chen et al. (2020) cita os principais problemas de sistemas de saúde baseados em redes 5G e comenta alguns requisitos necessários desses sistemas, como controle unificado, mecanismos de autenticação escaláveis e capacidade de defesa e segurança distribuídas. Tais desafios podem ser contornados pela utilização do *Zero-Trust* e é proposta uma aplicação com segurança em quatro dimensões, ou seja, utiliza uma ZTA que foca no sujeito, no objeto, no ambiente e no comportamento do sistema de saúde baseado em redes 5G. Então o artigo prossegue para estabelecer a base teórica dessa nova aplicação e realiza testes para verificar sua eficácia.

O artigo de Olsson et al. (2021) faz uma comparação do *Zero-Trust* em contraste com o modelo de segurança baseada em perímetro e comenta da facilidade de integração da ZTA com as redes 5G em função de alguns aspectos dessas redes. Esses aspectos são a identidade digital segura, transporte seguro, política do *framework* e a segurança no monitoramento. Ao final, é comentado os próximos passos da indústria das telecomunicações, dizendo que o *Zero-Trust* tem uma implantação gradual e baseada em decisões metódicas, e conclui que a implementação bem-sucedida dos princípios do ZT requer também a im-

plementação conjunta de processos da segurança da informação, de políticas e de boas práticas nos provedores de serviços de comunicações.

Embora não trate especificamente do 5G, no trabalho de Freitas et al. (2024), os autores trazem uma base teórica de gestão de controle de identidade e acesso, de métodos de autorização e da arquitetura *Zero-Trust*. É proposto, então, fazer uma implementação da ZTA em sistemas *e-health*, pois o uso do *Zero-Trust* ainda é pouco explorado na segurança de aplicações da área da saúde. Para isso, foi desenvolvido um sistema em que o ZT toma uma decisão dos acessos baseando-se nos valores das sensibilidades dos recursos e no nível de confiança calculado do usuário. Assim, foram feitos experimentos em diferentes cenários e conclui-se que o controle de acesso pelo *Zero-Trust* foi eficaz, já que foi possível identificar anomalias e fazer a proteção de recursos mais sensíveis.

Diante dos artigos abordados, pode-se ver uma presença do Zero-Trust como uma forma eficiente para aprimorar a segurança dos sistemas que envolvem redes 5G. Em particular, o trabalho de Olsson et al. (2021) menciona características do 5G que facilitam a integração do ZTA nessas redes, enquanto que o artigo de Freitas et al. (2024) propõe maneiras de implementação e experimentos para fazer teste apropriado do ZT.

Dessa forma, este trabalho traz uma integração do Zero-Trust como forma de proteção das aplicações associadas aos serviços do 5G. Utilizando a ZTA em conjunto com um método de controle de acesso, o trabalho faz uma avaliação se essas aplicações estarão protegidas, por exemplo, de ataques DoS ou possíveis roubos do chip do dispositivo.

4 Desenvolvimento

Neste capítulo são definidos os elementos principais para o desenvolvimento da aplicação que utiliza *Zero-Trust* para acesso aos recursos oferecidos pelos serviços das redes 5G, assim como a forma de avaliar os experimentos realizados. Como forma de organização da apresentação, a Seção 4.1 apresenta a ideia da aplicação a ser implementada; a Seção 4.2 mostra a definição do valor de confiança e das penalidades associadas; já na Seção 4.3 é descrita a modelagem do banco de dados; e, por fim, a Seção 4.4 define as características das fatias e a sensibilidade dos recursos.

4.1 Aplicação ZT-5G

A implementação da ZTA neste trabalho tem como base os componentes definidos por Teerakanok, Uehara e Inomata (2021), Rose et al. (2020), que possuem sua base teórica na Seção 2.6.2. A implementação, de modo geral, seguirá os métodos do trabalho de Freitas et al. (2024). O modelo de controle de acesso utilizado é o ABAC, pois as informações e atributos do dispositivo serão relevantes para a decisão final.

O funcionamento da aplicação se baseará na ideia de que o usuário, com o seu dispositivo, se conectará ao sistema e solicitará acesso aos recursos nas fatias, que seriam as aplicações associadas com cada serviço do 5G, passando pelo *Zero-Trust*. Para fazer a simulação da rede, os recursos são representados como processos ou *threads* e se conectam aos usuários e a ZTA por meio de sockets[2]. A autenticação do dispositivo pelo 5G não será implementada no projeto, porém a aplicação ainda deve receber o número do SUPI, para mostrar que o dispositivo foi devidamente autenticado.

O sistema seguirá um fluxo de acordo com a Figura 4.1. Assim, o PEP tem a função de disparar *threads* para cada requisição. Para tratar o acesso, o PEP inicia o PA do PDP, e de acordo com a decisão recebida, ele abre ou bloqueia ao acesso ao recurso solicitado. O PDP da ZTA analisa os atributos recebidos e valida se o perfil do

[2]Nós na rede compostos de endereço IP e porta utilizados para diferenciar processos distintos

usuário se manteve ou alterou de um acesso a outro. Na Seção 4.2 são definidas algumas penalidades de acordo com as características do acesso, além do cálculo da confiança. O *Policy Information Point* (PIP) tem o papel de fazer a conexão com o banco de dados, cuja modelagem é feita na Seção 4.3, além de fazer as ações no banco necessárias para a tomada de decisão do PDP, funcionando como um dos complementos da ZTA.

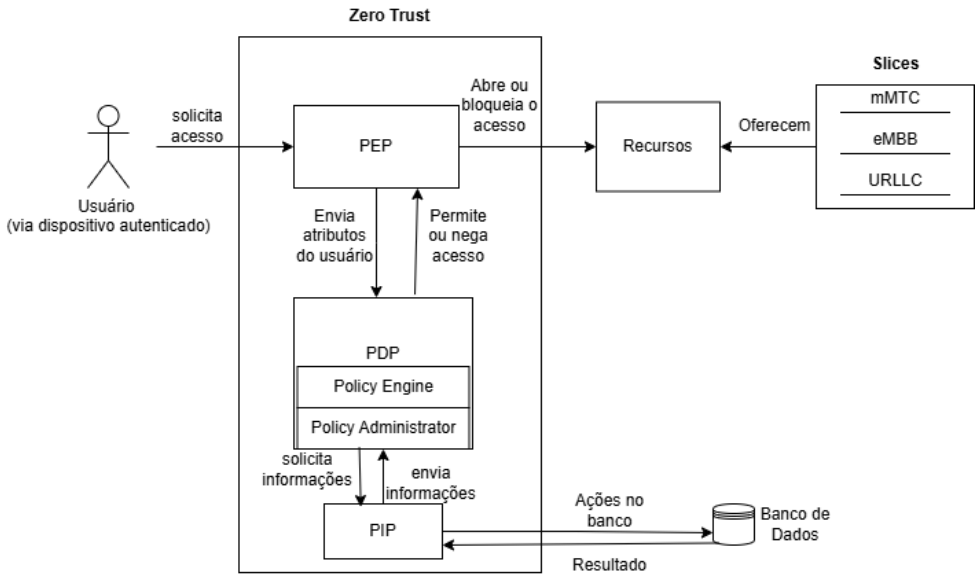

Figura 4.1: Fluxo de execução do sistema

Ao final, o PDP realiza o cruzamento de informações da confiança que foi calculada com a sensibilidade dos recursos, e, assim, o acesso é permitido ou negado, como indicado na Figura 4.2, que é a decisão a ser enviada ao PEP.

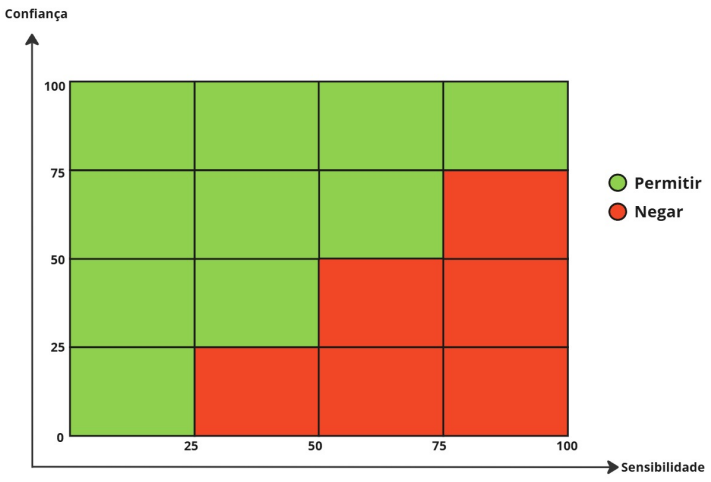

Figura 4.2: Diagrama de Permissões Confiança x Sensibilidade

A implementação utiliza a linguagem de programação Python[3], em função de suas várias bibliotecas que facilitam a criação de aplicações em redes, portanto muito útil para a proposta da aplicação. O código fonte do trabalho pode ser obtido em um repositório público do Github[4].

4.2 Nível de Confiança

Como citado na Seção 2.6, no *Zero-Trust* cada requisição possui uma confiança associada, a fim de que o sistema consiga decidir se essa requisição poderá ser feita ou não. Cabe então definir quais são esses níveis ou graus de confiança na aplicação.

Diante disso, foi estabelecido que o grau de confiança de uma requisição é um valor numérico de 0 a 100, e também possui penalidades associadas, ou seja, valores que diminuem a confiança de acordo com características específicas do usuário e do recurso que ele pretende acessar. Além disso, de acordo com o trabalho de Freitas et al. (2024), pode-se dividir a análise da confiança mediante as seguintes perspectivas e penalizações:

• **Confiança associada ao usuário** - Mede a confiança a partir da interação do usuário com o sistema. As penalizações nesse caso podem ser:

- P1 - Alterações significativas na localização do usuário considerando acessos recentes, ou seja, o usuário está acessando em locais muito distantes num curto período de tempo.

• **Confiança associada ao dispostivo** - Calcula a confiança a partir do dispositivo utilizado para acessar o sistema. As penalizações nesse caso podem ser:

- P2 - É a primeira vez que o dispositivo está sendo utilizado para acesso.
- P3 - O dispositivo tem características muito distintas do que o usual, ou seja, sua impressão digital foi modificada.

• **Confiança associada ao histórico** - Mede a confiança avaliando os acessos anteriores do usuário. A penalização nesse caso pode ser:

[3]https://www.python.org/
[4]https://github.com/vdapjf/Zero-Trust-5G

- P4: Frequência de acesso à recursos altamente sensíveis
- P5: Frequência de acesso no último minuto.
- P6: Múltiplas requisições negadas.

Freitas et al. (2024) também propõe a Equação 4.1, que descreve que a confiança de uma perspectiva é igual a 100, subtraindo o somatório de todas as penalidades, associadas a essa perspectiva, que foram identificadas.

$$C_p = 100 - \left(\sum_{n=1}^{N} A_n \right), \text{ onde } A_n \in [0, 100] \tag{4.1}$$

Na qual N é o número de fatores que foram avaliados, A_n é a avaliação de penalidade para o fator n e C_p é o valor da confiança na perspectiva p (contexto, dispositivo e histórico), definida no intervalo $C_p \in [0, 100]$. O valor da confiança final é dado pela Equação 4.2 (FREITAS et al., 2024).

$$C_f = (\sqrt{C_c \cdot C_d})P, \text{ onde P } = \begin{cases} \frac{1}{100} C_h, C_h > 0 \\ 0.1, C_h = 0 \end{cases} \tag{4.2}$$

Na qual C_h é a confiança com base no histórico, P é a normalização do valor de C_h no intervalo [0.01, 1], C_d é a confiança obtida a partir da avaliação do dispositivo, C_c é a confiança com base no contexto e C_f é o resultado final da confiança.

4.3 Banco de Dados

Com a finalidade de armazenar os dados dos acessos na aplicação, foi utilizado o banco de dados relacional PostgreSQL[5]. No código Python, a conexão do PIP do Zero-Trust com o banco foi feita utilizando a biblioteca psycopg2[6].

A Figura 4.3 representa a modelagem de todo o banco de dados, que possui 5 entidades. A tabela *Usuário* tem a função de guardar o nome do dono de cada dispositivo. A tabela *Dispositivo* contém as informações do dispositivo que realizará o acesso no sistema, que são o número do ID do chip (o número SUPI gerado pela autenticação no 5G),

[5]https://www.postgresql.org/
[6]https://pypi.org/project/psycopg2/

a chaveK e a *master session key* da autenticação, o endereço MAC, o *device fingeprint* e o ID do usuário ao qual ele pertence.

A tabela *Slice* representa as fatias da rede, com suas informações de IP, porta, largura de banda e latência ou atraso. Já a tabela *RecursoSlice* indica os recursos associados a cada um dessas fatias, com características do nome do recurso, o id do *slice* ao qual pertence e o valor da sensibilidade definida para cada um.

No final, há a tabela *Acesso*, que denota todas as características de um acesso a um recurso, que são a data que o acesso aconteceu, sua localização (em termos de latitude e longitude), o valor da confiança, o resultado emitido pelo Zero-Trust (se acesso foi permitido ou negado) e ids do dispositivo e do recurso ao qual o acesso está relacionado.

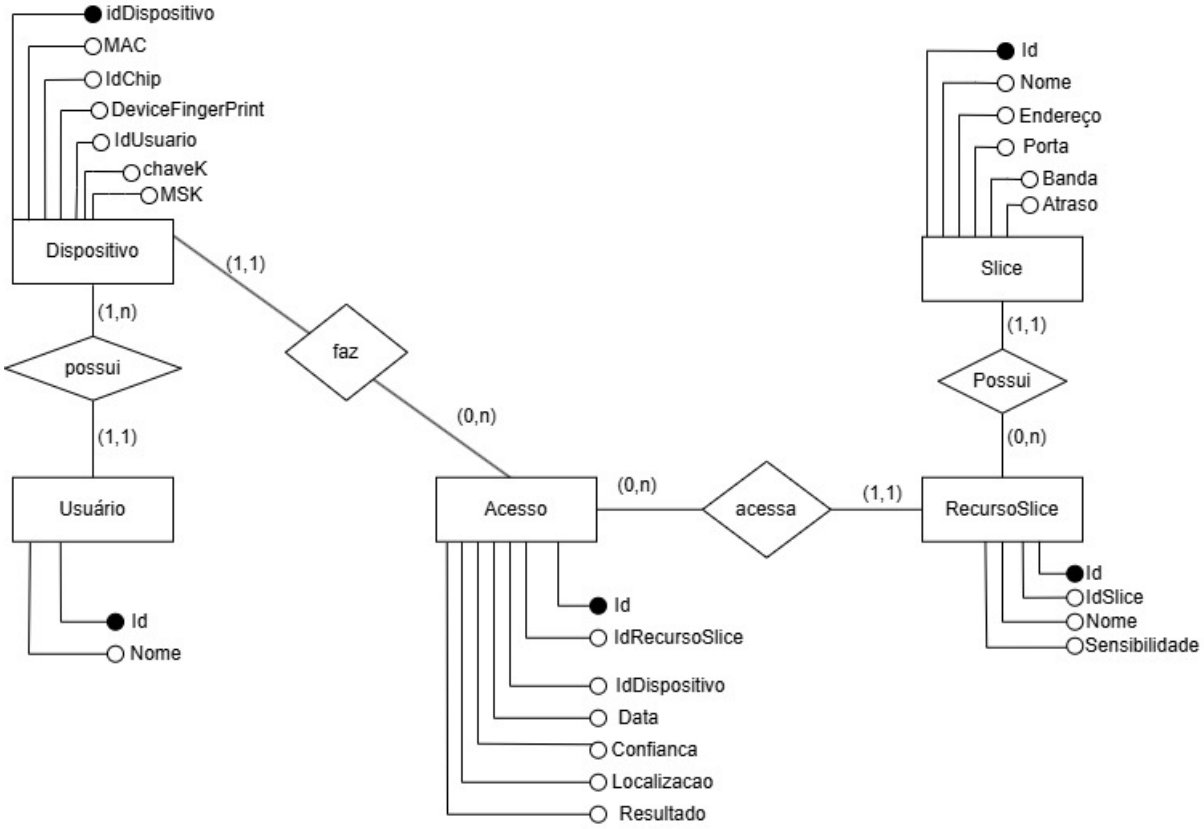

Figura 4.3: Diagrama entidade-relacionamento do banco de dados

4.4 Fatias da Rede e Sensibilidade das Aplicações

O sistema proposto contém três fatias da rede que representam os serviços oferecidos pelo 5G, descritos na Seção 2.1. Elas possuem as características definidas na Tabela 4.1, junto

com seus valores mínimos de confiança, que indicam o momento em que um dispositivo é permitido a acessar as aplicações em cada fatia. Para a proposta deste trabalho, esses valores de confiança foram ordenados de acordo com a latência exigida por cada um dos serviços do 5G e a banda fornecida foi a mesma para todas as fatias.

Como já indicado na Figura 4.2, para fazer a permissão ou não do acesso, é necessário fazer o cruzamento das informações da confiança e de sensibilidade. Tal sensibilidade foi definida como um valor arbitrário próximo ao valor mínimo de confiança de cada fatia.

Características dos *Slices*			
Slice	**Latência (ms)**	**Valor mínimo de Confiança**	**Sensibilidade das aplicações**
mMTC	50	25	30
eMBB	4	50	60
URLLC	1	75	90

Tabela 4.1: Tabela de características das fatias da rede

Para cada uma das fatias ofertadas na rede 5G, há aplicações e características associadas. Observando a Tabela 4.1, as aplicações associadas ao *Massive Machine Type Communications* (mMTC) possuem menor necessidade de latência, exigindo um valor de confiança e de sensibilidade mais baixos. Em relação às aplicações da fatia do tipo *Enhanced Mobile Broadband* (eMBB), têm latência até 4 ms. As aplicações de maior sensibilidade, associadas à fatia do *Ultra-Reliable Low Latency Communication* (URLLC), possuem latência muito baixa (até 1 ms), oferecendo, também um conceito relacionado à alta disponibilidade no acesso, referente ao termo "ultra confiança" (*ultra-reliable*).

5 Experimentos e Resultados

Neste capítulo são apresentados os experimentos e os resultados obtidos a partir da proposta apresentada no Capítulo 4, além de indicar conclusões a respeito das observações realizadas.

A instância foi construída manualmente e segue o formato da Figura 5.1, na qual é informado ao Zero-Trust as características do acesso do usuário, que são o tipo da ação (login ou acesso), o registro (que corresponde ao número do chip de autenticação do dispositivo), a sua localização (latitude e longitude), o endereço MAC, o valor *hash* da impressão digital do dispositivo utilizado e o horário em que aconteceu a ação. Para o caso de ação de login, o usuário informa a chave k e a *master session key* (MSK), para indicar que o dispositivo foi corretamente autenticado pelo 5G. Já para os acessos, que são a maior parte da instância, é necessário informar o nome da fatia e o nome da aplicação a ser acessada.


```
[
    {
        "TYPE": "LOGIN",
        "REGISTRY": "262013564857956",
        "K_KEY": "qjT7ApUYCM9p",
        "MSK": "98efef220b4e62a8ed2e77e25b4f6fbb17d4e948",
        "LATITUDE": "-21.7866751",
        "LONGITUDE": "-43.3688584",
        "MAC": "CE-F3-FD-BB-C6-F6",
        "DFP": "508481ff5e8d98e9c0c377abf57d96e24ed6c204",
        "TIME": "2024-02-01 15:35:19.047062"
    },
    {
        "TYPE": "ACCESS",
        "SLICE": "mMTC",
        "SLICE_RESOURCE": "Sistemas IoT",
        "REGISTRY": "262013564857956",
        "LATITUDE": "-21.7866751",
        "LONGITUDE": "-43.3688584",
        "MAC": "CE-F3-FD-BB-C6-F6",
        "DFP": "508481ff5e8d98e9c0c377abf57d96e24ed6c204",
        "TIME": "2024-02-01 15:36:19.047062"
    }
]
```


Figura 5.1: Exemplo de uma instância de acesso

5.1 Cenário 1: Uso Normal

Este cenário visa descrever uma situação normal de uso do sistema, ou seja, uma rotina diária do usuário que deseja acessar os recursos do 5G. Como cada usuário tem sua particularidade, foi estabelecido um procedimento padrão, que pode ser visto na Figura 5.2 que está num intervalo de tempo de 100 minutos.

Primeiramente, o usuário começa a acessar recursos do slice correspondente ao mMTC, pois possuem sensibilidades mais baixas e, portanto, não necessitam de uma confiança elevada. Após uma quantidade de acessos, sua confiança supera o valor de 50, e o usuário passa a poder acessar recursos do eMBB, logo ele tem a opção de também acessar o eMBB ou continuar acessando o mMTC. O valor da confiança aumenta até ultrapassar 75, assim o usuário consegue acessar o uRLLC, e a confiança se estabiliza.

Em dado momento, o usuário decide acessar recursos do uRLLC com uma certa frequência, o que, por sua vez, passa a acionar a penalidade P4 da Seção 4.2. Nesse caso, seu nível de confiança cai momentaneamente e volta a subir, o que pode ser visto no gráfico pelas quedas repentinas na confiança. Depois de alguns minutos, novamente o usuário acessa o uRLLC, e o seu valor de confiança cai, passa a subir de novo e se estabiliza. Dessa forma, ele é permitido pelo *Zero-Trust* a acessar todos os recursos, desde que não haja quebra nas penalidades impostas pela aplicação, o que vai ocorrer nos cenários seguintes.

5.2 Cenário 2: Roubo do Chip

O caso deste cenário tem como intenção mostrar a situação em que o chip do dispositivo utilizado pelo usuário foi, de alguma maneira, roubado por um invasor. Isso pode ocorrer de formas variadas, tais como falsificação na identidade para se obter cartão SIM igual ao original com a operadora ou roubo do próprio dispositivo para fazer a remoção do chip.

Assim, como nesse caso o chip será o mesmo, são necessárias avaliações nas outras características do dispositivo para avaliar que o usuário é, na realidade, outra pessoa. Uma vez confirmado, seu acesso a recursos mais importantes da rede deve ser restringido.

Para representar essa situação, na Figura 5.3, tem-se que os primeiros 100 acessos são os mesmos do cenário de uso normal. A situação se altera após os 100 minutos de uso

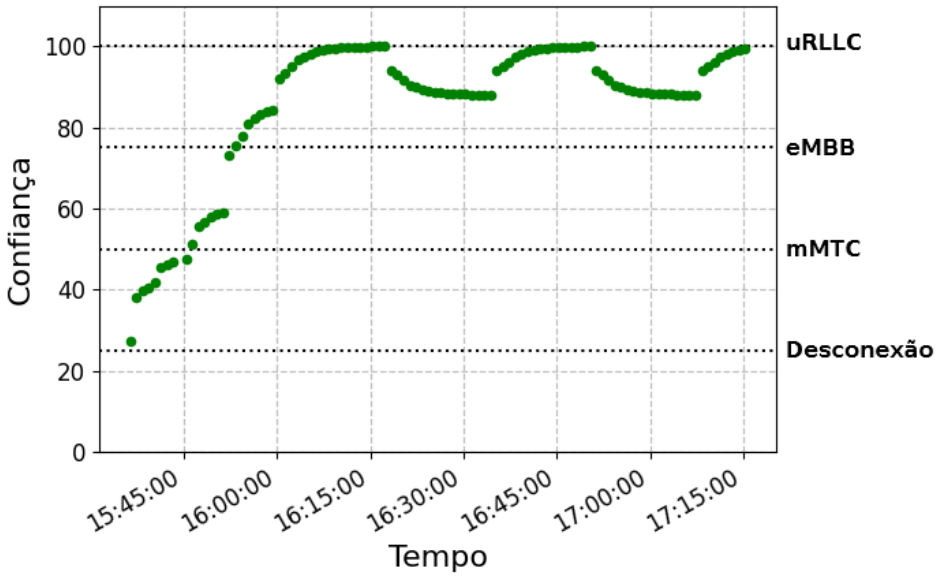

Figura 5.2: Gráfico da Confiança ao longo do tempo de acesso - Cenário 1

do sistema, pois a partir desse momento, os acessos passam a ser feitos por um invasor, cujo dispositivo, embora tenha o mesmo chip e, logo, número SUPI idêntico aos acessos anteriores, tem um *device fingerprint* diferente, indicando que o usuário, a partir desse momento, é, de fato, um atacante.

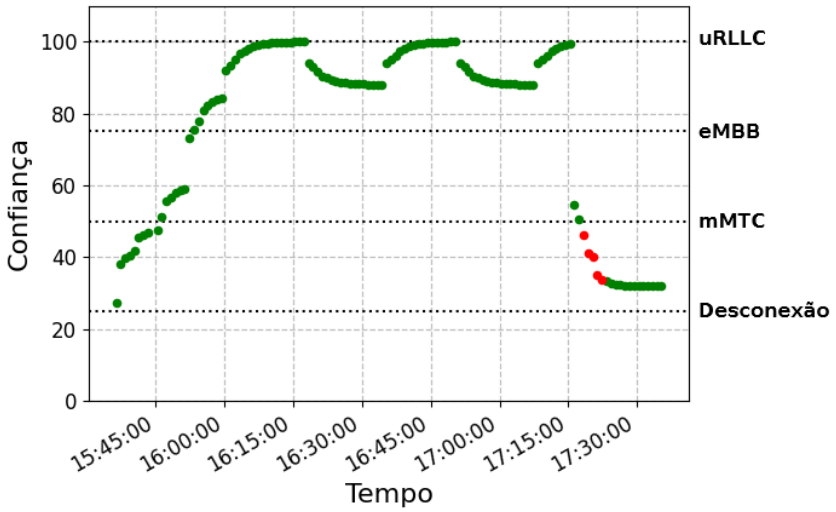

Figura 5.3: Gráfico da Confiança ao longo do tempo de acesso - Cenário 2

Imediatamente ao verificar que o *fingerprint* não é mesmo dos acessos anteriores, o Zero-Trust penaliza a confiança, já que o dispositivo quebra a penalidade P3 da Seção

4.2, e isso pode ser visto no gráfico pela grande queda no valor da confiança. À medida que o atacante acessa recursos dos *slices*, a sua confiança continua caindo vertiginosamente.

Em certo momento, é realizada a tentativa de acesso a recursos do eMBB, porém, seu acesso é negado por se encontrar numa faixa abaixo do que é permitido por essa fatia. Tal observação pode ser realizada ao identificar os pontos vermelhos do gráfico.

O nível da confiança se estabiliza depois de uma quantidade de acessos, porém ainda acima da faixa de desconexão, porque a intenção não é desconectar o invasor, apenas limitar o seu acesso aos recursos mais sensíveis. Logo, utilizando o ZT para controle do acesso, foi possível observar, no mesmo instante em que houve uma diferença nas características do dispositivo, que a rede é protegida de um usuário atacante, diminuindo sua confiança a ponto de só poder acessar recursos com baixa sensibilidade, que são os da fatia pertencente ao mMTC.

5.3 Cenário 3: Ataque DoS

Este cenário visa exemplificar a situação em que o usuário, a princípio legítimo, faz uma tentativa de ataque de negação de serviço. Para esta avaliação, consideramos que a sua intenção é tentar sobrecarregar a rede para inviabilizar o acesso aos recursos. Os ataques DoS, conforme explicado na Seção 2.4, podem ser classificados de diferentes formas, mas para o caso dos testes deste cenário, foi realizado um procedimento mais simples. Foi considerado que o usuário realiza uma sobrecarga de acesso ao enviar mais de 40 requisições em menos de 1 minuto de intervalo.

Como pode ser visto na Figura 5.4, novamente os 100 primeiros acessos são equivalentes ao cenário de uso normal. A partir de certo ponto, o usuário que estava acessando os recursos decide fazer uma quantidade de acessos anormal, cerca de 1 acesso a cada segundo. Isso imediatamente quebra a penalidade P5 da Seção 4.2, pois a frequência de acesso no último minuto foi mais alta que a permitida pelo sistema e, assim, a confiança do usuário é penalizada.

Conforme indicado na Figura 5.5, o usuário continuou realizando uma considerável quantidade de acessos, e sua confiança foi reduzindo ao longo do tempo. Ao final, o usuário sai da faixa de confiança do mMTC e é desconectado do sistema. Dessa forma,

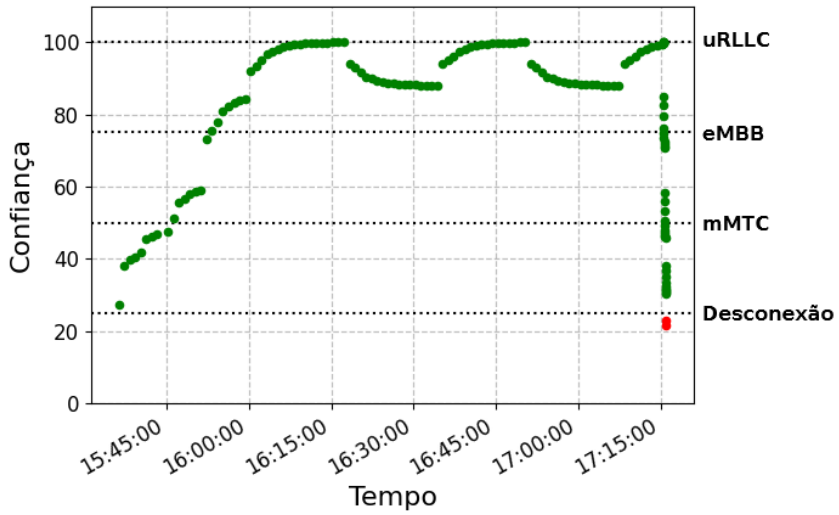

Figura 5.4: Gráfico da Confiança ao longo do tempo de acesso - Cenário 3

foi possível proteger os recursos de uma tentativa de ataque DoS, pois, mesmo que seja um usuário legítimo, o *Zero-Trust* não mantém a confiança a mesma caso ele se comporte de maneira que não é permitida no sistema; logo, ele é penalizado até o ponto de sofrer desconexão.

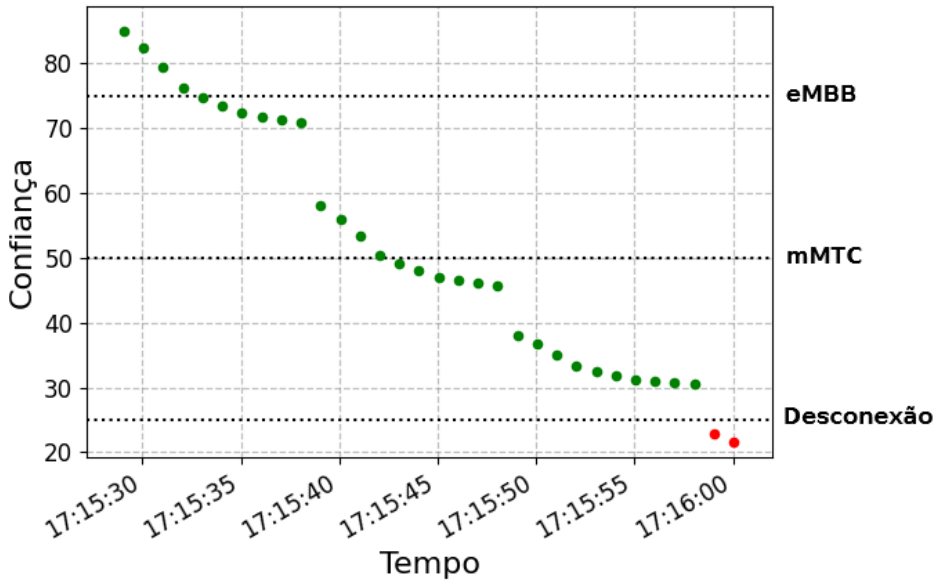

Figura 5.5: Gráfico da Confiança durante a tentativa de ataque DoS - Cenário 3

6 Conclusões e Trabalhos Futuros

Este trabalho apresentou uma proposta de implementação de uma aplicação *Zero-Trust* para fazer o controle de acesso aos recursos das fatias do 5G, com a intenção de aumentar a segurança da rede. Analisando os experimentos realizados, foi possível observar que a ZTA identificou imediatamente os usuários atacantes, considerando as características dos acessos que violaram alguma das penalidades impostas. No caso da tentativa de ataque DoS, por exemplo, o ZT derrubou a conexão de um usuário que, a princípio, era legítimo, mas realizou uma quantidade de acessos acima do permitido em um mesmo minuto. Assim, a partir dos resultados obtidos, a proposta mostrou-se eficiente em proteger recursos de fatias da rede com sensibilidade mais alta, como é o caso do URLLC, garantindo a segurança para tais recursos.

Considerando a possibilidade de trabalhos futuros, uma ideia a ser explorada é o aprimoramento da defesa do sistema contra ataques de negação de serviço. Como citado na Seção 2.4, há várias formas de ataques DoS, e no experimento relacionado, foi feito um ataque mais simplificado, logo não há garantias de segurança contra ataques mais complexos. Portanto, é interessante fazer um estudo mais aprofundado de melhorias no sistema para maior proteção contra esse tipo de ataque.

Outro ponto a ser investigado no futuro é a inclusão da autenticação do 5G durante o uso do sistema, pois na Seção 4.1, foi especificado que ela não seria incluída no desenvolvimento da aplicação. Logo, poderia ser observado como a inserção da autenticação, ou mesmo de outros elementos do 5G, afetaria o sistema.

Sugere-se como um possível próximo passo da avaliação da aplicação proposta e da sua modelagem, a integração a um ambiente SDN e 5G com a reprodução de tráfego de rede real. Para tanto, é necessária a aquisição de um conjunto de dados de acesso real, e posteriormente, a configuração de um ambiente SDN cujo controlador da rede realize as vezes do PEP. Após este passos, acreditamos que a migração do PEP para o ambiente core do 5G seja possível, a fim de concluir a integração. Investigações sobre cada um dos pontos citados são interessantes para o estado da arte do tema, e têm potencial para

avanços significativos para a pesquisa.

Independentemente do que mais poderia ser tratado a respeito do tema, a proposta e os experimentos responderam à principal questão de pesquisa deste trabalho, confirmando que uma implementação da arquitetura *Zero-Trust* sugere um aumento na segurança no acesso aos recursos e aplicações ofertados pelo 5G.

Bibliografia

3GPP. *5G System Overview*. 2022. Disponível em: ⟨https://www.3gpp.org/technologies/5g-system-overview/⟩.

AIELLO, S. Zero trust: A governance perspective. *SSRN 4146521*, papers.ssrn.com, 2022. Disponível em: ⟨https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4146521⟩.

ANATEL. *5G completa dois anos de implantação no Brasil*. 2024. Disponível em: ⟨https://www.gov.br/anatel/pt-br/assuntos/noticias/5g-completa-dois-anos-de-implantacao-no-brasil⟩.

CHEN, B.; QIAO, S.; ZHAO, J.; LIU, D.; SHI, X.; ... A security awareness and protection system for 5g smart healthcare based on zero-trust architecture. *IEEE Internet of ...*, ieeexplore.ieee.org, 2020. Disponível em: ⟨https://ieeexplore.ieee.org/abstract/document/9273056/⟩.

CISO ADVISOR. *Ataques de botnet IoT ameaçam redes de telecom no mundo*. 2023. Disponível em: ⟨https://www.cisoadvisor.com.br/ataques-ddos-de-botnet-iot-ameacam-redes-de-telecom-no-mundo/⟩.

DANGI, R.; LALWANI, P.; CHOUDHARY, G.; YOU, I.; PAU, G. Study and investigation on 5g technology: A systematic review. *Sensors*, M D P I AG, v. 22, n. 1, 2022. ISSN 1424-8220.

EDRIS, E. K. K.; AIASH, M.; LOO, J. Formalization and evaluation of eap-aka' protocol for 5g network access security. *Array*, v. 16, p. 100254, 2022. ISSN 2590-0056. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S259000562200087X⟩.

FREITAS, L.; COELHO, K.; NOGUEIRA, M.; VIEIRA, A.; NACIF, J.; SILVA, E. Controle de acesso sensível ao contexto e zero trust para a segurança em e-health. In: *Anais do XLII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Porto Alegre, RS, Brasil: SBC, 2024. p. 770–783. ISSN 2177-9384. Disponível em: ⟨https://sol.sbc.org.br/index.php/sbrc/article/view/29834⟩.

GONçALVES, D.; BITTENCOURT, L.; MADEIRA, E. Alocação de fatias de rede fim-a-fim para usuários móveis utilizando o simulador mobfogsim. In: *Anais do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Porto Alegre, RS, Brasil: SBC, 2022. p. 112–125. ISSN 2177-9384. Disponível em: ⟨https://sol.sbc.org.br/index.php/sbrc/article/view/21165⟩.

GOULART, G. R.; DANTAS, M. A. R. Controle de acesso baseado em papéis em ambientes assistidos. *Revista Eletrônica de Iniciação Científica em Computação*, v. 16, n. 5, nov. 2018. Disponível em: ⟨https://journals-sol.sbc.org.br/index.php/reic/article/view/1074⟩.

GUEDES, D.; VIEIRA, L.; VIEIRA, M.; RODRIGUES, H.; NUNES, R. Redes definidas por software: uma abordagem sistêmica para o desenvolvimento de pesquisas em redes de computadores. In: _____. [S.l.: s.n.], 2014.

HU, V. C.; KUHN, D. R.; FERRAIOLO, D. F.; VOAS, J. Attribute-based access control. *Computer*, v. 48, n. 2, p. 85–88, 2015.

ITU. *Minimum requirements related to technical performance for IMT-2020 radio interface(s)*. 2017. Disponível em: ⟨https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf⟩.

ITU. *Setting the Scene for 5G: Opportunities & Challenges*. 2018. Disponível em: ⟨https://www.itu.int/en/ITU-D/Documents/ITU_5G_REPORT-2018.pdf⟩.

KASPERSKY. *A tecnologia 5G é perigosa? Prós e contras da rede 5G*. 2023. Disponível em: ⟨https://www.kaspersky.com.br/resource-center/threats/5g-pros-and-cons/⟩.

MECHAILEH, J. A. *Segurança em Redes 5G*. 2023. Disponível em: ⟨https://edge.uol/en/insights/article/seguranca-em-redes-5g/⟩.

OLSSON, J.; SHOROV, A.; ABDELRAZEK, L.; WHITEFIELD, J. 5g zero trust – a zero-trust architecture for telecom. *Ericsson Technology Review*, v. 2021, n. 5, p. 2–11, 2021.

OYEYINKA, F.; IDOWU, S.; KUYORO, A.; JOSHUA, J.; AKINSANYA, A.; EZE, M.; SEUN, E. A critical comparative study and characterisation of access control model. *International Journal of Computer & Organization Trends*, v. 8, p. 7–17, 06 2018.

ROSE, S.; BORCHERT, O.; MITCHELL, S.; CONNELLY, S. *Zero Trust Architecture*. 2020.

TEERAKANOK, S.; UEHARA, T.; INOMATA, A. Migrating to zero trust architecture: Reviews and challenges. *Secur. Commun. Networks*, v. 2021, p. 9947347:1–9947347:10, 2021. Disponível em: ⟨https://api.semanticscholar.org/CorpusID:235396811⟩.

WANG, T.; GUO, Z.; CHEN, H.; LIU, W. Bwmanager: Mitigating denial of service attacks in software-defined networks through bandwidth prediction. *IEEE Transactions on Network and Service Management*, IEEE, v. 15, n. 4, p. 1235–1248, 2018.

XIA, W.; WEN, Y.; FOH, C. H.; NIYATO, D.; XIE, H. A survey on software-defined networking. *IEEE Communications Surveys & Tutorials*, v. 17, n. 1, p. 27–51, 2015.

XU, Q.; ZHENG, R.; SAAD, W.; HAN, Z. Device fingerprinting in wireless networks: Challenges and opportunities. *IEEE Communications Surveys & Tutorials*, v. 18, n. 1, p. 94–104, 2016.

YUAN, E.; TONG, J. Attributed based access control (abac) for web services. In: *IEEE International Conference on Web Services (ICWS'05)*. [S.l.: s.n.], 2005. p. 569.

ZHANG, P.; WANG, H.; HU, C.; LIN, C. On denial of service attacks in software defined networks. *IEEE Network*, v. 30, n. 6, p. 28–33, 2016.

ZLOMISLIć, V.; FERTALJ, K.; SRUK, V. Denial of service attacks: An overview. In: *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*. [S.l.: s.n.], 2014. p. 1–6.